NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

TERRORIST APPROACH TO INFORMATION OPERATIONS

by

Robert S. Earl
and
Norman E. Emery

June 2003

Thesis Advisor: Dorothy Denning
Co-advisor: Raymond Buettner

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Terrorist Approach to Information Operations		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Robert S. Earl and Norman E. Emery			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

ABSTRACT ***(maximum 200 words)*** This thesis provides insight into how terrorist organizations exploit the information environment to achieve their objectives. The study establishes an analytical IO framework, by integrating US military doctrine with a fundamental approach to IO theory. The framework proves useful in examining the IO tools terrorists have assembled and how they implement them to influence their target audiences. The thesis shows that terrorists are, indeed, naturally linked to the information environment by their nature and strategy. Generally speaking, all terrorists employ IO tactically to enhance their operations. However, many organizations have a profound understanding of the information environment and also have the ability to manipulate information to achieve their objectives. Since, terrorist organizations are militarily weaker than the states they face and cannot rely on physical attacks to accomplish their goals, they must adopt an information strategy to achieve their objectives. This thesis emphasizes three primary conclusions: first terrorist conduct violent attacks in the physical environment to enable operations in the information environment. Second, terrorist integrate offensive and defensive IO to survive and appear legitimate to potential supporters and to the state. Finally, terrorists intentionally target four different audiences: opposing, uncommitted, sympathetic, and active to influence their perceptions.

14. SUBJECT TERMS Information Operations, Information Warfare, Terrorism, Counter-terrorism, Intelligence, Counter-intelligence			**15. NUMBER OF PAGES** 162
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A TERRORIST APPROACH TO INFORMATION OPERATIONS

Robert S. Earl
Major, United States Army
B.A., Washington University, 1989

Norman E. Emery
Major, United States Army
B.A., Illinois State University, 1989

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Authors: Robert S. Earl

Norman E. Emery

Approved by: Dorothy Denning
Thesis Advisor

Raymond Buettner
Co-Advisor

Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis provides insight into how terrorist organizations exploit the information environment to achieve their objectives. The study establishes an analytical IO framework, by integrating US military doctrine with a fundamental approach to IO theory. The framework proves useful in examining the IO tools terrorists have assembled and how they implement them to influence their target audiences. The thesis shows that terrorists are, indeed, naturally linked to the information environment by their nature and strategy. Generally speaking, all terrorists employ IO tactically to enhance their operations. However, many organizations have a profound understanding of the information environment and also have the ability to manipulate information to achieve their objectives. Since terrorist organizations are militarily weaker than the states they face and cannot rely on physical attacks to accomplish their goals, they must adopt an information strategy to achieve their objectives. This thesis emphasizes three primary conclusions: first terrorist conduct violent attacks in the physical environment to enable operations in the information environment. Second, terrorist integrate offensive and defensive IO to survive and appear legitimate to potential supporters and to the state. Finally, terrorists intentionally target four different audiences: opposing, uncommitted, sympathetic, and active to psychologically influence their perceptions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

I. INTRODUCTION

A. TERRORISM – AN INFORMATION WAR.

When US President George W. Bush declared war against terrorism, or more pointedly, against Al Qa'ida, the United States entered an obscure paradigm of conflict. The terror organizations lurking in this paradigm are different from the conventional foes of our past and pose many asymmetric challenges for a nation accustomed to thinking about war as primarily inter-state conflict. Most notably, America has found itself at war with a covert, illegal, non-state actor with global reach. Terrorist organizations are not constrained by moral or ethical rules and regularly ignore state and international laws governing warfare. Terrorists rely on secrecy to survive and often live underground, which make them very hard to find and destroy. The fact that terrorists are non-state actors further adds to the difficulty the US faces in dealing with them. There are no state governments or authorities with which to negotiate or to hold accountable. Additionally, terrorists employ a strategy of warfare very different from our own. They cannot afford to fight a conventional attrition-based war, as we are accustomed, where the winning side in the conflict is the one who physically forces the other to capitulate. Terrorist organizations would quickly become extinct employing such a strategy against a powerful nation. Rather, terrorists fight an attrition-based war of the 'will'. They attempt to wear down the will of government leaders by terrorizing their populace. Albert Bandera suggests "terrorists try to exercise influence over targeted officials or nations through the intimidation of the public and the arousal of sympathy for the social or political causes they espouse" (Nacos, 1994, p.1). Terrorism is a political and psychological weapon directed at targets that neither caused nor are able to solve the problem that motivates the terrorists.

Usama bin Laden has waged such a psychological war of wills with the United States for nearly a decade. Al Qa'ida is suspected of conducting several attacks against the US to include: Somalia in 1993, the 1993 World Trade Center bombing, the 1998 Embassy bombings in Africa, and the suicide boat attack

against the USS Cole in 2000. The attack on September 11th, however, perhaps illustrates this psychological strategy most clearly. The nineteen radical Islamic men responsible for the devastation on September 11th were part of a covert organization with global reach and had been 'riding the rails' of American society for many months preparing for the attack on America. Their very lives had become a deception: posing as students and businessmen. This deceptive cover allowed them to live and work among us for months, gathering intelligence until the time came to act. Early Tuesday morning, September 11th, 2001, they boarded four United and American Airlines passenger planes. Armed with common grocery store box cutters, these men executed the bloodiest attack on American soil since the Civil War. Yet, Usama Bin Laden's main goal in undertaking the attack on September 11th was not merely to kill thousands of people. Rather it was likely meant to send a message worldwide to millions of people and to influence their governments. Bruce Hoffman suggests that "terrorism may be seen as a violent act that is conceived specifically to attract attention and then, through the publicity it generates, to communicate a message" (Hoffman, 1998, p.131). Bin Laden's 1998 *fatwa*, the Declaration of the World Islamic Front for Jihad against the Jews and the Crusaders, describes the U.S. presence in Saudi Arabia as a catastrophe that has humiliating and debilitating effects on the Muslim people. Bin Laden writes, "Since God laid down the Arabian Peninsula, created its desert, and surrounded it with its seas, no calamity has ever befallen it like these Crusader hosts that have spread in it like locusts, crowing its soil, eating its fruits, and destroying its verdure" (Lewis, 1998, p.14).

On September 11th, 2001, Al Qa'ida attacked the World Trade Center and the Pentagon, and had planned to hit either the Capitol or the White House. These targets were likely selected to send a message to four primary audiences: the active, opposing, sympathetic and uncommitted.

- The active audience: to Al Qa'ida supporters and active sympathizers, Usama bin Laden proclaimed that the US was vulnerable to attack. His organization had succeeded in destroying the WTC and striking the Pentagon, the US military headquarters.

The attack was likely intended to rally Islamic support for Al Qa'ida, encouraging enlistment into their ranks and, in general, to bring all Islamic peoples to join in his Jihad against the US and other Western countries.

- The opposing audience: Usama bin Laden's message was likely intended to strike fear in the US populace, generating doubt in the ability of the government to safeguard them. The attacks portrayed to the American public that despite all the government defenses—the army, police force, and FBI—Americans will never be safe from attack. Once civilians feel unsafe in their own homes and workplaces, daily life is disrupted, causing considerable harm to personal and national morale.
- The sympathetic audience: Bin Laden's message to the sympathetic audience was likely intended to rally other conservative Islamic state and non-state actors behind his Jihad against the US and Israel. He likely intended to unify the extreme fundamentalist, while also pressuring the more liberal Islamist members into becoming more conservative.
- The uncommitted audience: Additionally, the terror attacks sent a third message to international populace. To the rest of the world, bin Laden presented the attack as an example of his determination to achieve his political aims by any means and at any cost. The terror attack was intended to draw the attention of international public opinion to the conflict and bin Laden's demands.

Al Qa'ida's psychological strategy likely intended to use all three of these audiences to pressure President Bush to withdraw US troops from Saudi soil and other Muslim-held lands. (Ganor, 2002). This thesis further explores the relevance of the different audiences in chapter III.

Al Qa'ida and other terrorist organizations bring an interesting toolkit to the fight that enables them to compete in what is essentially a battle of information: a battle that involves sending terrifying information to one audience, while at the same time seeking the sympathy and support from another. Although it is the violent physical act of the terrorist that captures our attention, it is the psychological influence in the information realm that gives the terrorist leverage. We believe terrorist organizations rely on the power of information to sway public attention and pressure decision makers to make changes favorable to the terrorists. Dorothy Denning, author of *Information Warfare and Security* and

professor at the Naval Post Graduate School, suggests that terrorists are very adept at information warfare and often exploit emerging technology to leverage information (Denning, 1999, p.68).

Making the claim that terrorists enhance their coercive power by manipulating the information environment, this thesis will provide insight into this phenomenon. If the US is to combat terrorist organizations in the information environment, we must gain a better understanding of this toolkit that allows them to leverage information. The US Department of Defense (DoD) has developed theory and doctrine relating to Information Operations (IO) and provides great insight into activities in the information domain. US military units routinely employ IO against their adversaries. The possibility that terrorist organizations also employ IO tools against our national interests is real and deserves additional analytical attention and increased public awareness.

B. THESIS OVERVIEW—SCOPE OF THIS STUDY.

The purpose of this thesis is to explore different terrorist organizations to determine how they employ Information Operations to achieve their objectives. In order to explore this phenomenon, the thesis takes the following path. First, we examine key concepts to establish a general foundation for thinking about terrorism and Information Operations. Next, we survey the Department of Defense's approach to IO. The Department of Defense provides valuable insight into the concept of IO through theoretical and doctrinal publications. Additionally we explore Edward Waltz's theoretical perspective of the concept of Information Operations. Although other theories exist in the literature, Waltz's fundamental approach to the information environment provides a suitable framework for the purpose of this thesis. Adapting Waltz's framework to a series of terrorist case studies, we will provide a new framework illustrating how terrorists use Information Operations to achieve their objectives. Finally, the thesis concludes with a synopsis of the evidence and a net assessment of the terrorists' ability to leverage Information Operations to support campaigns of terror. By exposing how terrorist employ Information Operations, we hope to help the United States

combat these asymmetric enemies in the information domain and reduce their influence and attacks.

C. KEY CONCEPTS.

Before beginning a study of how terrorist organizations employ Information Operations, we must first establish a basic foundation. In particular four questions must be addressed. What are Information Operations? What are some common misperceptions of Information Operations? What is terrorism? Finally, why do terrorists use Information Operations? The answers to these questions provide the reader a foundation to further explore IO theory and doctrine, and the approach terrorists take to exploit the information environment.

1. What are Information Operations?

> There's a war out there old friend- a world war. And it's not about who's got the most bullets; it's about who controls the information. What we see and hear, how we work, what we think. It's all about information.
>
> *Cosmo*

The US Department of Defense offers two different approaches to operating in the information environment, which has resulted in a smorgasbord of different terminology. Information Warfare (IW) is a concept consisting of six existing functional elements that are only employed during actual times of conflict or combat. Information Operations (IO) is a concept consisting of two additional functional elements; however, IO is more comprehensive and is intended to be part of a strategic campaign conducted "throughout the full spectrum of conflict from peace to war and back to peace again" (Armistead, p.13).[1] Since active terrorist organizations are continuously alternating between violent attacks and peaceful activities, their actions are better explained with a full-spectrum

[1] Joint and Army doctrine differ slightly on what elements belong in IO. The IO field has developed rapidly and it may take time for a common position to emerge. IW: Operations Security (OPSEC), Psychological Operations (PSYOP), Military Deception, Electronic Warfare (EW) and Computer Network Operations (CNO), physical destruction; IO adds public affairs (PA) and civil-military operations (CMO).

approach to IO. Therefore, this thesis will use the term IO to explore terrorists' actions in the information environment.

The information revolution has ushered in advanced technology and new networking concepts that have changed the way we live and work in the world today. In Edwin Armistead's, *Hard Reality of Soft Power*, Dan Kuehl suggests that we live in what is called the Global Information Environment (GIE): an information fishbowl. He writes, "the Global Information Environment has become a battle space in which technology is used to deliver influential *content* in order to shape perception, influence decisions, and control behavior" (Armistead, 2002, p.4). More and more of the world's population are joining the GIE, creating a global hyper-sensitivity to information. In a world where information is becoming increasingly important, Information Operations are become increasingly potent. IO provides the means to leverage information, focusing on the 'wetware', the gray matter of the human brain where perceptions are formed and decisions are made. From a military perspective IO enables a commander to gain an information advantage at decisive moments over his enemy. With this information superiority, the commander can potentially exploit the enemy's vulnerabilities, saving friendly lives and greatly influencing the outcome of the battle.

In the preface to Winn Schwartau's book *Information Warfare,* John Alger highlights the goals of Information Operations: "those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to gain a significant advantage, objective, or victory over an adversary" (Schwartau, 1999). Information Operations is a relatively new concept, although most of its elements are not new. In fact, history is filled with examples of individual elements of IO being employed by skillful commanders. During biblical times the Israeli leader, Joshua, defeated the well-fortified city of Ai, by employing

deception, psychological operations, and sound operations security.[2] The US Army has in the last century routinely employed elements of IO. From the Normandy Invasion in World War II to General Schwartzkopf's famous left hook during the 1991 Persian Gulf War, psychological operations, deception, public and civil affairs, electronic warfare, and operations security have provided commanders valuable tools during many historical battles. Chapter II presents an example of US IO during the 1991 Persian Gulf War with Iraq. In the past ten years information technology has made profound advances, creating powerful information systems and communication networks. The US military has adapted this technology to create a new element of IO involving the use of computers and networks. Computer Network Operations is the only new element of IO. The thesis explores all of the elements of IO in detail in chapter II.

The concept of IO integrates all of the above individual elements into one strategy to provide the commander an unprecedented synergistic tool, which allows him to gain information superiority over his adversary at decisive points during the battle. Many of the IO tools do not rely upon advanced technology and are available to friend and foe alike. Therefore, the better we understand the power of information to influence decisions and develop the tools to leverage information, the greater advantage we will have in future battles. Concepts such as the Information Environment, Influence Operations, and the role of information to influence decisions will be further explained in chapter II as well.

[2] In roughly 1200 BC, Joshua captured the city of Ai by means of deception, shortly after the fall of Jericho. After suffering a minor defeat in his first attempt at taking the city, Joshua devised a ruse that has been repeated countless times since: the feigned retreat. Arraying the bulk of his host before the gates of Ai, Joshua offered battle, all the while hiding a goodly portion of his force to the rear of the city, out of sight. When the soldiers of Ai took the field and began battling his men, Joshua ordered a retreat designed to look as if it were a rout. When the exultant men of Ai came after them, Joshua's hidden force emerged and stormed Ai, overwhelming the skeletal force left behind and seizing the city. As the news hit the men of Ai their charge faltered, and Joshua wheeled his force and pinned them between his men and the now-captured city. Their force in disarray, the men of Ai were slaughtered. (Handel, 1985, and Dunnigan and Nofi, 1995.)

2. What are Some Common Misperceptions of Information Operations?

There are three common misperceptions many people have concerning Information Operations. First, since the advent of the information revolution and advanced technology, IO is often equated to the use of advance technology. However, the use of advanced technology does not constitute IO, but rather reflects our military's advanced state of modernization and sophistication. Chapter II gives an example in Somalia, when a technologically inferior foe, General Aideed, exploited the information environment to great effect. Equipped with an understanding of the power of information, Aideed turned a military defeat into an information war win. Second, IO is often thought of as merely the employment of one of its functional elements. For example, psychological operations (PSYOP) or computer network operations (CNO) are often singled out as being IO. While both are principle elements of the IO concept, when taken individually they do not adequately reflect the integration or strategy of IO. PSYOP leaflets and broadcasts, computer hacking, and network defense are all important elements of IO, but fail to individually create the full-spectrum synergy necessary to achieve information superiority. Finally, a common statement made about IO is: "IO is nothing new." As stated earlier, the principle elements of IO have existed since Biblical times; however, "What is new is bringing these elements together as components of the information element of combat power. The IO concept focuses efforts that before were diffuse" (FM 3-13 1-57).

3. What is Terrorism?

Terrorism by nature is difficult to define. The lengthy, evolving history of terrorism and today's faddish use of the word in the media has hindered us from adopting a widely accepted definition. Terrorist acts conjure up negative emotional responses in the victims (those hurt by the violence and those affected by the fear) as well as in the terrorists themselves. Therefore, when we label someone as a terrorist, we are subjecting him or her to our own moral judgment (Jenkins, 1978, p.3). People see the same act and interpret it according to their own beliefs and experiences. Many of the leading terrorist authorities would

agree that terrorism is difficult to define. Laqueur explains this difficulty in his book *The New Terrorism: Fanaticism and The Arms of Mass Destruction.* He quotes Nietzsche suggesting, "Only things without a history can be easily defined; terrorism, needless to say has a very long history" (Laqueur, 1999, p.6). Often many people refer to this difficulty in reaching a definition of terrorism as the old cliché, 'one man's terrorist is another man's freedom fighter'. However, Brian Jenkins dismisses this adage as simply not true. He suggests, "Most civilized nations have identified by law modes of conduct that are criminal, among them homicide, kidnapping, threats to life, and willful destruction of property" (Jenkins, 1978, p.4). He further asserts that even in war there are rules that regulate appropriate conduct. Terrorists do not abide by any of these rules. Although there are slight differences in the definitions of terrorism found in the United States government, these differences actually only reflect the emphasis of the function of each agency. The FBI provides a suitable definition for the purposes of this thesis.

"Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

4. Why do Terrorists use Information Operations?

Unlike the US military, which has only recently developed an IO strategy, terrorist organizations have existed for centuries employing a psychological strategy. The US military has generally relied on attrition-based warfare to achieve its objectives. Since terrorist organizations are usually not at military parity with a state, they cannot go toe-to-toe in combat and hope to win. Terrorists resort to IO, because that is the only option they have. To provide additional evidence of why terrorists resort to IO, we will briefly explore two perspectives of terrorism that grant insight into their strategy. First, the chapter examines Maurice Tugwell's psychological strategy of terrorism. Tugwell suggests that terrorists employ a strategy of psychological influence, relying on the use of terror to coerce a government to make changes favorable to their

cause. This strategy leverages the power of information to cause change and Tugwell claims "terrorists are in the business of changing minds" (1990, p.2). Subsequently, the chapter addresses Gordon McComick's terrorist influence process model. McComick's model provides insight into how most terrorist organizations exploit the information environment to influence their targets. His model walks through a four step process terrorists take to achieve their influence objective.

a. Maurice Tugwell's Psychological Strategy of Terrorism.

Many theorists have written about the strategy of terrorist organizations, offering different viewpoints about why terrorists do what they do; however, one expert, Maurice Tugwell, has made detailed studies of the strategic goals of terrorist, guerrilla, and insurgent organizations for over twenty years. Tugwell's perspective of this phenomenon suggests that terrorist organizations employ a long-term psychological strategy to achieve their objectives. His approach supports this thesis by providing insight into why terrorists conduct violent attacks and offers evidence that terrorist rely on the psychological influence of their violence to achieve their objectives. Furthermore, Tugwell's explanation illustrates the terrorists' natural bridge to the information environment.

Tugwell contends that the terrorist threat to societies and states is more about the adverse psychological influence they cause than the actual physical damage they inflict. He says "that terrorism essentially conforms to the Carl von Clausewitz' claim that war is the continuation of politics by violent means" (Radvanyi, 1990, p. 1). Tugwell points out that violent physical force often replaces the failure of peaceful persuasion; however, persuasion still remains the objective and the ultimate purpose of each action. He states that in the end "terrorists are trying to change the minds of their enemies" (Radvanyi, p.11). Terrorism, more than any other form of conflict, moves back and forth across the line between peace and war. "One day its leaders address the public through the news media, in the manner of politicians; the next day, they blow an

airliner out of the sky to underline their point" (Radvanyi, p.2). An ancient millenarian Jewish terrorist group known as the Zealots serves as an example to support Tugwell's claim. From AD 66 – 73 the Zealots ruthlessly assassinated anyone having to do with the Roman Empire: army soldiers, administrators, Jewish collaborators, etc. Using short daggers, known as *sica,* the terrorists would stage the attack in a busy square of the city or in an ally jammed with people. "The intimidatory power of the Assassins rested on their reputation of always killing their chosen victims, however long it took" (Radvanyi, p.2). The killing was usually very dramatic; the terrorists would emerge and slit the throat of the victim and then quickly retreat, blending back into the crowd. The violent attacks were designed to have long lasting psychological repercussions far beyond the immediate audience: the 10 to 20 people who witnessed the event. Over time the vicious reputation of the Zealots spread by word of mouth throughout all of present day Israel. Their reputation preceded them in the information environment to shape the perception of thousands of people, especially those opposed to the group and sympathetic to the Romans (Hoffman, 1998, p.88). Thus as Tugwell points out, the Zealots relied more on the psychological influence of their reputation to influence the populace than the slaying of their victims.

b. Gordon McCormick's Influence Process of Terrorism.

Gordon McCormick, former Rand analyst and current professor at the Naval Post Graduate School, suggests that nearly all terrorists follow a common influence process to achieve their objectives. McCormick's influence model also supports Maurice Tugwell's psychological strategy mentioned above. McCormick suggests that terrorists are naturally linked to the information environment, since they must follow logical steps in order to influence a decision maker. Figure 1 depicts McCormick's influence process model with four steps and three orders of effects.

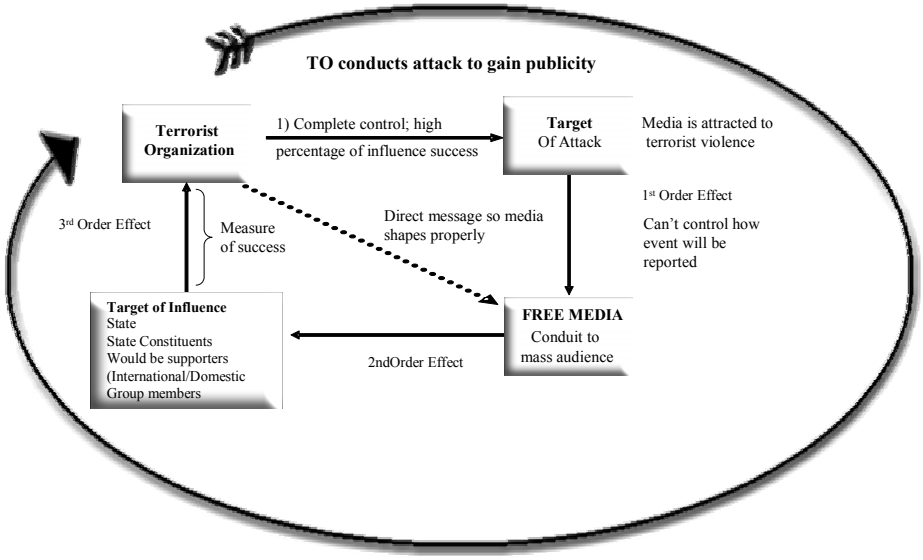

Figure 1. Influence Process Model by Dr. Gordon McCormick

In the first step the terrorists attack the immediate target, often involving dramatic acts of violence intended to capture the eye of the media. The immediate targets are often victims with no authority or individual ability to influence the government. Many terrorist attacks first appear like indiscriminate attacks; however, this is not true. Terrorist chose targets for their maximum publicity and to influence specific target audiences. The second target is the media, which generates the first order effect. The terrorists normally cannot control how the acts will be reported (negatively or positively). Knowing this, many terrorist organizations operate their own underground television, radio, and print media outlets. The also maintain their own informational websites on the Internet. Often times they deliver a direct message to the media through a proxy courier or phone call. During the recent US war in Afghanistan, Usama bin Laden provided video taped interviews to Al-Jazeera in order to deliver his message. The third step is when the media serves as the distribution point, propagating scenes of the attack to a wider audience, which is the target of influence. The second order effect occurs here. Today's technology often allows near-real time video

coverage of events. Al Qa'ida's attack against the US World Trade Center and Pentagon and the Chechen hostage taking in Moscow serve as two recent examples of the media providing live coverage of an attack. CNN alerted the entire world to the first attack against the Pentagon and World Trade Center and then provided live footage as the second American Airliner exploded into the side of the World Trade Center and the subsequent collapse of the building. Another example came in 2003 with the live coverage of 50 Chechen terrorists holding nearly 900 Russian theatergoers hostage. Video coverage highlighted the commandos attempted rescue. The police employed gas during the attack to incapacitate the terrorists. Unfortunately, due to the concentration of the gas and poor health conditions of many of the hostages, over 100 hostages died during the attack. The media provides the terrorists a conduit to four different audiences: opposing, uncommitted, sympathetic, and active. These audiences will be further addressed in chapter III. The third order effect occurs when the target of influence reacts. The measure of success is determined by who gains and benefits, impacting the terrorist group and completing the cycle.

The 1972 terrorist attack at the Munich Olympic Games provides an example of McCormick's terrorist influence model. Eight members from the PLO's Black September Organization had planned to take several Israeli athletes hostage and then make demands of the Israeli government to release Palestinian terrorists being held in prison. With the advent of television and worldwide broadcasting, the world watched as the German police foiled the Palestinians' original plan to move the hostages from helicopters to an awaiting Lufthansa 747 airliner. During the ensuing gun battle with the Germans, a terrorist leaped from one of the helicopters and tossed a hand grenade back into the cabin behind him, murdering all nine Israeli athletes with a hand grenade (Hoffman, p.72). Although the Black September operation failed to secure the freedom of their comrades in prison, the shock and violence of the attack at the Munich Stadium had a profound influence on television viewers around the world. The Israeli Olympic athletes served as a superb immediate target for the terrorists. The media coverage of the Games ensured that millions of people would be

watching. Although Black September's operation received negative publicity from the horrific fate of the athletes, the greater world audience became aware of the plight faced by the Palestinian refugees. Hoffman quotes Abu Iyad, the PLO's intelligence chief, admitting, "they didn't bring about the liberation of their comrades imprisoned in Israel as they had hoped, but they did attain the operation's other two objectives: World opinion was forced to take note of the Palestinian plight, and the Palestinian people imposed their presence on an international gathering that had sought to exclude them" (Hoffman, p.73). Eventually, international sympathy toward the Palestinian cause enabled Yassar Arafat and the Palestinians to gain a seat in the United Nations (Gallagher, 1992).

D. STRUCTURE OF THE THESIS: A CHAPTER OUTLINE.

This chapter provides an introduction to our thesis by presenting the need to understand how terrorist exploit the information environment and use IO to achieve their objectives. The chapter also established a basic understanding of Information Operations and terrorism, providing perspectives by two authors, Tugwell and McCormick, on the terrorists' use of information to achieve their objectives.

Chapter II explores the principle elements of IO prescribed in US military doctrine and explains the information environment. The chapter examines a perspective of IO developed by Edward Waltz. First, Waltz provides an explanation of the role of information in conflict. Next, he presents his operational model of IO activities in three conceptual domains. The chapter then adapts US military principle elements of IO to Waltz's conceptual domains in order to create a useful framework to apply to terrorists.

Chapter III develops the IO framework into an analytical tool that the thesis uses to evaluate the terrorist case studies. To accomplish this goal the chapter first explores works by several well-known terrorist authors to highlight the characteristics of terrorist organizations that can have an impact on how terrorists employ IO. With the theoretical understanding of IO established in

Chapter II, the chapter develops the framework by examining three aspects of the terrorists' approach to IO. First, the terrorists conduct the attack in the physical environment to directly influence an audience or to enable operations in the information environment. Second, the terrorists employ elements of IO as a force multiplier to gain legitimacy e.g. leverage with the state actor. Third, the terrorists are able to take the action in the physical environment and target their message to address multiple audiences.

Chapters IV and V provide evidence of our claims using two terrorist organizations, namely, Al Qa'ida and the Provisional Irish Republican Army. The chapters provide a brief historical background, presenting the respective non-state terrorist organizations and their operating environments to determine how they employ IO tools to leverage information against states. The chapters investigate examples from two distinctly different types of terrorist organizations: radical Islamic Fundamentalist religious groups and ethno-nationalist separatist groups. The terrorist group typologies categorized in the *1999 Government Report on Profiling Terrorist* provided a basis for case selection. We selected the organizations based on their histories of active terrorism, the availability of data, and their representation of different types of terrorist groups. Usama bin Laden's Al Qa'ida terrorist organization is a unique network of Islamic Fundamentalist groups with global reach seeking radical political reformation among liberal Islamic states and the eviction of Western influence from the Islamic world. The Provisional Irish Republican Army (PIRA) is broadly representative of ethno-nationalist separatist organizations. The PIRA sees itself as a nationalistic group working to free Ireland from English control and can be compared to other such groups as the Liberation Tigers of Eelam (LTTE), fighting in Sri Lanka, and the Euzkadi Ta Askatasuna (ETA), Basque separatists fighting in Northern Spain and Southern France. The PIRA is representative of a small number of highly professional underground armies, which draw on a long tradition of paramilitary resistance to the state's power. These two sample non-state organizations therefore have quite different requirements. The role of Information Operations serves different functions for each one.

Chapter VI provides a synopsis of how non-state terrorist organizations may incorporate Information Operations to achieve their objectives. The chapter provides general concluding remarks, reflecting commonalties and differences between the two types of terrorist organizations, each competing in very different operating environments. The chapter also offers a framework of terrorist information operations, highlighting tendencies and trends. It closes with a number of questions for further research.

II. THEORY OF INFORMATION OPERATIONS

> To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.
>
> - Mao Tse-tung, *On Protracted War*

The goal of this chapter is to explore the concept of Information Operations (IO) and establish a theoretical understanding of operations in the information environment. We accomplish this goal by first analyzing Department of Defense (Joint and Army) doctrine. Joint Publication 3-13, *Joint Doctrine for Information Operations;* Army Field Manual 3-13, *Information Operations: Tactics, Techniques, and Procedures;* and Army Field Manual 3-0, *Operations*, provide a doctrinal approach to IO. We selected DoD as our starting point, because the principles established in US military doctrine have proven to be sound during times of peace and conflict and provide a valuable basis for understanding IO. Next we examine a theoretical perspective to information domains and the influence of Information Operations by Edward Waltz, author of *Information Warfare: Principles and Operations*. Waltz constructs an information model of warfare, providing a better understanding of the role of information in conflict. Waltz's model of information domains provides the basis for establishing a theoretical understanding of IO.

Although we also reviewed other academic perspectives to the concept of Information Operations and the terrorists' use of IO (often referred to as information warfare), these works proved to be inappropriate for the focus of this thesis.[3]

[3] Other approaches to Information Operations include works from Dorothy Denning, Martin Libicki, Andrew Rathmell, and Mike Tanji.

A. INFORMATION ENVIRONMENT.

> The information environment is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself.
>
> US Army Field Manual 3-13

This section will first explore aspects about the information environment. US military doctrine often makes reference to two different yet coexisting arenas: the physical and the information arena. Humans live, breath, and walk in the physical arena. We see, hear, and touch objects that are real and exist in a physical state. US commanders make decisions that impact the physical arena such as to attack the enemy or defend. All of us are keenly aware of the physical arena, because we exist in it daily; however, many people do not realize that another arena coexists and oftentimes dramatically influences what happens in the physical. The information arena exists in the minds of humans, in decision-making processes, and information processing machines. Psychological and physical activities can affect this arena, shaping human perceptions and influencing peoples' beliefs. Corporate marketers commonly exploit the link between the two arenas, influencing consumers to buy products or services. Humans are attracted to visual aides: we tend to trust what we can see in the physical arena.

Often CNN and other popular news media rely on B-Roll (still pictures, audio, and real-time video) to capture the attention of their audiences. Advanced technology enables media outlets to incorporate B-Roll with the news broadcast, transforming an abstract, lifeless news article into dramatic and suspenseful stories. The visual aid of B-Roll enhances the 'believability' of information in the story. Because the media (television in particular) has access to such a large audience, it has wielded great power in American and world affairs. Media coverage of the US involvement in Somalia had great impact on President Clinton's decision to pull troops out of the country. "General Aideed manipulated the media to keep the militarily superior United States off balance…and forever changed US foreign policy in the region" (Armistead, 2002, p.11). This powerful

influence that B-Roll unleashes serves to segue into the unseen yet coexisting information arena, where information of all forms wields the power to influence. The US Army refers to this unseen arena as the Information Environment (IE) and treats it as another component of the battlespace (FM 3-13, p.1-2).

So what exactly is the IE component of the combat battlespace? Coexisting with the physical environment, the IE is a perceptual battlespace. Information or the denial of information shapes the IE, influencing decision makers, groups, and even whole populations. The IE typically is not limited to the linear battlespace that military commanders conceptualize, but activities in the IE oftentimes shape a commander's understanding of the battle and can profoundly impact his decisions in the physical environment. A commander can target systems and actors in the IE with the ultimate goal of impacting key adversary decision makers in the physical environment.

The IE includes "worldwide communication networks, friendly and adversary forces and organizations' command and control (C2) systems, and friendly, adversary, and other personnel who make decisions and handle information, including populations" (FM 3-13, p.1-2). Handling this information in the IE is a networked infrastructure of individual people, groups and organizations, and information systems (JP 3-13). Twenty-first century technologies, such as home computers, the Internet, and digital satellite communications, have networked the IE in such a manner that people world-wide can now be influenced. CNN broadcasted live to the world the tragic Al Qa'ida attack on September 11th 2001. Hundreds of millions of people watched the terrorists' spectacle unfold as the 2nd American Airlines passenger jet slammed into the World Trade Center, which subsequently collapsed upon itself, killing thousands of people inside. In the recent 2003 war with Iraq, embedded media reporters from the BBC, CNN, al-Jazeera, and other international media traveled with American military units throughout the war. Their broadcasts enabled anyone with access to a television or computer the ability to see the war live. Americans witnessed the US 3rd Infantry Division as it crossed the Tigris River and moved into Baghdad.

The US military employs Information Operations to gain an advantage over the adversary in the IE. This information advantage enables the conduct of successful combat maneuver operations in the physical environment. US doctrine calls this phenomenon information superiority[4]. Achieving superiority in the IE provides battlefield clarity to the friendly commander, while at the same time obscures the battlefield for the adversary, denying him options and possibly causing him to be more reactionary. The friendly commander can then trump the adversary movements at decisive moments, allowing him to "seize and retain the initiative" (FM3-13, p.1-17). Unlike air superiority, which can be maintained and easily determined, information superiority can be fleeting and gained or lost through the passage of time. It is critical when unable to maintain continuous information superiority to achieve it at decisive moments that provide the maximum benefits to friendly forces and disadvantage to the adversary.

The US withdrawal from Somalia in 1993 provides an example of a smaller, less-technical force achieving information superiority at a decisive moment against a larger force. Mohammed Farah Aidid, the dominant Somali warlord, led a ragtag guerrilla force against elite forces of the US Army in the streets of Mogadishu. According to the traditional rules of warfare, US General Garrison and his elite soldiers of Task Force Ranger won a tremendous victory against the Somali warlord. Aidid lost several of his top lieutenants in the raid and a large percentage of his supporters. Additionally, most of his ammunition stores were expended and his active fighting force was reduced by over 50% (Adams, 1998, p.71). [5]

Although General Garrison's superior forces tactically defeated the Somali gunmen in the streets of Mogadishu, Aideed trumped Garrison's success by exploiting the information environment. CNN's global transmission of jeering Somali citizens dragging corpses of US soldiers through the streets of

[4] FM3-0 defines information superiority as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".

[5] The toll of casualties read: 18 Americans and 1 Malaysian dead, 84 Americans and 7 Malaysians wounded; 312 Somalis dead and 814 wounded.

Mogadishu shocked the American populace and greatly influenced the decision of President Clinton to withdraw troops from Somalia. Adams quotes a senior military officer saying,

> By Saturday and Sunday we had won the war, but on Monday Aidid mounted a strategic attack in the information domain. The American people simply had not been briefed about this area of the battle space, and so when bodies started appearing on TV screens, Americans said, 'Wait a minute, nobody told us this was going to happen'- and Aidid won (p.72).

The psychological weight of the photos and video of dead US soldiers and the apparent inhumane treatment by the Somalis occurred at a time when most American people and the President were expecting to see US success in Mogadishu. Aideed succeeded in gaining information superiority by controlling the television images coming out of Mogadishu. CNN's images of the mutilated Army Rangers and the dead Somali civilians soured American TV viewers and became a major influence to pull US troops out of Somalia; "in essence, Aideed (sic) won the information war" (Libicki, 1995).

The growth of information technology (IT) and the global reach of real-time communications systems have made IO a potent instrument in swaying public opinion and influencing decisions. IT often amplifies the effectiveness of operations in the information environment, influencing audiences well beyond the field of battle. Yet, gaining information superiority (IS) is not necessarily determined by advanced technology or the lack thereof. IS is gained through skillful control of information at decisive points during or after the battle. The news broadcasts after the battle enabled Aidid to manipulate the American perception of what was really going on in Somalia. He was able to leverage this powerful influence in the information environment to finally gain victory in the physical environment.

B. INFORMATION OPERATIONS.

> Information operations (IO) are actions taken to affect adversary and influence others' decision-making processes, information, and information systems, while protecting one's own information and information systems (FM 3-0).

The United States first formally divulged the concept of Information Operations in 1996 as a component of Joint Vision 2010. Since then IO has evolved into a part of a strategy to achieve national objectives through non-kinetic means. "IO is an attempt by the US to develop a set of doctrinal approaches for its military and diplomatic forces to use and operationalize the power of information" (Armistead, 2002, p.11) IO is not a weapon; rather it is a process, a way of thinking about relationships. IO shapes the information environment by influencing peoples' perceptions and enables military or diplomatic operations in the physical environment. The US accomplishes this by synchronizing and de-conflicting the principle elements of IO (Armistead, 2002, p.6). This section first explores the elements of IO, providing the reader a fundamental understanding of the terms and military reference. Secondly, the section explores the offensive and defensive categories of IO. Offensive and defensive IO must be integrated to ensure the mission is successful: the adversary is defeated and friendly assets are protected (FM 3-13, p.1-13).

1. Elements of Information Operations.

As noted earlier in chapter 1, IO integrates several previously separate functions, forming a powerful synergy that enables the commander to shape the information environment. The US military publications provide a list of IO elements, supporting, and related activities (FM 3-13, p.1-14). For the purpose of this thesis we provide a description of the IO elements that are useful to the study. These separate elements are briefly described below:

a. Psychological Operations (PSYOP).

The US Military defines PSYOP as “operations that are planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behavior of foreign governments, organizations, groups, and individuals” (JP 3-53, p.v). PSYOP are conducted primarily to influence the adversary’s perception of the battle: to weaken his morale and break his will to fight. However, PSYOP are also used to disseminate information to the target audience to affect their behavior. Classical PSYOP techniques include the air dropping of propaganda leaflets and the use of loudspeakers to broadcast information in the target language.

b. Military Deception (MILDEC).

The US military defines Military deception as “those actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission” (JP3-58, p.v). Deception involves showing the adversary that which is false and hiding from him that which is real. The US employs physical and electronic means to provide this camouflage. Deploying inflatable tanks and artillery pieces as well as simulating radio traffic to fake the electronic signatures of old unit locations serve as realistic examples of deception techniques.

c. Operational Security (OPSEC).

The US military defines OPSEC as “the process of identifying critical information and subsequently analyzing friendly and enemy actions to detect security leaks, determining the acceptable level of vulnerability of critical systems, and directing actions to safeguard these systems” (JP3-54, p.v). OPSEC is often an integral part of deception (camouflage, concealment, and decoys) and can also contribute to PSYOP. Good OPSEC is essential to deny the adversary information concerning friendly operations. This is a critical aspect of gaining information superiority.

d. Public Affairs (PA).

The US military describes PA as operations designed to provide public information, command information, and community relations activities directed toward both the external and internal publics with interest in the DoD (JP3-61). PA provides truthful information to Americans and other friendly audiences, educating them with an accurate depiction of the situation. This is so that the public, Congress, and the news media may assess and understand the facts about the military and its operations (JP3-61).

e. Electronic Warfare (EW).

The US military defines EW as any military action involving the use of electro-magnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-51). The three major components of EW are electronic protect (EP), electronic support (ES), and electronic attack (EA). EP involves passive and active means to protect personnel and equipment from enemy EW. US forces use terrain masking, directional antennas, and other techniques to limit radio emissions. ES involves intercepting adversary electronic transmissions for further exploitation. US Forces use the intercepts to gather intelligence and also to locate or target the adversary's emitter. EA involves the use of directed energy to deny, disrupt, or degrade an adversary's use of the electromagnetic spectrum. US forces direct energy at an adversary emitter to jam voice and data communications and radar.

f. Physical Destruction.

The US military defines physical destruction as "the application of combat power to destroy or degrade adversary forces, sources of information, C2 systems, and installations" (FM 3-13, p.2-11). Not all physical destruction is part of IO. However, when direct and indirect fires from the ground, sea, and air forces are incorporated into the IO strategy to influence a specific objective, physical destruction becomes one of the strongest elements of IO. US Special Operations Forces are often used to carry out these operations.

g. Computer Network Operations (CNO).

The US military describes CNO as operations to exploit, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves and to safeguard against the same (JP 3-13 and FM 3-13). CNO is comprised of the Attack (CNA), Defense (CND), and Exploitation (CNE) of computers and networks. CNA and CNE operations are designed to penetrate adversary systems. Although the tools and techniques used to accomplish these operations are classified, the intent of the operations is to exploit and attack the adversary's information, computers, and networks. CNE is a form of cyber-reconnaissance, whereby computers are used to access an adversary's information remotely and gather intelligence. CNA is an offensive operation designed to attack an adversary's information, information systems, or networks with the intent to disrupt, deny, degrade, or destroy. CND operations are designed to protect and defend friendly information, computers and networks from attacks by the adversary. US network administrators incorporate strict access controls, authentication passwords, intrusion detection devises, and virus scanners to defend against adversary attacks.

h. Civil Military Operations (CMO).

The US military describes CMO as "activities that a commander takes to establish and maintain positive relations between their forces, the civil authorities, and the general population… where their forces are deployed in order to facilitate military operations and to consolidate and achieve objectives" (JP 3-57, p.vii). The relationship between the US forces and the host nation population always has an impact on how the local population receives the US presence in their country and often has influence on the population's acceptance or denial of US strategic goals.

i. Intelligence Support.

Although Intelligence is not officially an element of IO, intelligence support is vital to the success of the IO campaign. Intelligence provides critical information (who, what, where, and when) during the IO targeting process. Detailed intelligence is needed to provide IO planners information about the target audience's culture and society. Intelligence is also critical for the timing and as a means to measure the effectiveness of IO operations. Elements such as OPSEC, deception, and PSYOP require early implementation and maintenance in order to achieve the desired influence. Each operation requires specific target information to be effective. They also require intelligence feedback to ensure they are achieving the desired influence on the target.

2. Offensive and Defensive Information Operations.

US military doctrine dictates that IO should be pursued offensively as well as defensively. Oftentimes successful offensive IO is dependent upon the integration and synchronization of defensive IO elements (FM 3-13, p.57). "Offensive IO supports the decisive operation while defensive IO protects friendly force critical assets and center of gravity" (FM 3-13, p.2-3). Many of the principle elements and supporting activities are mutually supportive of each other. The success of military deception for example often depends upon OPSEC to ensure the plan remains secret not only from the adversary but also from friendly forces without a need to know. With references to US Army FM3-13, figure 2 illustrates the symbiotic and supporting relationship of offensive and defensive IO.

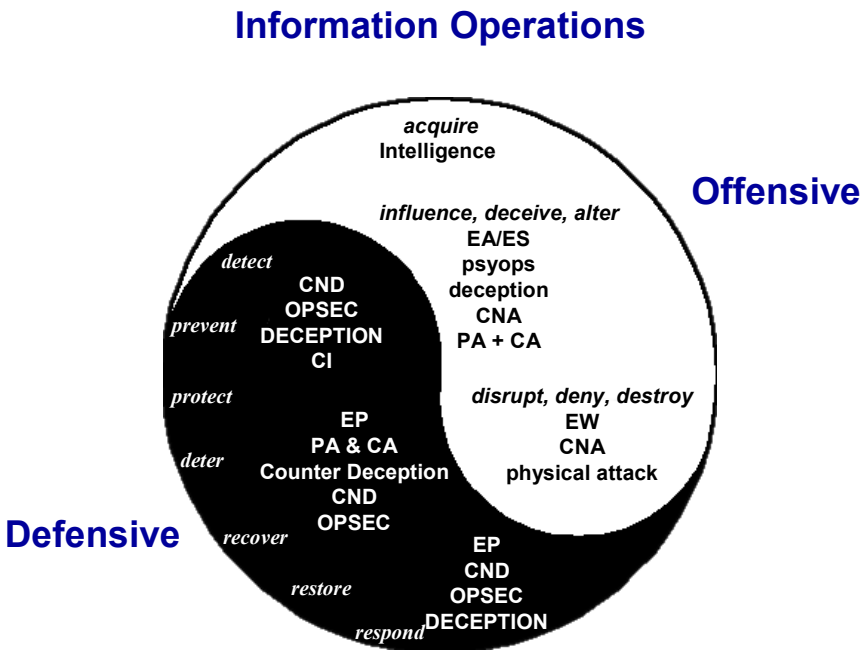

Figure 2. IO Offense-Defense Model

The Offensive-Defensive model reflects IO elements competing to gain dominance in the information environment. Offensively, IO seeks to acquire, influence, deceive, alter, disrupt, deny, and destroy the adversary's information and information processes. Defensively, IO attempts to detect, deter, prevent, protect, recover, restore, and respond to attacks by the adversary. Military commanders determine which elements of IO are needed to successfully accomplish the mission and ensure they are integrated and synchronized. Well planned and executed IO creates a synergistic influence that can effectively blind the adversary to the true intentions of the friendly forces and enable friendly forces to move and fight more decisively. Although integrating as many of the elements as possible provides maximum effect, all elements may not be required for each operation. The commander integrates select IO elements while taking into consideration the nature of the operation, the target, availability of resources and other factors that may support or hinder the operation.

a. Offensive Information Operations.

The US military describes offensive IO as “operations intended to destroy, degrade, disrupt, deny, deceive, exploit, and influence adversary decision makers and others who can affect the success of friendly operations. Offensive IO also targets the information and information systems used in the adversary decision making processes” (FM 3-13, p.1-16). Offensive IO can target multiple different audiences including: adversary decision makers, civilian populations, critical communications facilities, and other information systems. Broadly speaking, the goals of offensive information operations are to adversely influence the enemy’s sources of information on the battlefield. Through careful planning and implementation, offensive IO can provide the means to achieve information superiority in the information environment. Achieving information superiority has become increasingly important in conventional warfare and often is the determining factor in achieving final victory (Khalilzad & White, 1999, ch.7).

b. Defensive Information Operations.

The US military describes defensive IO as “the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes” (FM 3-0). Defensive IO is critical to the success of offensive IO and normal combat maneuver operations. Commanders must integrate defensive elements to protect and defend friendly assets and safeguard relevant information. The defensive goals are to deter, prevent, protect, detect, recover, restore, and respond against adversary attacks in the information environment. Activities such as counter deception, counter propaganda, and counterintelligence (CI) defend against adversary offensive IO. Protecting the information infrastructure and information in the physical environment is crucial to ensure that information is timely and accurate and information systems remain reliable.

During the 1991 Persian Gulf War, the US military successfully employed several elements of offensive and defensive IO to achieve victory against the Iraqi forces under Sadaam Hussein.

> Major emphasis was placed on Command and Control Warfare (C2W), CA, and PA activities during Operations Desert Shield and Desert Storm. Commanders integrated OPSEC, military deception, PSYOP, and EW efforts during Desert Shield to pave the way for successful combat operations. During planning for Desert Storm, the senior leadership recognized that Iraq's C2 was a critical vulnerability whose destruction could enable victory with minimal friendly loss (FM 100-6, p.3-1). DESERT STORM demonstrated the effectiveness of the integrated use of operational security (OPSEC) and deception to shape the beliefs of the adversary commander and achieve surprise. Deception and OPSEC efforts were combined to convince Saddam Hussein of a Coalition intent to conduct the main offensive using ground and amphibious attacks into central Kuwait, and to dismiss real indicators of the true Coalition intent to swing west of the Iraqi defenses in Kuwait and make the main attack into Iraq itself" (Joint Staff Special Technical Operations Division, quoted in JP 3-13.) During Desert Storm's air operations, the enemy was selectively blinded by EW and physical destruction to mask friendly force movements and operations. Deception operations continued to enforce erroneous enemy perceptions of the CINC's intentions. EW and precision air strikes against C2 targets were used to disorganize and isolate Iraqi forces… Fully aware that the enemy, as well as the public at home, was focused on PA coverage of the confrontation, the coalition used that coverage to confuse the enemy by encouraging speculation on the place, time, and size of the impending attack... After the cessation of hostilities, CA elements enhanced the restoration of Kuwaiti governmental and social order and responded promptly and effectively to one of the central unanticipated consequences of the war as Iraqi forces created an enormous refugee crisis in the northern Kurdish provinces of Iraq and in southern Turkey (FM 100-6, p.3-1).

C. THEORETICAL PERPECTIVE.

This section explores a theoretical perspective of IO by Edward Waltz, author of *Information Warfare: Principles and Operations*. Waltz provides a simple operational model of IO that this thesis has adapted to observe how terrorist employ IO. The model consists of three conceptual domains

(psychological or perceptual, information infrastructure, and physical), where IO activities can influence decision makers.

1. Role of Information.

Before introducing Waltz's operational model, however, it is important to explain the role of information in conflict at a fundamental level. Understanding the role information plays in conflict is important to further explore how IO activities exploit information to achieve an influence. Waltz proposes a simple two-character model to illustrate the role of information in conflict. The model can be applied to two opposing countries at war just as easy as it can be applied to two individuals. Waltz's model starts with an attack character, Adam, engaging a defending character, Dave. Dave must determine the best way to react to Adam's attack. Adam's objective is to influence or coerce Dave to respond in a way favorable to Adam. "This is the ultimate objective of any warring party- to cause the opponent to act in a desired manner: to surrender, to err or to fail" (Waltz, 1998, p.4). Adam may use physical force or any non-kinetic means available to achieve his objective. As a result Dave may exhaust his resources, deciding he can no longer go on, and surrender to Adam. Dave may also fall victim to Adam's deception and unwittingly make decisions in favor of Adam.

Waltz's *Role of Information Model* (Figure 3) provides a fundamental illustration of the power of information in conflict. Waltz suggests there are three factors that influence Dave's decisions to react to Adam's attack:

1. Dave's physical capacity to act. Based upon battle casualties and equipment readiness, Dave may not have the capacity to continue the fight.

2. Dave's will to act. Dave's will is a measure of his resolve, determination, and commitment to continue the fight. The will is the hardest element for the attacker to measure, because there is no template or tool available to estimate the will of an opponent. Confronted with certain defeat and death, some leaders will press on, without regard to consequence, while others will quickly give up in order to save their own skin.

3. Dave's perception of the situation. This is an abstract factor and is based upon Dave's understanding of information. "It is measured in terms such as accuracy, completeness, confidence or uncertainty, and timeliness" (Waltz, 1998, p.5). During conflict, Dave's decisions are determined by his perception of the situation, which can differ from the truth.

How then can Adam influence Dave to act in a manner favorable to his objectives? With the factors listed above, Waltz contends that Adam has several options available. He can directly attack Dave's capacity to act by attacking his combat assets in the physical domain. This will decrease Dave's physical ability to continue fighting, pressuring him to surrender. Secondly, Adam can attack the information domain, where Dave's intelligence sensors, command and control, and communications asset are located. This attack might blind Dave, obscuring the battlefield and increasing the 'Fog of War'. Thirdly, Adam can attack Dave's perceptual domain, where he analyzes and processes information to develop an understanding of the battlefield. The main target here is Dave's mind. Although Adam is likely to employ several non-kinetic means to shape Dave's perception, carefully timed and selected physical targets also shape Dave's understanding of the battlefield. Finally, Adam can attack Dave's will to fight: his morale and commitment. Figure 3 illustrates Waltz's model and the four options available for Adam to attack Dave.

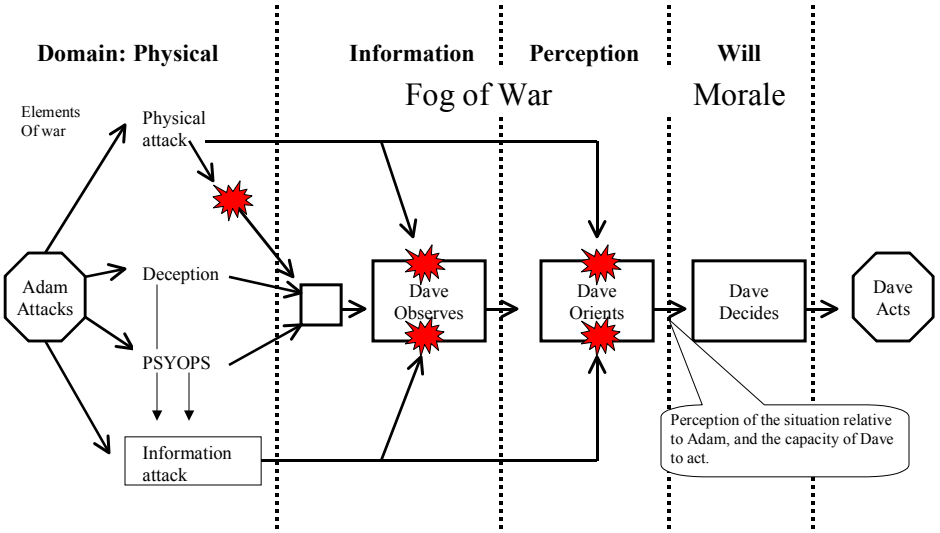

Figure 3. Role of Information Model by Edward Waltz, p.6

Notice in the figure above that Dave attacks Adam in the physical domain, destroying or denying Dave's physical capacity to fight (targets such as military weapon systems and personnel, equipment, roads, bridges, and other line of communication). Adam also physically attacks Dave in the information domain, destroying his ability to see and hear the battlefield. The attack inhibits Dave from observing Adam's movements and from commanding his own forces on the battlefield. "Physical attacks on observation (intelligence sensors, communications) or orientation processes (command nodes) deny valuable information" (p.6). Dave's understanding of the situation becomes increasingly obscured. Deception, OPSEC, and PSYOPS form Adam's information attack and strike Dave in the information and perception domains. The attacks corrupt Dave's perception of the situation, shaping his understanding of the conflict and making him vulnerable to poor decision making. EW and CNA target the electronic processes and content of the information infrastructure (sensors, communication links, and processing networks) that provide Dave the ability to see and hear the battlefield (observation and orientation). These attacks have

the ability to directly affect Dave's ability to receive information and can greatly impact Dave's ability to perceive the situation.

If Adam can successfully exploit the information available to Dave and influence Dave's ability to process the information, Adam can profoundly affect Dave's perception of the battlefield and possibly decrease his will to continue fighting. Additionally, Adam can conduct physical attacks against Dave with the intent of denying, destroying, or corrupting information available to Dave. It is important to note that physical destruction is an element of IO, when it is planned and synchronized to achieve an effect or intended influence on the adversary.

2. Operational Model of Information Operations.

Waltz suggests that the basic principle underlying the shaping of the Information Environment is influence. Operations in the Information Environment that influence the perceptions, beliefs, and opinions of a target audience can enable operations in the physical environment. Waltz contends that IO creates influence in three conceptual domains: perceptual or psychological, information infrastructure and the physical domain (Waltz, 1998, p.148). Influence operations shape the information environment by affecting the perception and battlefield clarity of adversary decision makers, policy makers, or even entire populations. Waltz suggests that the highest-level target in the IE is in the perceptual domain: the human mind. The second domain, the information infrastructure, processes, manages, and stores the information (Waltz, 1998, p.148). Humans are often dependent upon information infrastructure to transmit and receive information. Oftentimes infrastructure failure can attribute to poorly made decisions. The physical environment forms the third domain, where physical attacks or threats set up actions to influence the target in the information environment. Figure 4 illustrates Waltz's three conceptual domains. Waltz places the perceptual domain first to illustrate its priority in shaping the information environment. The decision maker's perception of the situation serves as the primary target in the Information Environment.

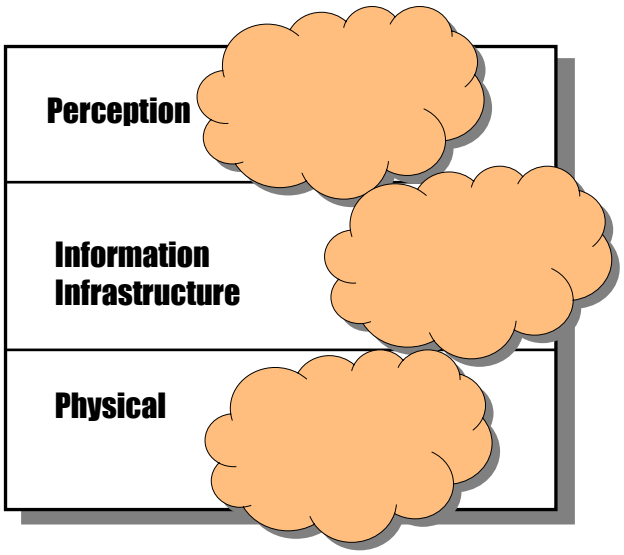

Figure 4. IO Conceptual Domain Waltz

A typical US Army Tactical Operations Center (TOC) serves as an example to illustrate the relationship of the three domains. The commanding officer serves as the chief decision maker for the unit. He is advised by a staff, which is responsible to continuously monitor the friendly and enemy situation. They analyze enemy intelligence and friendly capabilities and make recommendations to the commander, who makes the final decision to act. The staff maintains a current picture of the battle through a vast network of intelligence sensors, friendly units, and reconnaissance assets.

- The minds of the commander and his staff comprise the perceptual domain.
- The vast network of sensors and the staff's analysis processes form the information infrastructure domain.
- The TOC and the military assets operate in the physical domain.

D. IO FRAMEWORK.

This chapter examined US Military Doctrine, highlighting the basic principles that serve as the cornerstones to information operations. The primary goal of information operations is to gain superiority in the Information Environment at a decisive point in time to enable successful operations in the physical environment. Edward Waltz suggests that Information Operations shape the Information Environment by influencing people. He first provides a fundamental explanation of the role of information in conflict to establish a basic understanding of the power of information. Subsequently, Waltz presents an operational model of Information Operations, explaining how IO activities can generate influence in three different domains: the perceptual, information infrastructure, and the physical. Figure 5 illustrates the IO framework established by incorporating the principle elements of IO, prescribed by US military doctrine, with Waltz's operational model of IO.

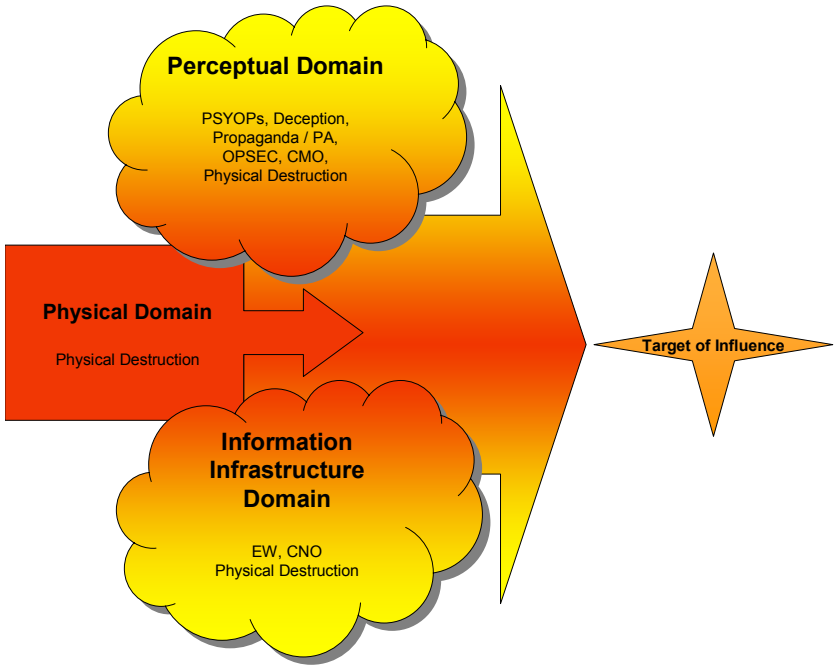

Figure 5. Information Operations Framework

US military doctrine prescribes six elements of IO that have the power of direct or secondary influence in the perceptual domain: Physical Destruction, Operations Security, Psychological Operations, Military Deception, Public Affairs / Propaganda, and Civil Military Operations (CMO). These operations target the gray matter of the human mind, influencing what the commander perceives and often forming biases or preconceptions that can profoundly effect his decisions. The elements that directly influence or occur in the information infrastructure are Physical Destruction, Electronic Warfare and Computer Network Operations. These operations are designed to affect or defend the electromagnetic spectrum, information systems, and the information that supports decision makers (FM 3-13, p.2-2). Physical destruction directly affects the physical domain and has the ability to influence the perceptual domain with its destruction. US IO focuses these influence operations in all three domains to shape the information environment and enable operations in the physical environment.

The thesis offers this fundamental perspective of Information Operations as a simple framework to apply to terrorist organizations. Terrorist organizations are different from US military units and approach the information environment under different conditions. Chapter III will apply the framework developed here to the asymmetries of terrorist organizations. This process will hopefully provide an approach to IO that is consistent with the terrorists' goals, motives, and operating environment.

III. TERRORISTS' APPROACH TO INFORMATION OPERATIONS

Terrorists' strategic use of physical violence as a tactic to influence multiple targets predates modern technology and mass media. The Assassins, a Middle Eastern group active in the tenth century A.D., "sought not only the death of their enemies but also the "surrounding publicity which could bring attention to their cause (Reich, 1998, p.264). The Zealots, as previously discussed, waged a campaign in 66-73 A.D against Roman occupation of what is now Israel with dramatic and very public murders. Their strategy was to use violence as a psychological weapon beyond the immediate victim and send a "message to a wider, watching target audience (Hoffman, 1998, p.88). Before 24 hour news channels, these groups relied on conducting violence in the presence of mass witnesses and the ensuing word of mouth to further their cause. This strategy shows perhaps that aspects of the modern concept of Information Operations are inherent to the tactics of terrorists' operations.

The goal of this chapter is to produce a general IO framework for terrorists that will be applied to specific terrorist organizations in subsequent chapters in order to determine how they employ elements of Information Operations. To accomplish this goal, the chapter builds upon the theoretical understanding of IO established in chapter II by exploring three factors that can have an impact on how terrorists employ IO. The first is that often terrorists employ elements of IO to overcome a legitimacy dilemma. The terrorist must remain covert to stay alive, yet must overtly gain legitimacy, e.g. leverage with the state actor and the populace. Secondly, the terrorists conduct acts of violence in the physical environment to directly influence an audience or to enable operations in the Information Environment. Thirdly, the terrorists take the physical acts and 'spin' an influential message, addressing multiple audiences. The chapter then revisits the elements of IO, exploring a terrorist's perspective of their meaning and using that perspective to evaluate if groups deliberately apply IO to their operations.

Finally, the chapter concludes by summarizing the terrorists' approach to IO and providing a graphic representation of the analytical framework.

By contrasting DoD methods against terrorist methods, this chapter develops a new perspective of IO that terrorists rely on to achieve their objectives. The chapter illustrates that terrorists must take a different approach to IO and that elements of IO are an integral part of a majority of terrorist operations. To ensure that the action in the physical environment achieves their desired influence in the Information Environment, the terrorists select their targets by applying an IO lens. This concept is further explained in this chapter.

A. ORGANIZATION OF TERRORIST GROUPS.

What does a Catholic, working class, PIRA volunteer from Falls Road in Belfast have in common with an Islamic Fundamentalist in the towering Hindukush of Afghanistan or a Marxist Revolutionary in the jungles of Colombia? Terrorist organizations differ greatly in their goals, means, and operating environment as will be described later in subsequent chapters. However, nearly all terrorist organizations share one common trait. They are illegal organs hunted by a higher authority and dependent upon secrecy for survival. This covert, illegal nature provides insight into why terrorist organizations may apply Information Operations in order to survive and further their objectives. Understanding the conditions that cause the deliberate or unplanned use of IO may enhance predictive analysis and further develop effective counter terrorism strategies.

1. Legitimacy Dilemma.

The covert and illegal nature of terrorist organizations creates an interesting dilemma for groups wishing to appear legitimate in the eyes of the state and to their 'would-be' supporters. Terrorists must sacrifice secrecy for efficiency in order to gain legitimacy as a viable threat, and the sacrifice increases the risk of failed missions and getting caught. While numerous terrorist experts have written about the nature of terrorist organizations, one historian, J.

Bowyer Bell, has made detailed studies of the nature of terrorist, guerrilla, and insurgent organizations for a quarter of a century. Bell's analysis highlights an important dilemma most terrorist organizations face: they must appear to be legitimate organizations in order to gain leverage with the state and to appear attractive to sympathizers and supporters, yet they must remain a low enough threat as well as secret and hidden from the state in order to stay alive. J.B. Bell has coined this 'covert-illegal' commonalty shared by all terrorist organizations as the Dragonworld. Bell describes the Dragonworld as a 'dream for dramatic change'. He claims "terrorists live in a world that is not structured by traditional values or by personal consideration, but rather by an ideal that cannot be achieved except by recourse to violence" (1999, p.81). Terrorists freely employ abhorrent tactics, ignoring rules established in the Geneva Convention, conventional laws of warfare, and even fundamental human rights. This lawless nature of terrorism is supported by their own code of ethics, which is not consistent with accepted codes of ethics. As a consequence of violating domestic or international laws, they are hunted, and so must pay considerable attention to maintaining their security, not only so their operations will be successful, but also so they will not get caught.

As a group moves forward in its lifecycle it is faced with sacrificing secrecy for efficiency of operations in order to stay viable (McCormick lecture, 2002). "As a general rule, the greater the secrecy, the greater the inefficiency of the organization or operation; absolute secrecy assures absolute chaos" (Bell, 1990, p.203). The Shining Path spent ten years building an underground secure and clandestine organization, but sacrificed some of its operation secrecy when it launched its campaign of violence in 1980 (Crenshaw, 1998, p.17). Groups at this point need a synergy of action to minimize their risk or make it worthwhile. Terrorist organizations seek change: political, religious, or ideological; however, they often lack public support and are too weak to legitimately fight for their cause. They must emerge from this underground, described by Bell, to appeal to the populace and gain support; yet must avoid being caught by the state counter-

terrorist forces. Bell states, “It is impossible to overstress the penalties paid by those on the run: to survive, appear normal, and still operate" (1998, p.81).

This section explores the terrorists’ use of IO by examining both components of the dilemma. First, how they employ elements of IO to remain secret and covert and then how they are able to emerge from Bell’s Dragonworld to gain respect and legitimacy from the state and supporters.

a. Employ IO to Stay Alive.

The first and most vital aspect of the dilemma terrorists must overcome is their vulnerability to the states’ counter-terrorist forces. The PIRA employs several key elements of IO in order to remain covert and unseen by the British intelligence forces. Active PIRA members skillfully integrate deception and a strict ‘street sense’ of operational security into their operations. Members blend into the populace, making it extremely difficult for British forces to distinguish active members from normal Irish citizens. Eamon Collins, a former PIRA intelligence operative, notes “IRA volunteers operating in rural areas, wanting to blend in with the hedges, fields, and trees, could wear camouflage jackets, but that’s not the gear for towns and villages. You have to blend in with the local population: you look like a mechanic, or a postman, or a bank clerk, not Fidel Castro” (Gerwehr & Glenn, 2000, p.41). PIRA members never keep written orders, addresses, or target information on their body. Written and telephone communications are strictly controlled and normally encoded. Logistics and direct action operations are separate. Often the operative moves to the target area without a weapon or bomb, only to recover it from a hide site or another member posing as a street vendor near the target. The PIRA organizational structure also provides protection against detection. The PIRA operated under the historical Irish Army structure complete with traditional army hierarchy and military titles for its members until the late 1970s. However, this organization efficiency undermined their OPSEC, enabling British intelligence to easily template and infiltrates their organization. Members of the Provisional IRA cited

this weakness as the one of the main reasons behind the 1977 reorganization. Wright quotes members stating:

> The old system came close to identifying those responsible for different operations, for if a car was hijacked in Turf Lodge, and used in a bombing expedition or such the like, the British knew that the unit which carried out the operation was based at Turf Lodge. Then all they would have to do is arrest all the known suspects in that area, torture them, and eventually they would get one confession, implicating the others involved (Wright, 1990, p.154).

The PIRA evolved into a cellular organization to better protect information and improve operation security. By the end of 1978 British intelligence was admitting: "we know little of the detailed workings of the hierarchy in Dublin. In particular, we have scant knowledge of how the logistical system works, nor do we know the extent to which the older, apparently retired, republican leaders influence the movement" (Wright, 1990, p.154). The cellular structure compartments the active units from the command structure and support personnel. This makes British infiltration into the cells nearly impossible and also limits the extent of damage when a cell becomes compromised.

Al-Qa'ida, serving as an umbrella organization for many Islamic Fundamental terrorist groups[6], is a very unique organization (Alexander & Swetnam, 2001, p.5). Yet, arguably, Usama Bin Laden relies on the same elements of IO as the PIRA to remain covert and survive. The cornerstone of bin Laden's strategy to 'stay alive' had been the impenetrable sanctuary from which he operated. His headquarters and training camps were located high in the Hindukush Mountains in Khuasan, Afghanistan, extremely forbidding terrain that isolates him from counter-terrorist units. This created a permissive environment that allowed al Qa'ida to sacrifice some operation secrecy for improved operating frequency, with minimum risk. Bin Laden incorporated the vast cave and tunnel networks, built during the 1970s to defeat the Soviets, into his strategy to provide secrecy and security for his operations. His 1996 declaration of war states "By the grace of Allah, a safe base is now available in the Hindukush Mountains;

[6] Groups include al-Jihad, Abu Sayyff, Islamic Jihad, Hamas, Hizzbollah, and Mujahadeen.

where the largest infidel military force in the world was destroyed" (Robbins, 2003, p.358). Additionally, bin Laden benefited greatly from the Afghanistan Taliban government providing him safe haven. Prior to September 11th, 2001, there were no direct threats to his headquarters and training base. This permissiveness allowed terrorists to easily blend into the Afghan civilian population.

b. IO as a Force Multiplier.

To overcome the legitimacy dilemma, White contends that terrorists must somehow appear to be more capable than they actually are in order to gain respect and legitimacy from the government and the populace. Brian Jenkins states "all political terrorists want to give the illusion that they can fight on another level" and they use force multipliers to support that illusion (White, p.16). Force multipliers allow a terrorist organization to increase its' striking power without increasing its size (White, 2002, p.16). Jenkins suggests they employ four force multipliers routinely to accomplish this illusion and add to their aura: technology, transnational support, media, and religion (p.17). The force multipliers are not weapons per se, rather they constitute a process of information exploitation intended to influence decision makers and shape public opinion (Armistead, 2002, p.6). Jenkins' force multiplier concept is too incomplete to fulfill the needs of our thesis as a terrorist IO typology. However, the inclusion of technology and media makes the concept adaptable and his theory describing the terrorists' need to appear legitimate very useful. Jenkins' theory is primarily based upon the target audience's perception of the terrorist organization. Since most terrorists are too weak to directly confront the state in the physical environment, they seek to achieve their objective of 'legitimacy' in the information environment. They often employ elements of IO as a 'force multiplier' to accomplish this. Two of the force multipliers categorized by Jenkins, technology and the media, facilitate the terrorists' use of Information Operations. Hoffman contends that the merging of these two force multipliers, coined as the 'information revolution', has created opportunities for terrorists to manipulate the media and influence multiple

audiences. Advanced technology has made the world more transparent, creating a global 'fishbowl', where even local events can have international influences. Clearly the real-time footage of 9/11 transmitted instantly around the world had profound impacts not only on all Americans, but on the international community as well (Hoffman, 1998, p.153).

Militarily speaking, IO serves as a force multiplier in support of physical operations much like artillery serves as a force multiplier supporting infantry or armor units. The supporting role of Information Operations is a key element in US doctrine. This concept is also relevant to the terrorists' use of IO. Since most terrorist organizations cannot or choose not to combat states militarily, they must rely on force multipliers that "allow a small group of individuals to operate as if they were a larger group" (White, 2002, p.16). White suggests that force multipliers are exceptions to the following rule of thumb: "The larger the group, the larger the level of activity" (p. 17). Terrorists use force multipliers, including Information Operations, to increase their striking power and influence, without increasing their size. This is integral to a group's survival and ability to achieve its goals.

2. Physical Environment Enables Terrorist IO.

As previously indicated, terrorists have demonstrated as early as 67 A.D a strategy of using violence to spread their message in the information environment to help achieve objectives. Technology such as computers and mass media helps promote success beyond a smaller audience, which is why they are force multipliers. As noted in Chapter II, conventional US military doctrine and theory proposes that Information Operations are intended to supplement and enable successful combat operations in the physical environment. The US targets information assets in all three of Waltz's domains: adversary decision makers and the populace in the perceptual domain, networks and processes in the information infrastructure domain, and physical information activities in the physical domain. During the recent war in Afghanistan, the US successfully targeted the world's Muslim population with an IO campaign to

isolate the al Qa'ida terrorists and Taliban supporters. US diplomats influenced leaders of other nations to cut off support to al Qa'ida and promoted Muslim solidarity alongside the United States against an enemy of Islam. The US also made it perfectly clear that the US would not tolerate states harboring terrorists. This IO campaign effectively cut off bin Laden and the Taliban leadership from any significant outside support and enabled the US to physically invade Afghanistan with little opposition and resistance. Thus, the IO campaign served as a supporting activity, shaping the Information Environment and enabling successful operations in the physical environment.

The US military achieves victories in the physical environment by waging battles in the physical environment, using the Information Environment to help support our objectives and reduce costs of war. Terrorists act in the physical environment not to make tactical gains in the physical environment, but to wage strategic battle in the information environment; therefore the PE enables many of the activities in the IE to occur. Terrorists exploit the IE to reduce the necessary actions in the PE, because a group cannot face a state in the PE. A battle in the PE is a war of attrition a terrorist group will surely lose. If Hamas or Popular Front for the Liberation of Palestine (PFLP) detonates a bomb at a crowded café in Haifa or at an Israeli checkpoint in the West Bank, their intent is not to kill Israelis for tactical gains, but rather to support strategic objectives. Terrorists are not attempting to make tactical gains or influences by killing civilians or shutting down checkpoints, but often to speak to a wider audience. The act can demonstrate ongoing group activity to its members (the Hamas website chronologically lists all hostile actions by group members or supporters) or perpetuate a psychology of terror to citizens, its government, and a state's allies or supporters. A terrorist organization cannot capitalize or reinforce on tactical gains in the PE, since resources are limited and attacks are generally too isolated to have an effect on a state. The attacks on the US on September 11th were extremely devastating, the most catastrophic terrorist attack in our nation's history. However, al Qa'ida did not or could not quickly follow through with similar or even smaller attacks on US interests in the PE. While sometimes a

group's physical attack may serve merely as only a tactical purpose, such as a retribution killing or destruction of a key C2 node, it often has the dual or primary purpose of having a strategic impact, and targets are chosen because they have strategic impact-terrorists view targets through an inherent IO lens.

Michael Radu suggests that although US Information Operations may often impact the adversary's perception or will to fight, normally, we rely on victory in the physical environment to win the battle (ed. Radvanyi, p.121). This is primarily true because we seldom lack the combat power necessary to overwhelm the adversary's forces. By contrast terrorist organizations can never hope to achieve a sustained victory against a state by attacks in the physical environment alone. Employing weapons of mass destruction (WMD) such as biological and nuclear weapons still cannot give a group a sustained victory. Cities and states can recover from such attacks, and it is highly unlikely a group has the resources to execute several WMDs. Therefore, even with WMD, terrorists cannot play in the state's arena. Groups often rely on attacks in the physical environment as the supporting activity[7] to enable their operations in the information environment. Michael Radu suggests that terrorist organizations use military operations to supplement their political war. Political war, he claims is "ultimately propaganda … a coherent, consistent, and conscious attempt to manipulate facts, images, perception, and emotions" (p.122).

McCormick's Influence Process Model (explained in chapter I) supports this assertion. He suggests that terrorists need either a physical act or direct communication with the media in order to get second and third order effects in the information environment, which influences one or more target audiences. Without the first, second and third order effects, terrorists are not afforded the opportunity to influence anyone beyond the immediate attack victims. This reinforces that IO is the supported activity (vice supporting activity for conventional forces) for terrorists, that the physical act enables the activities in the information environment, that actions in the physical domain are minimized

[7] supported activity is main effort; supporting activity supports main effort

but maximized in the information infrastructure and perceptual domains. This conclusion produces a hypothesis that terrorist and conventional forces at war have an inverse relationship in these domains, as depicted in Figure 6. This helps visualize the difference of application of IO by each force. The figure uses the Waltz IO conceptual domains to demonstrate the inverse approach the terrorists take toward the employment of Information Operations compared to the US military.

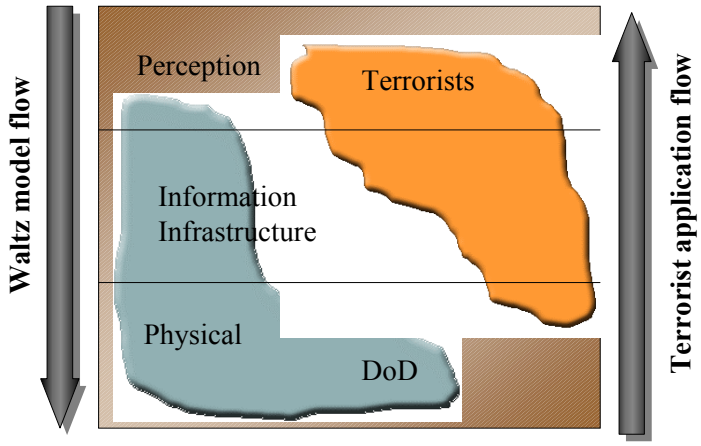

Figure 6. Activity within IO Conceptual Domains

The figure also graphically portrays the larger presence by DoD in the physical domain and inversely the larger reliance by terrorist in the perception domain. This understanding is important when comparing terrorist group activity to that of a conventional military. The terrorists' approach and application of IO are different because they have a different approach to their operations. It could be said that DoD set the conditions with IO before the physical attack while terrorists set conditions in the physical domain before their information attack. However a group that has greater parity with a state will likely have less reliance on IO (Buettner, email, 2003). For example, the FARC has more military parity with its opposing state than Hamas or IRA with theirs, and conducts proportionately different acts in the physical domain instead of perception

domain. The disparity is perhaps another factor requiring terrorist groups to have a heavy reliance on IO to achieve their objectives.

3. Terrorist IO Target Audiences.

> Terrorism is aimed at the people watching, not the actual victims. Terrorism is theater. (Jenkins, as cited in Nacos,1994, p. 75)

Joanne Wright (1990), author of "Terrorist Propaganda," suggests that terrorist operations, including physical destruction, has specific targets and messages, which are adjusted or emphasized according to the target selected or the particular tactic being used. Terrorist Information Operations essentially are about transmitting a message. A message must have a sender and a receiver, but not just any receiver. The audiences are a critical component of operations; terrorists understand what an audience likely needs to hear in order to be influenced and selects targets and subsequent actions accordingly. For example, the ETA (Spain) would target not just the local populace but the international audience as well in order to ensure continued support and sympathy. Each target plays a role in their quest to accomplish their strategic objectives. She claims that terrorists often target three separate audiences in their publicity efforts. She contends the three influential audiences are comprised of people who are *uncommitted*, *sympathetic*, or *active* in the terrorist organization. For the purpose of this thesis we have added a fourth audience comprised of those people who are *opposed* to the terrorists. Wright describes the uncommitted audience as having two components: the general public of the country where the terrorists are operating and the international public. Neither audience knows much about the terrorist group or its cause. Generally, the audience maintains a neutral perspective, often viewing the terrorists as political activists, yet they remain vulnerable to terrorist propaganda and being coaxed into becoming sympathetic toward the terrorists. Wright describes the sympathetic audience as those people who already have a broad historical or ideological sympathy with the terrorists and are familiar with their political aims. This audience keeps the political debate on the terrorists' aims rather than on the violence. On a practical level, they

provide food, money, or shelter to the active members; they also provide the majority of recruits into the organization. The sympathizers can also have a limited active role of aiding secrecy by not providing or divulging information to the state on terrorist activity and their whereabouts. The active audience is made up of those people who are self-confessed members of the terrorist organization, including those in prison. The active audience is often the target of the terrorist groups' internal propaganda, also known as auto-propaganda. The fourth audience, comprised of those people who directly oppose the group, includes the state's government, rival paramilitary groups, and anti-terrorist units. This audience actively seeks to discover, discredit, and destroy the terrorist group. Figure 7 illustrates the four audiences described above by Wright. The chapter further develops this framework by examining how terrorists select potential targets through an IO lens in order to specifically influence a target audience.

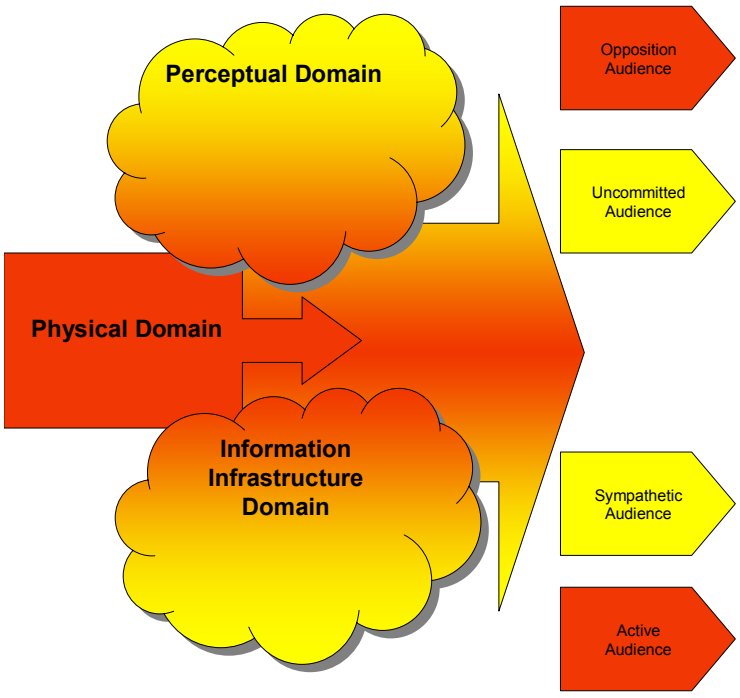

Figure 7. Audiences

A terrorist groups' understanding of their audiences lends credence to the theory that groups inherently view targets and operations through an IO lens. This might explain why groups involve their IO related actions from the beginning as opposed to the DoD practice of adding IO to their operations. Essentially, they

do not have to ask themselves "what can we do to get an edge in the perception domain," because it is an inherent part of operations conception and planning (the main difference between sub-state and conventional forces planning). Figure 8 illustrates the process, where a group determines its strategic objectives and selects its targets to support the objectives. The targets are viewed through the IO lens so planned operations incorporate minimum physical domain presence and maximum perceptual domain influence. The resulting impact on the target audiences reinforces the strategic objectives, and the cycle continues until a group succeeds or ceases operations.

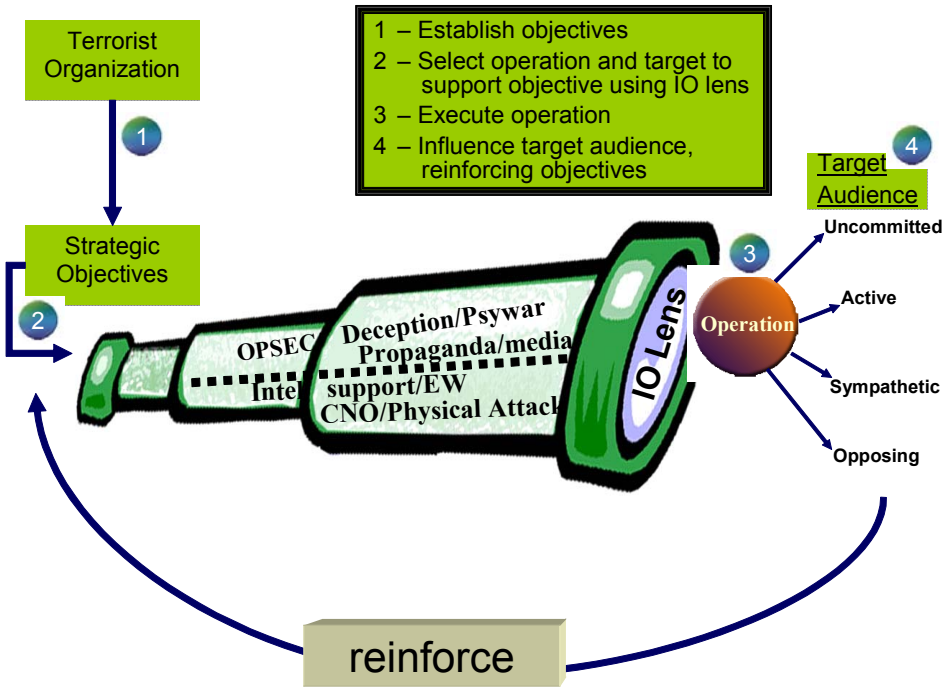

Figure 8. Terrorist IO Target Lens

Usama bin Laden's unprecedented attack against the United States on September 11th, 2001 is a recent example of a single attack meant to convey messages to multiple audiences. The targets were selected not only to influence the Bush Administration and US government (opposing audience) and most of the American citizens (uncommitted audience), but also international audiences (Buettner[8] lecture, 2001). The message was that the most powerful nation could

[8] LCDR (ret) Ray Buettner, Associate Professor of Information Sciences, Naval Postgraduate School.

not protect its citizens (Nacos, 1994, p. 60). The lethalness and willingness of the attacks sent a message to other audiences such as Israel (opposing), Saudi Arabia and other moderate Arab states (uncommitted). The attacks appealed to sympathetic audiences in Iraq, Lebanon, and other anti-US states to join al-Qa'ida's cause. Bin Laden conveyed a message to the Muslim population worldwide for different reasons. The attacks also signaled commitment to current and potential members in the active audience, as well as financial, political and logistical backers in the sympathetic audience. The al Qa'ida attacks in May 2003, were likely designed to reach multiple audiences, by showing the opposing audiences the organization is still functional and able to operate as a network (the near simultaneous attacks in several countries). The attacks demonstrated to the active and sympathetic audiences that the group is operating, to continue support, to join the cause, or to continue with assigned missions.

Many terrorist groups are able to influence more than one target audience from a single attack in the physical environment by applying a slightly different 'spin' to the story. The propagandist can only achieve this by understanding their audiences. The Internet and other advanced technology allow numerous terrorist organizations to transmit their messages directly to audiences worldwide in several different languages. The Hamas Website (www.palestine-info.info/), for example, is a portal site in six languages: English, Russian, Indonesian, Arabic, Persian, and Urdu. Each site is hosted on a server in a different country and targets a different audience. Although the sites usually have similar headline stories, they often vary in perspective, structure and content. This is evident even without translation, through the use and placement of photos. Hizzbollah in 1998 operated three separate "web sites: one for the press office (www.hizbollah.org), another to describe its attacks on Israeli targets (www.moqawama.org), and the third for news and information (www.almanar.com.lb) "(Denning, 2001, p. 69).

B. A TERRORIST'S APPROACH TO IO.

> Information warfare, as a separate technique of waging war, does not exist. (Libicki, 2001, Preface).

Martin Libicki's[9] statement likely was meant to apply to conventional militaries; it is true even more so with terrorists. The terrorist use of the various elements is significant and an inherent component of almost all terrorist operations. Terrorists could not cease their application of IO and succeed in achieving their objectives. Terrorism is a form of unconventional warfare and often in unconventional conflicts; the strategic objectives cannot be reached through victories in conventional military battles. The victory must be achieved through indirect methods. Maurice Tugwell argues that as a consequence, the campaign becomes one of leverage where the objective is to move the 'asset' (a policy, a territory, the right to govern, and so on) into a liability that the state sees it as no longer worth fighting for. Tugwell suggests that propaganda is key to achieving this objective. This, he says "brings the propagandists onto the central and dominating feature of the battle space landscape" (Tugwell, 1992, p.75). In this battle of the weak against the strong, the prime targets for the terrorists are not the physical assets of the state for these are its strengths. Rather, the terrorists target intangible assets: the state's legitimacy and the will of its population and security forces (Wright, 1990, p.10). The violent physical act of terrorism is only the most recognizable form of propaganda. Bruce Hoffman suggests "terrorism is specifically designed to have far-reaching psychological effects beyond the immediate victims or the objects of the terrorist attack" (Hoffman, 1998, p.43). Through the publicity generated by their violence, terrorists seek to obtain leverage, influence, and power they otherwise lack in order to effect political change on either a local or international level (p.44).

One of the enduring axioms of terrorism is that it is designed to generate publicity and attract attention to the terrorists and their cause (Hoffman, 1998, p.154). We have established in this chapter that by design or necessity terrorists

---

[9] Maritn Libicki, Senior Fellow, Institute for National Strategic Studies, speciales in application of information technology to national security.

are forced to use the information environment to wage their battles and win their wars. Information is a valuable currency. Terrorist have evolved into the ultimate IO warriors, yet are likely unaware the concept even exists. Since terrorists rely so heavily upon success in the information environment to achieve their objectives, it would seem logical that they have developed a keen understanding of how to best leverage the information. Groups understand the synergistic value of applying the elements of what the DoD calls Information Operations to accomplish their objectives either out of necessity or due to deft strategic planning. While the US military relies upon doctrine and military publications to explain how to incorporate and employ elements of IO, terrorists seem to operate under an inherent yet unwritten IO strategy. Out of necessity they integrate the different elements of IO. Generally, terrorist groups have developed their own 'IO toolkit' based upon actions that have worked for their predecessors or other terrorist groups. The IRA has a long history of deceit, ambush, and propaganda from which to draw experience. Al Qa'ida's al-Jihad manual provides scenario driven guidance and direction to active members, such as actions taken prior to a bombing to gain the most attention, and how to maintain secrecy during an operation (see "OPSEC" section in this chapter).

An example of a coordinated terrorist IO campaign occurred in Latin America in the 1960's. Carlos Marighella, a Brazilian revolutionary terrorist, published practical guides[10] for terrorism (White, 2002, p.114). Marighella espoused a two phase strategy of causing violence and then giving the violence meaning. Violence was good for causing panic among the ruling class by selecting targets of symbolic value that appealed to multiple audiences. The entire "terror campaign was accompanied by a psychological offensive to provide peripheral support for terrorists," essentially a coordinated IO campaign (White, 2002, p.115). Manighella's method for organizing a terror campaign could be viewed as the first formal IO doctrine, and has been used over the past 40 years by different political groups from the Japanese Red Army to the Freeman of Montana (White, 2002, p.114). Terrorists cannot confront states in the physical

[10] For the Liberation of Brazil and The Minimanual of the Urban Guerilla

environment. Since a majority of a terrorist organization's activity is in the perception domain, a terrorist's approach to IO is similarly altered. The DoD uses IO to support actions in the physical environment, and the doctrine and approach supports that. Terrorists wage their battles in a different medium than the DoD, so it is logical their approach and application of the IO tools would be different. These differences also make a 'side by side' analysis difficult, if not misleading. We first must gain an understanding of what generally comprises terrorist Information Operations in relation to our established doctrine. To do so, it is also necessary to operationalize the conventional elements of IO in terms that make sense to terrorists. Elements such as EW and computer network operations are difficult to analyze, if done in accordance with DoD doctrine. Much of the doctrine is written in order to exploit our advanced technology and equipment. Terrorists simply cannot or do not need to employ the same expensive and resource intensive equipment that we do. The following paragraphs revisits IO elements and Waltz's conceptual domain explained in Chapter II; however, we redefine the elements of IO to relate to terrorist activity. This redefining of terms will help to identify how terrorist use IO.

1. Elements of IO.

DoD uses offensive IO to support a physical battle though use of PYSOP leaflets, use of deception, OPSEC and EW. Terrorist use offensive IO principally to influence a variety of people, including potential supporters and use physical acts of violence to enable their IO messages (Denning email, 2003,). Terrorists use defensive IO to stay alive by maintaining secrecy and subverting collection and detection by the state.

a. Psychological Operations (PSYOP).

Terrorists' use of PSYOP is generally labeled as psychological warfare. Psywar is generally accomplished through propaganda and the actual acts of terror, and is essential for recruitment and influencing populations and governments. Terrorists manipulate facts, images, perception, and emotions to

gain a political edge and legitimacy. The violent act itself is a form of psychological warfare (Hoffman, 2001). Bruce Hoffman states, "terrorism may be seen as a violent act that is conceived specifically to attract attention and then, through the publicity it generates, to communicate a message" (Hoffman, 1998, p.131.) Generally, all acts of propaganda fall under psywar. Different types of propaganda include auto-propaganda (acts aimed internally) and most media-related releases and products. Many groups such as the PIRA and Hamas use leaflets or handbills as a means of communicating messages to the local population. The United National Leadership of the Uprising used leaflets to coordinate non-violent civil disobedience acts in Israel and even to counter dissenting messages of other Palestinian groups (Robinson, 1997, p.158). al Qa'ida distributed professionally made CD-ROMs throughout Muslim countries as part of their recruiting process (see Chapter VI). Auto propaganda is used to instill or reinforce ideas into a group's followers. Perhaps the best example of auto propaganda by al Qa'ida is selling the concept of virgins and a rewarding afterlife as a means to enlist martyrs and keep the thousands of followers involved in a protracted struggle (Hoffman, 2001, p.10).

b. Deception.

Terrorist use of deception parallels DoD's use. Deception is used to delay or prevent discovery of true attacks (critical when acts in the physical environment are executed at the minimum) or a group's operations in general. Preventing discovery of groups' activities and its members is key to survival. In May 2001, bin Laden deceived U. S. technical collection systems by allowing a major attack plan to be monitored (Walcott & Strobel, 2001). The U.S. believed two major attacks were going to occur against American targets on the Arabian Peninsula. We reacted with increased security and travel advisories, which appeared to have thwarted or dissuaded bin Laden from carrying out the attacks. al Qa'ida controlled the information we received, provided a credible course of action, and affected our decision makers. Al Qa'ida caused the US to believe it had stopped the major attacks, while it was merely a deception to conceal the

real target on September 11th (Walcot & Strobel, 2001). The group also likely evaluated our reaction in order to exploit further weaknesses or modify tactics as part of the September 2001 attacks. Hijackers and suicide bombers employ tactical deception by concealing their missions and attacks. One al Qa'ida technique to defeat surveillance is the use of code words (see Chapter VI).

c. Operations Security (OPSEC).

OPSEC can be defined as secrecy for terrorists and is a key weapon in their campaigns. DoD is proficiency based and OPSEC is generally a tertiary priority behind intelligence and friendly unit requirements. Terrorist groups are secrecy based making secrecy one of the more critical elements for terrorists' success and survival. J. Bowyer Bell detailed in his book *Dragonworld* how secrecy is the fabric that envelops the covert world of terrorists. Secrecy is a necessary and priority element of all covert organizations, and is sometimes degraded as groups grow in size or undertake large operations (McCormick lecture, 2002). Al Qa'ida produced a document called the Jihad Manual that (Hoffman, 2002) had explicit, "micro managing" instructions on operational security. The manual demonstrates the organization's understanding and commitment to maintaining secrecy; secrecy of operations is tantamount to success of physical environment actions, the precursor to the intended influence effects.

d. Public Affairs (PA).

Media is the Public Affairs equivalent in the context of terrorist operations and is a critical IO element. There would be little value if an embassy bombing did not receive media coverage (Nacos, 1994, p 48-49). The media images of planes crashing into the Twin Towers reached around the world within an hour of the event. The media also transmitted images of Palestinians and radical Muslim students in Pakistan rejoicing upon seeing or hearing of the news, an example of media's effectiveness. DoD focuses on disseminating the truth externally and internally to help audiences understand its strategy; terrorists want

to use media for their propaganda, even though it may focus on violence (White, 2002, p.258). Although news reports rarely report a group's goals or objectives, often any audience is better than none. Terrorists do not just want attention, but the exploitation of news, which implies strategy and timing. Carlos the Jackal in 1975 waited patiently for the television camera crews to arrive before making his dramatic and televised escape (Hoffman, 1998, p.142). Media acts are designed to achieve the desired effect of presenting information that leads to confidence in the terrorists' group and their ability to conduct operations (one audience), to convey a message (accuracy not relevant) about a group's past, current or future activities or intent (various audiences). The media is also a conduit for groups to learn from other groups' successes and failures (Crenshaw, 1998, p.11). The media can give a group legitimacy and standing (Nacos, 1994, p.66), because without media, some groups such as the PLO would not exist (White, 2002, p.258). Terrorists must use the media to spread their terror to larger audiences and gain the maximum potential leverage that they need to effect fundamental political change. "Terrorism is theater," Brian Jenkins declared in his 1974 seminal paper, explaining how, "terrorist attacks are carefully choreographed to attract the attention of the electronic media and the international press" (Hoffman, 1998, p.132). Even when an operation fails, groups can still be winners if they draw media attention. This was evident in the years following the 1972 Olympics hostage crisis failure, when thousands joined Palestinian groups in 1974 and Arafat was allowed to address the UN General Assembly in 1975 (Hoffman, 1998, p.73). Terrorist will sometimes deliver their message directly to the media to better control their message (see Influence Process Model, Chapter I). Examples include 1986 interviews with Abul Abbas of the PLO and Abu Nidal (Nacos, 1998, p.62) and al Qa'ida sending audio and video messages to al-Jazeera (Fingel, 2003). Usama Bin Laden issued a Declaration of War in 1996 through al-Qa'ida that was a rally call for his organization against Christians and Jews. Media outlets such as CNN and major US newspapers gave the declaration international attention with significant coverage of the document's bold wording against the United States. Hizzbollah has guaranteed dissemination

of its message by owing and operating a radio station and newspaper in Lebanon (Kramer, 1998, p.131). Many groups such as al Qa'ida (see Chapter VI), Hizzbollah, Hamas, Zapatistas, and Tamil Tigers operate web sites as a viable media outlet. In 1998, 12 of the 30 groups on the State Department's list of terrorist organizations had a web presence (Denning, 1999, p. 68).

e. Electronic Warfare (EW).

For practical and costs reason, terrorists rely on off the shelf technology such as ham radios, scanners, jammers, and IR technology (Denning lecture, February 2003). There are examples of groups subverting state EW systems and using electromagnetic spectrum weapons. The FARC used single-sided band radio equipment to government communications during a 1998 offensive (Denning lecture, Feb. 19, 2003). Remote detonated bombs have been used against US troops in Somalia and Afghanistan ("Bomb Explodes," 2003). The PIRA used remote detonated bombs in the 1970's to reduce accidental deaths. The tactic proved so effective Britain was forced to develop electronic countermeasures (Hoffman, 1998, p.180). PIRA demonstrated their adaptability by progressing from radio frequency to radar to microchip in order to counter the countermeasures (see also Chapter V). Remote technology was used in an assassination attempt on Prime Minister Thatcher in 1984 and Prime Minister Major in 1991 (p.180). Chapter V further explores the PIRA's use of EW in their operations. Aidid subverted US EW in Somalia by having knowledge of our systems and using low tech means such as drum codes and runners to degrade collection (Arquilla, & Ronfeldt, 2001, p.11). Al Qa'ida used similar electronic protect measures in summer of 2001 to mislead US electronic collectors about the group's operations. Bin Laden used low-tech means such as couriers to communicate and conduct financial transactions (Walcott & Strobel, 2001). Finally, the Japanese group Middle Core Faction in 1985 used EW in support of operations when they cut strategic power and communication cables supporting computer controls, and jammed police and rescue frequencies to delay response by authorities (Denning, 1999, p. 180).

f. Physical Destruction.

The physical attack is the most basic of all terrorist tactics and is an important component in the IO strategy; a springboard to allow others elements to be integrated. “Psychological Warfare employs physical destruction at times for psychological effect “(Buettner, personal communication, May 2003). Hoffman considers armed propaganda (violent acts with clear symbolic intent) a critical element in terrorists’ operational calculus (1998, p.160). While DoD generally uses conventional military means to execute its doctrine, terrorist’s acts include kidnapping, political murder and bombings. Physical attacks are necessary to get first order effect (media attention) in the influence process (Influence Process Model, Chapter I). Spectacular and brutal deeds assure terrorists of substantial press coverage and public attention; otherwise they “would throw roses if it would work” (Nacos, 1994, p.8). A rule of thumb for successful terrorist Information Operations is that violence cannot be indiscriminate; it must be purposeful and deliberate, sustained and omnipresent in order to achieve maximum effect in perception domain. (Hoffman, 1998, p.161) Narodnaya Volya (People’s Will) used bombing and murder in attempting to bring about revolution in 1870 (Kramer, 1998, p.136). The method of individuals using extreme acts became known as “propaganda by deed,” (Kramer, 1998, p.136) Using physical attacks, as a means of influencing targets is as old as terrorism itself. The Zealots (66-73 A.D.) staged deaths so they had psychological repercussion (Hoffman, 1998, p.88), while the Assassins in tenth century A.D sought death and publicity. The Jewish terrorist group Irgun in 1948 used violence in place of a military strategy to undermine resolve and attract international attention to its quest to create a Zionist state (Hoffman, 1998, p.48). It is likely future acts of destruction will include destruction of computer and automation systems in support of main attacks, such as the Middle Core Faction attack in 1985 in Japan.

g. Computer Network Operations (CNO).

Terrorist cyberspace actions are not yet a critical tactic or threat, although this is the one area terrorists can quickly gain parity with states. The

majority of cyber related activity appears to be mainly defense (communication and coordination) and exploitation (intelligence collection), with very little attack (physical or digital destruction). Computers are critical for use in fundraising, money laundering, and propaganda, but their use alone shouldn't be viewed as cyber tactics or capabilities. Terrorists use of information technology merely represents its availability, ease of use, and affordability. Cyber tools are still insufficient for terrorists, because the costs are too high, and may never be viable as long as traditional methods are viable (Nelson, Choi, Iacobucci, Mitchell, & Gagnon, 1999, p. vii). CNO has the potential to cause widespread effects, but actual usage is limited to using the latest in encryption tools (p.32). Although several scenarios have demonstrated worse case results, there is no proof cyber warfare would be worth the investment when the possibility of a pay off can be small (Denning, p.70). The psychological pay off is still greater for traditional acts of terror such as bombing and hijacking (p.70). A 1999 Naval Postgraduate White Paper analyzed terrorists' use of CNO and categorized acts and activity as "cyber attack" (CNA) and "cyber support" (CND) (Nelson, et al.,1999, p.10). Cyber support allows a security conscience organization to flourish using available secrecy tools such as encryption and steganography (hiding messages within documents and images in plain sight. Cyber support such as communication, planning and coordination, recruiting, fundraising, money laundering is arguably invisible to actions for the cause but still part of the IO rubric of CNO. Cyber support augments or enhances normal terrorist CAN activities, such as degrading confidentiality, integrity, and availability (p.11). Cyber attacks include interruption of Defense C41 Systems and destruction of SCADA sensors. The White Paper goes in depth on tactics, resources, and likely application or courses of actions different groups would take. The IRA conducted Computer Network Exploitation when it infiltrated computerized database to steal information and used encryption to conceal files (Denning, 1999, p.68). Al Qa'ida has been researching weaknesses of Supervisory Controls and Data Acquisition (SCADA) systems (Venke & Ibrahim, 2002). Hamas uses "encrypted Internet communication to transmit maps, pictures and other details pertaining to

terrorists attacks" (Denning, & Baugh, 1999). Groups appear to use the Internet more to influence public perception than launch attacks.

There are limited examples of cyber attacks by groups. The Zapatista's use of Internet is possibly the most widely known. The Zapatista National Liberation Army (EZLN) compensated for lack of physical power in Mexico by dominating the information space. On April 10, 1998 Zapatista supporters (coordinated through the Internet) organized a denial of service (DOS) attacks against Mexican President Zedillo's website (Denning, 1999, p.73). Another example involved a coordinated computer network attack on Israeli infrastructure by the Palestinian hacker group UNITY (Denning, lecture, 2003). The attack was effective, but the hackers likely were only sympathizers of terrorist causes, and were not organized or directed by any terrorist groups. Steganography has gained widespread attention but there is no evidence to support it having been used by terrorists (Denning lecture, 2003). In the 1970's the Italian Red Brigade conducted physical attacks against computers and telecommunications systems (Denning, 1999, p.68.) The group launched 27 attacks on electronic, computer, and weapon businesses in order to strike "at the heart of the state" (Denning, 1999, p.69). A likely terrorist cyber attack would be in support of a physical attack. A cyber attack alone might go unnoticed in the clutter of daily life, but have more significance if conducted simultaneously with a physical attack (Lewis, p.4). A strategy in the future would be to combine distributed denial of service (DDOS) and communication jamming techniques against emergency services in conjunction with a large scale attack to create further chaos, degrade response, and increase damage and fatalities (Vatis, 2001, p.15).

h. Civil Military Operations (CMO).

Successful terrorist organizations must conduct a variation of civil military operations in order to gain and retain popular support within a country it operates (FARC, Hizzbollah) or among its transnational followers (PIRA, al Qa'ida). "Winning hearts and minds" is key to continued recruitment or financial

support and maintaining secrecy. While the US military uses CMO to influence and coordinate foreign civilian activities and civil organizations, terrorists use similar actions on indigenous or sympathetic populations. This is accomplished through a combination of propaganda and activities designed to win support. The FARC may provide a rural community with wealth or provide protection the government cannot. Hamas provides for families of suicide bombers, which gains not only community approval, but also it is also key inducement for recruitment. A group with community support improves its secrecy element, critical when states conduct internal offensives.

i. Intelligence Support.

Terrorists inherently rely on humans to gather intelligence, while DoD relies on technology. Terrorists are very successful in intelligence gathering, although human collection is riskier and time consuming. Given that constraint, groups likely take it into consideration as part of operation planning. Good intelligence is critical to support terrorist planning and objectives, and allows for coordination (Libicki, 2001, 4-1). Analysis of Al-Qa'ida's attacks on the USS Cole, the African embassies, and in the United States shows how al Qa'ida made up for a lack of sophisticated equipment with simple and secret information gathering ("Update: Investigation," 2000). Intelligence is critical for successful terrorist actions in the physical environment, which sets the stage for actions in the influence domain. This is done by conducting active and passive intelligence gathering and using insiders ("Update: Investigation," 2000). An example of poor intelligence undermining the critical timing associated with most terrorist acts occurred in Rome in 1969. The Popular Front for the Liberation of Palestine planned a sensational hijacking of a TWA flight "to coincide with a scheduled address by President Nixon to a meeting of the Zionist Organization of America" (Crenshaw, 1998, p.9). Nixon sent a letter instead (p.9).

j. Comparison of IO Methods.

Figure 9 illustrates elements of Information Operations, comparing some DoD methods of employment as discussed in chapter II to the terrorist methods discussed in this chapter. The figure reflects a few general methods of employing IO to illustrate the different approach terrorists take to IO.

IO Element	**Department of Defense Methods**	**Terrorist Methods**
PSYOP	Leaflets, broadcasts	Leaflets, physical attack, auto-propaganda
Deception	Feints, ruses	Concealing weapons, counter EW, proxies
OPSEC	Classification or limited release of information	Covert network, isolated cells, controlling actions prior to attack
Physical Destruction	Precision guided weapons, conventional forces, SOF, C2 nodes destruction	Car bombs, assassinations, hijackings, kneecappings, resource theft
EW	EA, ES, EP with ground, sea, air assets	Counter EW, scanners, DF and RF detonators
Public Affairs	External/internal information program	Media exploitation
Civil Military Operations	CA, SOF	Support families of suicide bombers; provide resources, protection or wealth to community

Computer Network Operations	Mostly CND communication and coordination) and CNE (intelligence collection)	CNA (DOS, destruction of nodes, hacking) CND (communication and coordination) CNE (intelligence collection
Intelligence Support	Sensors, UAV, HUMINT, SIGINT	Network of sympathizers, insiders, spies; active intel cells

Figure 9. Comparison of IO Elements

2. Terrorist Activity in the Conceptual Domains.

In chapter II, we discussed Waltz's theory on three main conceptual domains in order to set up a model to evaluate terrorists' use and application of IO. This section explores Waltz's information domains and highlights the common activities that terrorist conduct in each, showing that even most apparently singular-effect actions support a larger IO strategy.

a. Operations in the Perceptual Domain.

Terrorist use several elements of IO in the perceptual domain to directly influence the decisions of key leaders and populace. Often they integrate elements of PSYOP, Deception, OPSEC, PA & CMO, and Physical Destruction to leverage information in this domain.

Terrorists conduct strategically timed physical attacks such as bombings and assassinations as part of their psychological terror campaign. Often the selection of the target carries 'political weight' that is beneficial to their cause. Psychological warfare operations such as coercive bargaining, fear propaganda and death threats are proven tactics in influencing and shaping

perceptions. Protests, fatwas, and other activities often are used as a deception to disguise their true intentions, degrade the state's counter terrorist efforts or to provoke a 'heavy-handed' response from the government in order to exploit it. Secrecy enables the terrorist organization not only to hide its operations and training, but also to inhibit the state from discovering the true strength of the organization. Terrorists often adopt names such as Army, Brigade, or Front in order to 'sound' bigger than they actually are. Terrorists rely heavily upon public relations with the media and the population to propagate their message (propaganda) to different audiences, recruits new members into the organization, and appeal to sympathizers for financial support. Websites are also a cheap, flexible and valuable resource to reach international audiences (Denning, 1999).

b. Operations in the Information Infrastructure Domain.

Terrorist use this domain to protect information, communicate, and disrupt its enemies' command and control. Groups have demonstrated significant use of CND, but few terrorist organizations have the capability to conduct electronic warfare or CNA. However, groups like the FARC and IRA have demonstrated a limited ability to combat the state in the electromagnetic spectrum. The IRA succeeded in implementing electronic bypasses to subvert British electronic jamming of IRA remote detonating bombs. They also successfully wire tapped police and rival paramilitary phones to gather intelligence. Computer network operations are also not a critical component tactic, or threat, although terrorists do use cyberspace to communicate with other members and to conduct intelligence collection on potential targets. Computer scams and credit card theft have also been used in fundraising and money laundering. Defensive actions include Aidid subverting US EW collection systems by using low tech means such as drums codes and runners (Arquilla & Ronfeldt, 2001, p.11).

c. Operations in the Physical Domain.

The physical attack in the physical domain often provides the strongest influence in the information environment. Attacks such as suicide bombings, leadership assassinations, and hostage taking often provide overwhelming influence. DoD doctrine for physical destruction requires an attack to specifically affect a C2 node, terrorists use the attacks to enable or support a strategy in the IE. Examples include the Japanese Red Army killing 28 tourists in the Tel Aviv airport in 1972 to gain world-wide media coverage and to propel themselves "onto the world stage" (Nacos, 1994, p.50).

C. SUMMARY.

Violence and the threat of violence are the sine qua non of terrorists (Hoffman, 1998, p.183); terrorists plan operations to capture the attention of the media and to shock, impress, or intimidate the public and government with a deliberate planned application of violence (p.183). War and terrorism are about influencing the opponent. Terrorists hope to influence their targets to cede to their demand. This does not mean all terrorist actions are IO, but terrorist actions do inherently incorporate more elements of IO than DoD and they do it well. Terrorists rely often on violent attacks in the physical environment to enable their influence operations in the information environment. Thus, the physical attack serves as an enabler to IO.

This chapter attempts to establish a general IO framework for terrorists, thus providing a means to evaluate the terrorist case studies in subsequent chapters. In building the framework, the chapter first explores the covert, illegal nature of terrorist organizations. The terrorists' nature presents the organization a dilemma: the group must remain covert and secret to stay alive, yet must overtly gain legitimacy from the state and populace. The legitimacy dilemma establishes the first part of the framework by relating why terrorist employ IO in order to remain secret and then use it as a force multiplier to gain respect and legitimacy. This provides evidence that terrorist inherently integrate many elements into their operations to succeed. Next, the chapter examines the

terrorists' reliance on actions in the physical environment to support activities in the information environment and on how integral IO are to basic terrorist operations. This forms the second part of the framework and is conceptually different from the US military's use of IO to support combat operations in the physical environment. Next, the chapter presents Wright's analysis on the different audiences that terrorist must appeal to in order to gain influence. Finally, the chapter provides a terrorists' approach to IO by operationalizing the terms used to describe elements of IO. Figure 10 builds upon the IO framework presented in Chapter II, graphically depicting how terrorists apply elements of IO in each domain in order to affect the information environment and influence multiple audiences.

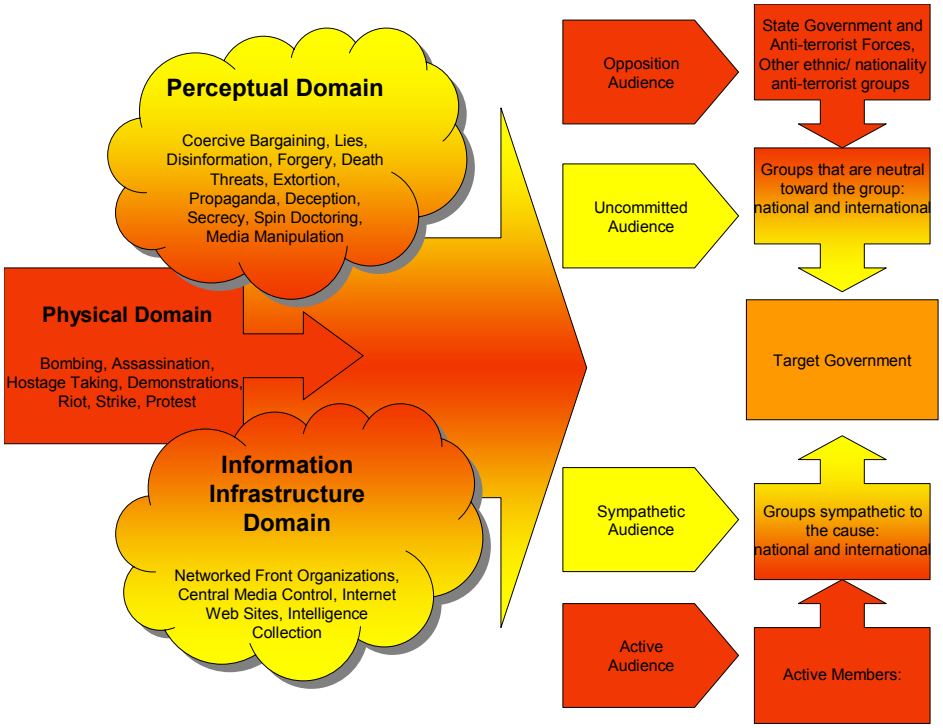

Figure 10. Terrorist IO Framework

The terrorist IO framework enables us to explore terrorist organizations and graphically depict how a group employs its IO toolkit to influence different audiences and achieve their strategic objectives. The IO framework incorporates

focal points established in this chapter: the legitimacy dilemma; using information as a force multiplier; using physical attacks to enable IO in the information environment; and the terrorists targeting of different audiences.

The IO framework illustrates how actions in one or more domains can influence one or more audiences in order to ultimately affect the target. The framework shows inherently how important and integrated IO is to standard terrorist operations.

Evidence suggests that terrorist may fully understand their legitimacy dilemma and their reliance upon the information environment. Their choice of IO tools suggests that they comprehend the power held in Waltz's information domains. Terrorists also seem keenly aware of the different audiences facing them. Terrorists understand their audiences and also use force multipliers to maximize advantages. While these assertions may not exist as published or written doctrine, it apparently exists for many groups as a strategy. Chapters IV and V will apply this framework to two different types of terrorist organizations to determine how they employ elements of IO.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. AL QA'IDA

This chapter analyzes how al Qa'ida (Arabic for "the base") employs Information Operations to achieve their strategic objectives. In order to gain an appreciation of the goals, motives, and operating environment of al Qa'ida, the chapter first explores the historical background of the organization and its charismatic leader, Usama Bin Laden. The chapter next develops an IO toolkit, consisting of the IO elements frequently used by al Qa'ida. The chapter then analyzes the group's major actions since 1996 to determine how the organization employs IO to achieve its strategic objectives. The depth of information available compared to the IRA is less, as many of the group's activities are not yet documented or declassified. The model introduced at the end of Chapter III is applied to determine the group's ability to use IO as a force multiplier to gain legitimacy and influence actions in the information environment. Finally, the chapter summarizes the findings of the analysis and provides a general assessment of al Qa'ida's use of IO.

A. BACKGROUND.

1. History.

Al Qa'ida is a transnational terrorist group responsible for executing the devastating attacks on United States soil on September 11, 2001, which killed 2,826 of the world's citizens and destroyed a symbol of America's economic dominance. The group "funds and orchestrates the activities of Islamic militants worldwide" ("US Embassy", 1998, p.3). and "attempts to radicalize existing Islamic groups and create Islamic groups where none exist" ("Al-Qa'ida," 2003). al Qa'ida serves as an umbrella organization for many Islamic Fundamental terrorist groups[11], and has supported Muslim fighters in Afghanistan, Algeria, Bosnia, Chechnya, Eritera, Kosova, Pakistan, Somalia, Tajikistan and Yemen"

[11] Groups include al-Jihad, Abu Sayyff, Islamic Jihad, Hamas, Hizzbollah, Mujahadeen, and al-Gama'a al- Islamiyya

("Al-Qa-ida," 2003). It is an adaptive and nimble international terrorist group dedicated to opposing non-Islamic governments with force and violence (US Embassy, 1998, p.3). It is a dangerous group that can function on different operation levels, which means it does not have a single modus operandi or unique profile (Hoffman, B. 2002). It grew out of the Afghan war against the Soviets, and its core members consist of Afghan war veterans from all over the Muslim world. Al-Qaida was established around 1988 by the Saudi militant Usama bin Laden and at one time operated in at least 60 countries (Jenkins, 2002, p. 9). In February 1998, bin Laden announced the formation of an umbrella organization controlled by al Qa'ida 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)" ("Al-Qa-ida," 2003), which is a coordinating body for groups worldwide (Alexander & Swetnam, 2001, p.6). Bin Laden formed this group specifically to conduct jihad against America and Israel ("Al-Qa-ida," 2003). He gained international prominence with his fatwas (religious rulings on Islamic law) and suspected masterminding of attacks on US targets such as the USS Cole in Yemen in 2000 and the East African embassy attacks in 1998. "Based in Afghanistan, bin Laden used an extensive international network to maintain a loose connection between Muslim extremists in diverse countries" ("Al-Qa'ida," 2003). Al Qa'ida stayed in touch "with an unknown number of followers all over the Arab world, as well as in Europe, Asia, the United States and Canada" through high-tech means, such as faxes, satellite telephones, and the internet" ("Al-Qa'ida," 2003).

Usama bin Laden's headquarters and training camps were located high in the Hindukush Mountains in Khuasan, Afghanistan, extremely forbidding terrain that isolated him from counter-terrorist units. Bin Laden incorporated the vast cave and tunnel networks, built during the 1970s to defeat the Soviets, into his strategy to provide secrecy and security for his operations. Bin Laden benefited greatly from the Afghanistan Taliban government providing him safe haven. Prior to September 11th, 2001, there were no direct threats to his headquarters and training base. Al Qa'ida active cells were and remain dispersed throughout the

world, often operating as sleeper cells. Leading up to the 9/11 attacks on the US, active members of al Qa'ida operated within the US, posing as students, professors, and businessmen until they received the 'execute' order from bin Laden (Robbins, 2002, in Howard & Sawyer, 2003, p. 358).

Al Qa'ida's tactics and capabilities include "bombing, hijacking, kidnapping, assassination, and suicide attacks" (Alexander & Swetnam, 2001, p.32). Additional tactics include sabotage, cyber-based strike, shooting, vehicular bombing, biological, chemical, and kidnapping (Venke & Ibrahim, 2002). At one time the group actively sought weapons of mass destruction, and have been linked to production of chemical and biological agents (Alexander & Swetnam, 2001, p. 32). A recent CIA report states the group's "ultimate goal is the use chemical, biological, nuclear or radiological weapons to cause mass casualties," but near term use of these weapons will likely be for small-scale attacks ("CIA: al-Qaeda," 2003). The group relies on criminal activity to finance operations, including front organizations, false charities, money laundering, stolen car trafficking and credit card fraud (Elliott, 2002). Very few books and unclassified material exist on the analysis of al Qa'ida's activities before and after attacks on the USS Cole and the embassies in east Africa, and on September 11th. The United States continues to gather new data through debriefing of captured members and peripheral associates.

2. Goals.

The organization's primary goal is the overthrow of what it sees as the corrupt and heretical governments of moderate Muslim states, and their replacement with governments based on the rule of Sharia (Islamic law) ("Al-Qa'ida," 2003). Al-Qa'ida is intensely anti-Western, and views the United States in particular as the prime enemy of Islam. The group advocates destruction of the United States, which is seen as the chief obstacle to reform in Muslim societies. According to a 1998 indictment against bin Laden and members of al Qa'ida for the 1998 US Embassy bombing in Kenya, al Qa'ida opposed the US for four reasons. "First, the United States was regarded as an 'infidel' because it was not

governed in a manner consistent with…Islam. Second, the United States was viewed as providing essential support for other 'infidel governments and institutions…Third, …al Qaeda opposed the continued presence of American military forces in Saudi Arabia…following the Gulf War. Fourth, al Qaeda opposed the … arrest, conviction and imprisonment of persons belonging to al Qaeda or its affiliated terrorist groups…"("US Embassy", 1998, pp. 4-5). One of the principal goals of al-Qa'ida has been to drive the United States armed forces out of Saudi Arabia (and elsewhere on the Saudi Arabian peninsula). Bin Laden has issued three fatwas, calling upon Muslims to take up arms against the United States, indicating that such attacks were both proper and necessary (indictment, 1998, p. 5).

3. Organization.

Usama bin Laden, a Saudi, founded al Qa'ida and served as its emir-general at least through the US invasion of Afghanistan in 2001. It is unclear if he is still alive, or what role he currently plays in the group's strategy and operations. Another prominent leader is Dr. Ayman al Zawahiri, leader of Egyptian Islamic Jihad. Zawahiri serves as a mentor to bin Laden and is often considered his deputy. Muhhamed Atef (deceased) was the heir apparent to take over leadership of al Qa'ida. Another prominent leader was Abu Zubaydah (captured), who was responsible for external affairs. According to Alexander & Swetnam (2001), al Qa'ida in 2001 had a command and control structure that included a consultation council, majlis al shura (p.3). "The council considered, discussed, and approved major policies and actions, including terrorist operations and the issuing of fatwahs" (p.3). Bin Laden, Zawahiri, Atef, and nine others sat on this council ("US Embassy", 1998, p. 7). The group's military committee, previously run by Atef, "considered and approved military matters" (p.3). Other known committees were the business committee, which oversaw front businesses, fundraising, and financial matters. These companies operated like wholly owned corporations, and included al Hijra Construction, Ladin International (Import-Export) and Taba Investments (Snyder, Wendelken, and

Wallace, 2003). A religious (fatwa) committee oversaw Islamic studies and deliberated religious rulings before consideration by the consultation council. The media committee assembled and printed information and publicized statements of bin Laden; it additionally "served as a conduit for messages, including reports on military and security matters from various" cells ("US Embassy", 1998, pp.7-8). Al Qa'ida also had a travel office (p.3). The group has several standing cells, such as Logistics and Training (Snyder, Wendelken, and Wallace, 2003). The logistic cells were region specific and provided forged documents, arms, transportation and equipment. The training cells recruited new members and trained local groups, and assist surveillance teams in their regions. The training cells could become operational if ordered. Bin Laden formed for al-Qa'ida a political arm called the Advice and Reform Council (ARC) in Sudan in 1994 after his family publicly denounced him (p.5). Bin Laden and al Qa'ida leadership have used the ARC to publish "several statements condemning the Saudi and western governments" (p.5). Figure 11 illustrates al-Qa'ida's structure.

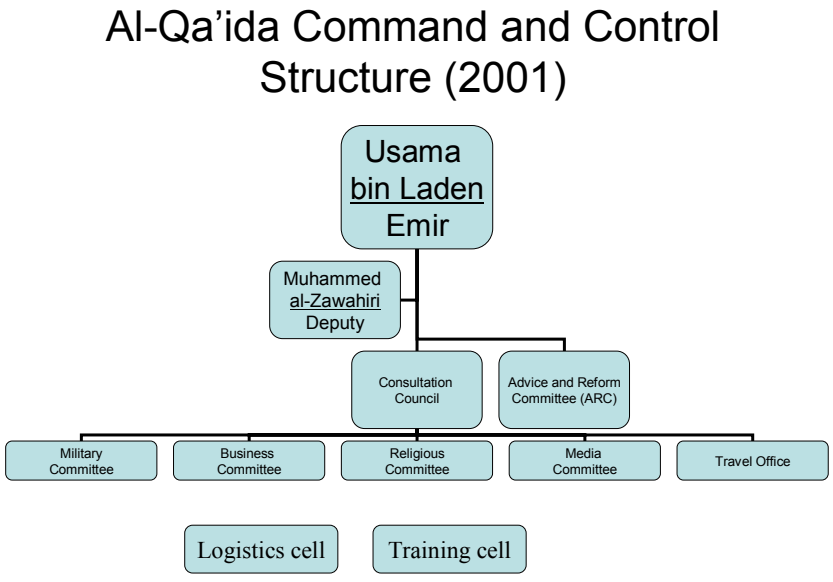

Figure 11. AL-Qa'ida Command and Control Structure, May 2001

Front organizations include Internet based groups, false organizations or companies, and dubious charities. Islamic Studies and Research Center, which

runs drasat.com, is purported to be a made up name and doesn't exist (Thomas, 2003, p.2, 7). Al-Qa'ida uses Islamic humanitarian "charities" in the US and other countries to conduct their fundraising (Thomas, p. 4). One of the United States organizations was Mercy International Relief Agency (Alexander & Swetnam, p.29). "Analysts found al Qaeda and humanitarian relief agencies using the same bank account numbers on numerous occasions" (Thomas, p. 4). The group's religious affiliation with the Muslim faith may be a far-reaching common bond. The group is able to have its message spread by clerics in mosques around the world, while Muslim charities can raise or launder its funds in plain sight. Bin Laden formed the ARC as another means of publishing the group's statements.

4. AL Qa'ida Supported Attacks.

Neither bin Laden nor al Qa'ida have claimed responsibility for any attacks (to include the 9-11 attacks), making it unclear which attacks the group was responsible for and which were conducted by loosely connected supporters. The following attacks have been linked to al Qa'ida or its associates.

- **"Nov. 28, 2002:** Suicide bombing at an Israeli-owned hotel in Mombasa, Kenya, that killed 15 people and injured 80. Also, shoulder-fired missiles narrowly missed an Israeli Arkia airline plane carrying 261 passengers.
- **Oct. 28, 2002:** American diplomat Laurence Foley is shot by a lone gunman at close range as he walked to his car outside his home in the Amman, the capital of Jordan. Libyan Salem Saad bin Suweid and Jordanian Yasser Fathi Ibrahim have been arrested in connection with the murder.
- **Oct. 12, 2002:** 202 people were killed in a bombing of a nightclub frequented by westerners in Bali, Indonesia.
- **Sept. 11, 2001:** Four U.S. planes were hijacked and crashed into the World Trade Center, the Pentagon and a field in Pennsylvania killing 2,826 people.
- **Oct. 12, 2000:** Bombing of the USS Cole anchored in Aden; 17 sailors killed; 39 wounded.
- **Aug. 7, 1998:** Bombings of U.S. embassies in Kenya and Tanzania kill 224 people, including 12 Americans.
- **June 25, 1996:** Bombing of Khobar Towers apartments at a U.S. military barracks in Dhahran, Saudi Arabia; 19 U.S. airmen killed; 372 Americans injured.
- **Nov. 13,1995:** Bombing at U.S. Army training headquarters in Riyadh, Saudi Arabia; 5 Americans killed, 31 wounded.

- **Feb. 26, 1993:** Truck bomb at the World Trade Center in New York City kills 6 and injures more than 1,000" ("Attacks linked," 2003).

B. AL QA'IDA INFORMATION OPERATIONS TOOLKIT.

1. Different Audiences.

Al Qa'ida has a key understanding of the message receiver, whether it is its own followers, the Muslim population, or moderate Muslim and Western state leaders. Al Qa'ida has developed several means to leverage the information environment and influence the four different audiences described in chapter III, including the *Opposing, Uncommitted, Sympathetic,* and *Active* audiences.

The Opposing audience consists of several entities directly opposed to the goals of the al Qa'ida. Al Qa'ida often selects the United States as the primary target for physical attacks or propaganda, but also has included Saudi Arabia, Britain, Australia, Israel, and Norway[12]. These physical attacks, which are relatively meaningless from a military or attritional point of view, are designed to provoke a counter-action that will have a major impact in the perceptual domain.

According to Wright (1990), the uncommitted audience has two components: the general public of the country where the terrorists are operating and the international public. There are a significant number of Muslims who likely do not approve of terrorism or a group's use of Islam as justification of its actions, but also do not support Western policies or influence. A recent RAND report states that citizens of northern Pakistan towns have high resentment toward the jihadists for leading hundreds of their young men to slaughter (Elliott, 2002). Al Qa'ida tries to unite or mobilize Muslims around the world, despite the ethnic and cultural differences. Al Qa'ida uses propaganda such as fatwas, media releases, and websites in this effort.

The sympathetic audience is comprised of those people, locally and internationally, who already have a broad historical or ideological sympathy with the terrorists' expressed political aims (Wright, 1990, p.77). Al Qa'ida has

[12] A press release in May 2003 threatened attacks in Norway, although the country has not been involved in the war on terrorism.

reached out to this audience by trying to bridge “Islamic brotherhood and a hatred for the United States and its allies” (Orbach, 2001, p.5). This audience also has the majority of potential recruits for the organization. “[T]he attacks of Sept. 11, 2001 were potentially an effective recruiting weapon” (Elliot, 2002). The al-Jazeera network has been an important conduit to the sympathetic audience because of the station’s credibility with many Muslims (who may have distrust of Western media). Al Qa’ida has attempted to unify this sect of Muslims by championing the Palestinian cause or declaring support for Iraq in 2003, as well as decrying Western occupation of Muslim Holy Land. Although such crises are peripheral or unrelated to al Qa’ida’s goals, they represent opportunity to create solidarity and bring more followers into its fold; they also represent an understanding of the value of the information medium by setting the group up as the underdog against the large enemy, a David and Goliath scenario (Fighel, 2001). Bin Laden has promoted his cause to this audience through media, capitalizing on all conflict to promote his own agenda (Schweitzer, “bin Laden Productions”, 2001). Al Qa’ida uses physical attacks on the United States to incite a response, which the group then asserts is as an attack on Islam. By not claiming responsibility for any of its attacks (al Qa’ida generally only issues declarations of praise or support for the attacks), the group can create the image of a persecuted victim at the hands of the “infidels.” This helps to keep the sympathetic audience emotionally involved in the cause and to justify further violence.

The active audience is made up of those people who are actively engaged in or directly support violent actions. al Qa’ida uses ‘auto-propaganda’ in order to target the active audience. Auto propaganda is used to instill or reinforce ideas into a group’s followers. The intent is to defend and protect active members from Western influence and help retain their convictions. The members hear only information that is conducive to the cause. Al Qa’ida regularly provides vague or misleading interpretations of the Quran to motivate recruits and followers (Paz, 2001). Evidence of this was evident in letters written by the 9/11 hijackers. The hijackers spent months in the US prior to the operation and yet remained

committed to the mission despite exposure to Western influences. This highlights the success of this technique. Perhaps the best known example of auto propaganda by al Qa'ida is the use of the concept of a rewarding afterlife surrounded by virgins in order to enlist martyrs and keep the thousands of followers involved in a protracted struggle (Hoffman, 2002, p.10). The group also uses websites and other media mediums to get a message to this audience (see Public Affairs, CMO, and Propaganda section).

Usama bin Laden's unprecedented attack against the United States on September 11th, 2001 is an example of a single attack meant to convey messages to multiple audiences. The targets were selected not only to influence the Bush Administration and US government (opposing audience) and most of the American citizens (uncommitted audience), but also international audiences (Buettner lecture, October 2001). The message was that the most powerful nation could not protect its citizens (Nacos, 1994, p. 60). The lethalness and willingness of the attacks sent a message to other audiences such as Israel (opposing), Saudi Arabia and other moderate Arab states (uncommitted). The attacks appealed to sympathetic audiences in Iraq, Lebanon, and other anti-US states to join al-Qa'ida's cause. Bin Laden conveyed a message to the Muslim population worldwide for different reasons. The attacks also signaled commitment to current and potential members in the active audience, as well as financial, political and logistical backers in the sympathetic audience. Figure 12 illustrates the al-Qa'ida audiences with the framework introduced in chapter III.

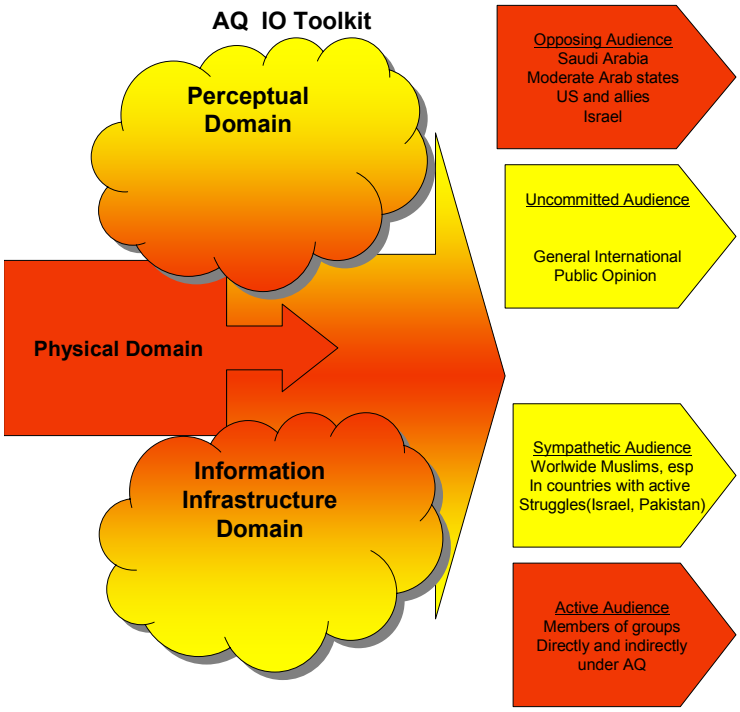

Figure 12. Al Qa'ida Audiences

Al Qa'ida may have miscalculated its ability to influence international audiences on September 11th, 2003. Bin Laden underestimated the mobilizing impact of his physical attacks, violating a critical Tugwell principal (see chapter I). The physical environment is a delicate environment that can at times undermine actions in the information environment, at which point it is difficult or impossible to recover. Bin Laden tried to recover by taking his message directly to the media via videotape and voice recorded speeches. Using al-Jazeera, he was able to find a launching point for the message; however, the majority of key international such as BBC and almost all US media outlets "refused to broadcast or transmit the tapes in America" causing the media campaign to fail (Boaz, 2002).

Figure 13 illustrates al Qa'ida's tactics and techniques, applied to the framework proposed in chapter III. Evidence suggests that the terrorists have developed significant capability in each of Waltz's information domains.

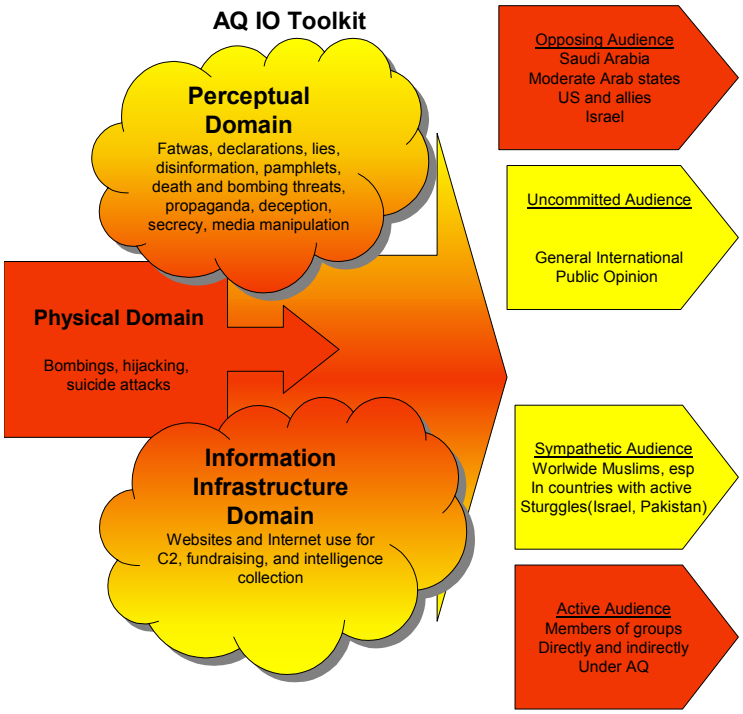

Figure 13. AL Qa'ida IO Tool kit

2. Elements of the Toolkit.

a . PSYOP and Deception.

Al-Qa'ida used the US's heavy reliance on technology-based intelligence sensors to deceive us in the fall of 2001 (Tiboni, 2001). Usama bin Laden's terrorist network was fully aware of the collection systems, such as spy satellites, and voice and signal intercepts, that were monitoring its actions. Bin Laden used low tech means such as couriers to communicate and conduct financial transactions (Walcott & Strobel, 2001). In May 2001, bin Laden deceived U. S. technical collection systems by allowing a major attack plan to be monitored (Walcott & Strobel, 2001). The US believed two major attacks were going to occur against American targets on the Arabian Peninsula. The US reacted with increased security and travel advisories, which appeared to have thwarted or dissuaded bin Laden from carrying out the attacks. The group likely evaluated US reaction in order to exploit further weaknesses or modify tactics as part of the September 2001 attacks. Defense News even ran an article

trumpeting the use of Information Warfare to thwart the attack (August, 2001). US overconfidence and heavy reliance on technology contributed to the disastrous results in Sep 2001. Hijackers and suicide bombers who conceal their missions and attacks employ tactical deceptions. One technique was the use of code words such as “honey” (explosives CD-ROM), “little girl” (forged driver’s license), and “toy” (pistol) to make intercepted conversations appear innocuous to intelligence analysts (Buncombe, 2003). The group conducts cyber deception by continually moving its main websites (see next two sections) to unsuspecting Internet Service Providers (ISP) and existing websites in order to remain active.

Propaganda, in addition to the psychological terror from physical attacks, is a key element of the group’s psychological operations and is discussed in depth in the following section.

b. Public Affairs, CMO and Propaganda.

Al Qa’ida uses the media as a psychological offensive, conditioning and response (Fingel, 2003). The real-time footage of 9/11 transmitted instantly around the world had profound impacts not only on all Americans, but on the international community as well (Hoffman, 1998 p.153). Bin Laden understood the tools of modern terrorism were not limited to explosives, bombs and automatic weapons, “but also the mini-cam, videotape, television, and the Internet” (Hoffman, 2002, p. 10). Usama Bin Laden issued a Declaration of War in 1996 through al-Qa’ida that was a rally call for his organization against Christians and Jews. Media outlets such as CNN and major US newspapers gave the declaration international attention with significant coverage of the document’s bold wording against the United States. He also circulated a professionally produced and edited two hour al Qa’ida recruitment tape in March 2001 throughout the Middle East, an example of his exploitation of “twenty first century communications and weapons technology in the service of the most extreme, retrograde reading of the holy war “(Bergen as cited by Hoffman, 2002, p. 11). The tape became a popular and successful propaganda tool, and was converted to CD-ROM and DVD formats and loaded onto the Internet. Hoffman

asserts that the crowning evidence of Bin Laden's "communication acumen and clever manipulation of media was the pre-recorded, preproduced, B-roll…that bin Laden had queued and ready for broadcast within hours of the commencement of the American air strikes on Afghanistan on Sunday, October 7th" (Hoffman, 2002, p.11).

The May 2003 attacks in Saudi Arabia were preceded by a media release proclaiming a large attack by al Qa'ida was going to occur soon on Saudi soil. The specificity deviated from previous broad generic declarations, and could be an attempt of reasserting legitimacy among opposing and sympathetic audiences. When an al Qa'ida representative states a large attack will occur, and it does, the resulting psychological impact of credibility and terror can make the number of deaths less significant. The deviation is a signal that the group may be on the downward slope of its life cycle, and is conducting action is previously did not need or want to do. Al Qa'ida used the media to reassert it legitimacy in order to continue to make gains in the information environment. Once reestablished as a credible threat, the group may be in a position to go back to its subtle/passive/limited use of media.

The following websites have been linked to al-Qa'ida since September 2001, according to Timothy Thomas[13] (2003) in his article, "Al Qaeda and the Internet." There are also various sites of alleged members or sympathizers that are used to communicate or post propaganda. This medium can be a significant recruiting tool

- "Alneda.com, which US officials said contained encrypted information to direct al Qaeda members to more secure sites, featured international news on al Qaeda, and published articles, fatwas…and books" (p.2). The website has also supported al Qa'ida's command and control of its dispersed forces, allowing them to work independently. The site provided "leadership via strategic guidance, theological arguments, and moral inspiration"

[13] LTC (ret) TimothyThomas US Army, analyst, Foreign Military Studies Office, Fort Leavenworth, Kansas.

(p.5), The site also published personal information of 84 al Qa'ida fighters captured in Pakistan so sympathizers could contact their families (p.5).

- "almuhrajiroun.com, an al Qaeda site which urged sympathizers to assassinate Pakistani President Musharraf" (p.2).
- "jihadunspun.net, which offered a 36 minute video of Osama bin Laden"(p.2).
- "7hj.7hj.com, which aimed to teach visitors how to conduct computer attacks" (p.2).
- "aloswa.org, which featured quotes from bin Laden tapes…and support for the al Qaeda cause" (p.2)
- "drasat.com, run by the Islamic Studies and Research Center (which is allegedy a fake center) and reported to be the most credible of dozens of Islamist sites posting al Qaeda news" (p.2)
- qassam.net, assan.com, jehad.net, alsaha.com, islammemo.com, mwhoob.net, and aljehad.online

Al Qa'ida used the Internet in the aftermath of the 9/11 attacks to justify its actions and to target prominent dissenting Muslims. According to Thomas (2003), Al Qaeda's two websites, alneda.com and drsat.com, ran commentary that "Muslims are committed to spread Islam by the sword" because Islam and the West do not share fundamental values (p.3). Subsequently, "several Muslim critics of al Qaeda's policies withdrew their prior condemnation" (p.3). Thomas states this is an example of ideological warfare working. The Center for Islamic Studies and Research's (a made up organization, according to Thomas) website is valuable auto propaganda tool. The site "has 11 sections, including reports on fighting in Afghanistan, world media coverage of the conflict, books on jihad theology, videos of hijackers' testaments, information about prisoners held in Pakistan and Guantanamo Bay, and jihad poetry" (p. 7).

A well known example of al Qa'ida auto propaganda previously mentioned is the selling of the concept of a rewarding afterlife with adoring virgins to enlist martyrs and keep followers committed to the cause. Part of this promise is the "martyr would feel no pain in his sacred attack and ascend immediately to glorious heaven containing "rivers of milk and wine…lakes of honey, and the services of 72 virgins", where the martyr will see the face of Allah and later be joined by 70 relatives" (Hoffman, 2002, p. 10). This propaganda is aimed not only at potential members but also current members. As previously discussed, letters left behind by the 9-11 hijackers made common references to the afterlife concept along with passages of the Quran. This is especially significant, given most of the hijackers lived in the United States several months prior to the hijackings.

c. EW and CNO.

Al Qa'ida has significant defensive EW capability; primarily the knowledge and deception of US EW collection capability (see PSYOP and Deception). Bin Laden used low-tech means such as couriers to communicate and conduct financial transactions (Walcott & Strobel, 2001). Members fighting the United States in Afghanistan have used remote detonation of bombs against soldiers. It is possible al Qa'ida intercepted electronic communications alerting of the arrival of the USS Cole, though US Naval authorities believe the arrival was gained by means of aggressive human intelligence collecting ("Update: Investigation into the Bombing of USS Cole," 2000).

Al Qa'ida's use of computer network operations is more documented and likely more significant than its EW use. It uses the net as an ideological weapon (Thomas, 2003) for its cause (see also Public Affairs, CMO, and Propaganda). There is no evidence of al Qa'ida using cyber tools as a weapon, although other Muslim radical sub-state groups like Hizzbollah or Hamas have directed attacks or had attacks conducted in their name. The Internet is an excellent tool for terrorists because it provides anonymity. Users can create and delete accounts with large companies such as America Online,

use instant messaging, use anonymous login tools and navigate chat rooms. Additionally, users "can access cyber cafes, university and library computers…to further hide the source of the messages" (Thomas, 2003, p.3). The 9-11 hijackers used these locations to communicate anonymously around the world prior to the hijacking. An al Qa'ida laptop recovered in Afghanistan showed several visits to the French Anonymous Society, which offered "a two-volume Sabotage Handbook online" (p. 3). The virtual world allows al Qa'ida to continue to communicate. Even though their websites can be shut down, a site can quickly reemerge, likely hosted by an unsuspecting ISP. The group's site, "www.alneda.com, was originally located in Malaysia until" May 13th, 2002, reappearing in Texas (http://66.34.191.223/) on June 13th. Another al Qa'ida site, www.drasat.com, appeared in Michigan on June 21st before being quickly shut down (Thomas, 2003, p.4). Thomas considers this shell game cyber deception. Several US personal websites serving as unsuspecting hosts have had al Qa'ida web pages secretly attached ("Islamic Hackers," 2003).

The Internet allows a security conscience organization to flourish with available tools, such as encryption in email and websites. According to al-Jazeera, Mohammed Atta (one of the pilot terrorists on 9/11) reportedly sent a simple and open message to al Qa'ida leadership referencing the status of his mission. The message read "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering" (as quoted in Thomas, 2003, p.7). The message likely references the coordination of the 4 hijacking crews. Thomas reports "Al Qaeda uses prearranged phrases and symbols to direct its agents. An icon of an AK-47 can appear next to photo of Osama bin Laden facing one direction one day, and another direction the next" (Thomas, 2003, p.7). Icons can change color, messages hidden of pages that have no link connection, "or placed openly in chat rooms" (Thomas, 2003, p.7).

The Arab TV station al-Jazeera last year played audio recordings of bin Laden speeches and showed a note supposedly signed by him. The notes praised recent attacks on a tanker in Yemen and soldiers in Kuwait (Thomas,

2003, p.4). These messages were picked up and “spread around the Internet, offering virtual proof that bin Laden was alive” (Thomas, 2003, p.4). Thomas believes this allows bin Laden to lead in absentia, even after death, as “his image can be manipulated through or Internet broadcasts so that he appears confident, even healthy” (p.4).

A website associated with al-Qa’ida, 7hj.7hj.com, provides instruction for Internet users on “how to conduct computer attacks, purportedly in the service of Islam” (Thomas, 2003, p.8). al Qa’ida has been researching weaknesses of Supervisory Controls and Data Acquisition (SCADA) systems (Venke & Ibrahim, 2002). It is unclear the extent of its knowledge, its intent, or even if the group is capable of carrying out such an operation. The virtual threat of computer attacks may be al Qa’ida’s most significant cyber tactic (Thomas, 2003, p.4). “Cyber-fear is generated by the fact that what a computer attack could do (bring down airliners, ruin critical infrastructure, destroy the stock market, reveal Pentagon planning secrets, etc.) is too often associated with what *will* happen” (Thomas, 2003, p.4). Although many worse case scenarios have been suggested, such as bringing down the stock exchange or disrupting utilities, a likely al Qa’ida cyber attack would be in support of a physical attack. A cyber attack alone might go unnoticed in the clutter of daily life, but have more significance if conducted simultaneously with a physical attack (Lewis, 2002, p.4). A possible strategy in the future would be to combine Distributed Denial of Service and communication jamming techniques against emergency services in conjunction with a large scale attack to create further chaos, degrade response, and increase damage and fatalities (Vatis, 2001, p.15).

d. OPSEC.

Al Qa’ida produced a document called the Jihad Manual, which had explicit, “micro managing” instructions on operational security (Hoffman, 2001). Secrecy is a necessary and priority element of all covert organizations, and is sometimes degraded as groups grow in size or undertake large operations. The manual demonstrates the organization’s understanding and commitment to

maintaining secrecy; secrecy of operations is tantamount to success of physical environment actions, the precursor to the intended influence effects. Al Qa'ida's al-Jihad manual provides scenario-driven guidance and direction to active members such as how to blend into society in order to maintain secrecy during an operation.

Al Qa'ida had originally planned to launch a boat bomb at the USS Sullivan (Schweitzer, "The Bin Laden Principle," 2001). A miscalculation of the weight of the explosive charge sank the boat, delaying the operation for 10 months, eventually attacking the USS Cole in October 2000 (Schweitzer, 2001). The coordinator's ability to keep the operation a secret after a public failure is a testament to the group's OPSEC capability.

e. Destruction.

Al Qa'ida's physical attacks are the result of thorough intelligence and extensive planning and coordinating. Each attack is likely designed to speak to multiple audiences in the group's quest to reduce Western influence and install strict Islamic rule in moderate Arab governments. The attacks are designed to have a profound psychological impact by striking fear among the victims, and perhaps those that stand beside them. The use of suicide bombers for physical attacks is "a central part of the terror organizations' psychological warfare" (Schweitzer, "Suicide Terrorism and the September 11 attacks," 2002).

f. Intelligence.

Analysis of Al-Qa'ida's attacks on the USS Cole, the African embassies, and in the United States shows how al Qa'ida made up for a lack of sophisticated equipment with simple and secret information gathering ("Update: Investigation," 2000). Intelligence is critical for successful terrorist actions in the Physical Environment, which sets the stage for actions in the Information Environment. This is done through use of the Internet, conducting active and passive intelligence gathering, and using insiders ("Update," 2000). The "Internet

is used to gather information on potential targets," according to Thomas (2003, p.6). The Muslim Hackers Club (no known al Qa'ida link) provides information, tutorials, chat rooms, and connectivity to other extremists groups (p.6). Information discussed includes Secret Service code names and potential targets such as Center for Disease Control in Atlanta, FedWire, and weaknesses on SCADA systems. One captured al Qa'ida computer contained imaging data and "engineering and structural architecture features of a dam" (p.6).

C. BATTLE ANALYSIS OF 9/11 ATTACKS.

This section analyzes al Qa'ida's direct use of IO elements for the 9/11 attacks in order to show the extent and level of synchronization. Al Qa'ida used the full spectrum of IO to hijack four commercial airliners and crash three of them into their intended targets.[14]

Operational Secrecy was a key element for success for the 9/11 attacks. OPSEC kept the group viable amidst targeting due to the 2000 attack on the USS Cole. OPSEC allowed 19 (and possibly more) terrorists to without suspicion to take flight training and reside without detection in the United States for several months prior. OPSEC allowed al Qa'ida to conduct a believable deception by convincing the United States the group would conduct large scale attacks in the summer of 2001 against US interests in the Middle East. OPSEC allowed terrorists to communicate, coordinate, train, and transact funds in the months and years prior without detection (though at least one did not arrive in the US due to VISA issues [Elliott, 2002]). The Jihad Manual (see OPSEC section) provided OPSEC guidance in minutia to those taking part in operations. OPSEC kept bin Laden's and al Qa'ida's connection nebulous, forcing the onus unto the US to prove their involvement.

Recruiting members and retaining their commitment to the cause and mission requires a significant auto-propaganda program. Recruitment for the attacks likely stemmed from media products (CD-ROMs and leaflets), attention

[14] One airliner crashed into the Pentagon, and two others hit both towers of the World Trade Center. The fourth plane, intended for the capitol (Elliott, 2002), crashed in Pennsylvania.

garnered from previous attacks (embassies and the USS Cole), and bin Laden fatwas and statements following US attacks on his base in Afghanistan. Bin Laden surviving those attacks created a mythical persona, increasing the impact of his words, which resonated with disenfranchised Muslim males. Al Qa'ida exposed members to an immersed environment of Islamic studies full of vague and misleading scriptures of the Quran, which justified and necessitated personal sacrifice and attacks on the West. The indoctrination can explain how the hijackers remained committed to the mission despite experiencing a Western way of life for several months in 2001. Auto propaganda was likely key in getting its members to fight the vastly superior US military forces in 2001 and early 2002. All these events contributed to the attacks on September 11, 2001, despite being seemingly unrelated.

An important part of the 9-11 attack was the deception several months prior (see paragraph (a) in previous section). Al Qa'ida was able to get the US to respond to indicators of a large scale attack in the Middle East. US actions further legitimized al Qa'ida as a credible threat. US actions further revealed US response and collection methods, and likely diverted attention from the 9/11 attacks. The deception involved OPSEC, counter EW, and intelligence support. Intelligence played a key role in knowing what, when and how electronic systems were monitoring actions and conversations, and in selecting credible deception targets. The group likely measured the effectiveness of the deception, shoring up its own weakness and exploiting the US based on its reactions.

Deception also involved the various front organizations and scams used to finance these operations. The use of code words made intercepted conversations seem harmless or meaningless. Such tactics were necessary when members communicated on the Internet via cyber cafes, libraries and educational institutions. Websites were established or commandeered, providing forums for messages, coordination, and propaganda, before and after the attacks. Various encryption tools were used to protect sensitive data. Intelligence support was critical in learning commercial flight info, which is available as open source.

The crashing of the planes itself provided the psychological warfare message. Worldwide media supported the tactic by replaying within an hour images of the planes crashing, and later the towers tumbling. The media captured the fate of its victims, the horror, apathy, and joy of citizens around the world. Bin Laden released a statement commending the attacks but not claiming responsibility. Al Qa'ida websites immediately rolled out information designed to capitalize on the attacks. The sites information not only reached out to sympathetic and active audiences, but also targeted prominent Muslim leaders who had criticized the attacks. The physical attacks had occurred, and it was time to orchestrate the actions in the information environment. Once the anticipated American air strikes occurred, bin Laden immediately release a prepared "B-Roll" video to al-Jazeera (credible media source for many Muslims). The film contained images and speeches that increased his mysticism. He attempted to unite populations and different audiences by making the Palestinian cause also al Qa'ida's cause, and improving al Qa'ida's support within Afghanistan and Pakistan.

Figure 14 is the terrorist IO framework applied to al Qa'ida's use of IO in the 9/11 attacks.

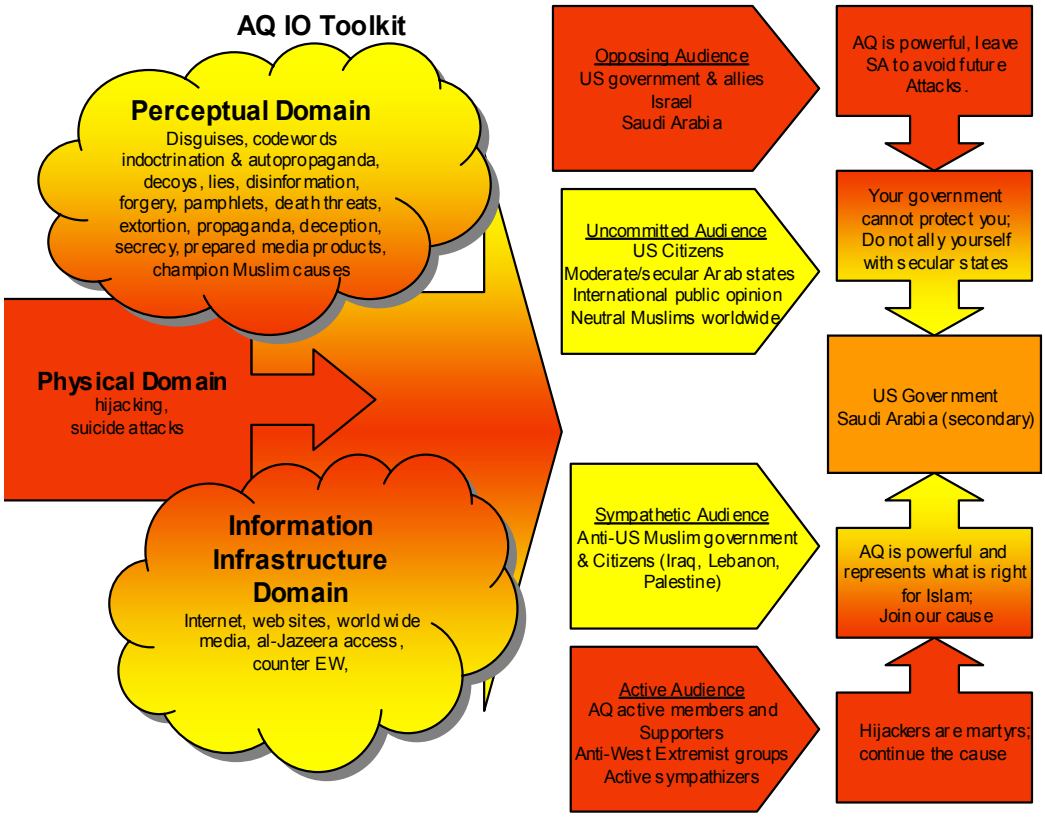

Figure 14. Al-Qa'ida 9/11 Attack

D. SUMMARY

This chapter gave an overview of al Qa'ida, including its history, goals, and motives. The chapter then explored al Qa'ida's IO toolkit. First, it examined how the terrorists oriented their messages to influence multiple audiences. Oftentimes, targets are specifically selected for the influence that their death will bring about. Secondly, the chapter examined the principle elements of IO that al Qa'ida has at its disposal. Evidence from this chapter suggests that al Qa'ida has developed a fairly diverse IO toolkit containing many of the principle elements of IO discussed in chapters II and III. Its greatest strength lies in its use of propaganda and the media, while Computer Network Operations are currently underused but could to be developed further. Its understanding of the information environment, however, is significant, using it to ascend to legitimacy and to communicate with worldwide audiences.

V. PROVISIONAL IRISH REPUBLICAN ARMY

This chapter provides an analysis of how the Provisional Irish Republican Army (IRA) employs Information Operations to achieve their objectives. The chapter first explores the historical background of the organization in order to gain an appreciation of the goals, motives, and operating environment of the organization. The chapter then develops an IO toolkit consisting of the IO elements frequently used by the IRA. Next, the chapter analyzes the time period from 1969 to present, known as 'the Troubles'. This period of time was selected because the Provisional IRA first came into existence in the late 1960s, splintering off from the Official IRA. The Troubles was also one of the IRA's most active times, providing ample opportunity to observe how it employs IO. Finally, the chapter applies the framework established in Chapter III to evaluate the IRA. The chapter concludes with a summary of the findings and provides a general assessment of the IRA's use of IO.

A. BACKGROUND.

1. The Operating Environment.

Sectarian violence between the Protestant and Catholic communities, which has polarized Northern Ireland for hundreds of years, has cultural roots dating back to the Norman invasion in 1170 and the English plantations in the 1600s[15]. Centuries of violence in Ireland and the "memory of the battles of Kinsale (1601) and the Boyne (1690) between the Protestants and the Catholics is kept alive in Republican circles today" (Laqueur, p.33). Irish Catholics have long harbored feelings of betrayal, oppression, and inequality toward the British

[15] The Norman invasion in 1170 first brought the English presence to Ireland. The English presence disrupted the ethnic balance in Ireland. Many Irish viewed the English as an invading force. In the 1600s England dramatically worsened the situation. The English began to create plantations in Ireland, often taking the land from the Catholic Irish and giving it to the Protestant British settlers (Moody & Martin, 2001, p.153). The mistrust and feelings of betrayal resulting from the colonization by Protestant settlers were further aggravated by centuries of political and social segregation of Catholics and Protestants in all of Ireland. After the victory of William of Orange (the Protestant challenger who deposed the Catholic King, James II), laws were enacted by the all-Protestant Parliament of Ireland barring Catholics from all offices, land ownership, schooling, and other avenues leading toward wealth and education (Darby 1976, 4).

and the Irish Protestant Loyalists. These feelings have generated a strong sense of Irish-nationalism among the Catholics, resulting in a low-intensity armed conflict between the three entities. Outgunned and out resourced by the British troops deployed to Ireland, many Irish Nationalists resorted to irregular tactics and terrorism, spawning one of the most persistent terrorist organizations in existence: the Irish Republican Army.

2. History of the IRA.

J. Bowyer Bell has conducted detailed research and writings about the origins and development of the IRA. He suggests that the terrorist organization originated from a New York based Irish relief organization in the late 1800s. Comprised of Irish immigrants, the Irish Republican Brotherhood (IRB) initially provided financial relief for relatives still in Ireland. However, following the American Civil War, many Irish American war veterans decided to return to Ireland and attempt to reclaim Ireland from the British and Protestant Unionist. From the 1870s until 1916 the IRB terrorized the British forces and Protestant supporters with a campaign of bombings and assassinations. Their physical attacks were intended to intimidate the British from carrying out their loyalties to England. Striking fear into the British supporters, the IRB hoped to alienate them from the Irish population. Finally in 1916 Patrick Pearse, a beloved Irish icon, cultural zealot, and active member of the Supreme Council in the IRB, forever changed the face of the Irish resistance. In what has become known as the 1916 Easter Uprising, Pearse and a few thousand IRB supporters seized the city of Dublin, claiming from the General Post Office that the revolutionaries had formed a new Irish Republic. Once the British overcame the initial surprise of Pearse' success, they quickly surrounded the city and pounded it with artillery. With most of Dublin in ruin Pearse decided to surrender to the British with terms (Bell, 1974). "He sent the terms using a new title, the Commanding General of the Irish Republican Army, to the general in charge of British forces" (White, p.84). Pearse's terms transformed the Irish Republican Brotherhood into the Irish Republican Army. It is important to note that most of the Irish citizens in Dublin

did not support or approve of Pearse's actions. In fact many condemned him for the resulting ruin of the city; however, the subsequent acts taken by the British changed everything. The British executed Patrick Pearse, James Connolly, and many other IRB leaders and sentenced most of the active supporters to long prison terms. This stark British action negatively influenced thousands of Irish citizens, souring their perception of the British. Jonathon White suggests that Pearse had actually expected such a reaction by the British and hoped to incite Irish nationalism. He writes "Pearse was a romantic idealist who felt the revolt was doomed from the start but believed it necessary to sacrifice his life to keep the republican spirit alive" (White, 1990, p.84). Although the British thwarted the revolt, the subsequent 'martyrdom' of Pearse and brutal treatment of his fellow Irishmen actually increased the sympathy for the terrorist group. Pearce's action suggests that, from its inception, the IRA understood the potential power of the information environment. Subsequent tactics used by the IRA incorporated Pearce's approach: provoking a heavy response from the British and then appearing as though they are victims of British oppressive rule.

From 1916 until 1921 the British deployed regular army soldiers to Ireland to combat the IRA in what became known as the Black and Tan War. British soldiers, trained to conduct battle in World War I, were ill prepared to face the unconventional battle in Ireland. Many Irishmen viewed British forces as invaders, affording the terrorists safe havens and security from the British. Stalemated and exhausted from the violence, the British and Irish signed a treaty to partition Ireland in 1922. The treaty established a free Irish Republic consisting of the southern 26 counties. The six remaining northern counties, including the city of Belfast, formed Northern Ireland and remained under the control of Britain. Disappointed and betrayed by the agreement to divide Ireland, many 'die-hard' members in the IRA ignored the pact and continued fighting not only against the British forces but also the Free Irish forces in the southern Republic. This led to a costly Irish Civil War that continued sporadically until the 1930s. Tired of the seemingly endless violence, public support for the terrorists subsequently dropped. Public support for the group remained low throughout the

40s and 50s, despite continued attempts by the Official IRA to incite nationalistic feelings.

3. Sinn Féin and the Provisionals.

Sinn Féin, formed in 1905, is the oldest political party in Ireland and the only one with representatives in both political jurisdictions: Northern Ireland and the Irish Republic.[16] The party has always sought to end British rule on the island and maintains that the British have betrayed the Irish people. Gerry Adams serves as the current leader of Sinn Féin. Highlighting the organization's Marxist-socialist tendencies, he claims that "the Irish are victims of the social and economic system which is not geared to Irish interests but in the interests of foreign and native capitalists or in the military and strategic interests of a British government and its superpower allies" (Bell, p.53).

During the late 1960s as civil-rights issues sprang up all over in Northern Ireland,[17] many radical members of the IRA grew dissatisfied with the soft defensive path the organization was pursuing. This became evident in 1969 during the Protestant marches in Londonderry that ended in the battle of Bogside (explored later in this chapter). The IRA was ill prepared to fight the British forces and could not defend the Catholics from Protestant violence. As a result the most radical members splintered away from the IRA in 1969 and formed the Provisional IRA (PIRA). The PIRA established a hard stance, rejecting Northern Ireland as a British-imposed statelet and claiming that Northern Ireland's very existence denied the Irish people their right to national self-determination (Bell, p.52). Throughout this time most of the Catholics in Northern Ireland were

[16] BBC reported that Sinn Féin has 74 counselors, 18 Assembly members and two Westminster MPs in Northern Ireland and 62 counselors and one TD in the Irish parliament. The party's principal political objective is to end British rule in Ireland (BBC, History, 1999).

[17] In 1967 the Northern Ireland Civil Rights Association (NICRA) was set up and organized street demonstrations to lobby for civil rights. The Stormont (Irish) government branded the movement a front for the IRA and banned its marches. In October 1968 the RUC used heavy-handed tactics to disperse a Civil Rights Association march in Londonderry and in January 1969 a People's Democracy march was attacked. Tensions between Catholics and Protestants deepened and by August 1969 Catholics were being burned out of their homes and shot on the streets of Belfast (BBC, History, 1999).

unemployed and oppressed, especially the youth. The emergence of the PIRA, a new, more radical organization, appealed greatly to many Irishmen who had lost hope. Bell suggests that the PIRA offered the youth a vocation and a chance to change the situation affronting the Irish people. "The organization became their identity, their life" (Bell, p.82).

Sinn Féin serves as the political wing of the PIRA, providing the organization political representation. Although the two organizations are officially separate, Sinn Féin has often opened a path for the PIRA to indirectly negotiate with the British government. The political organization also enables the terrorists to voice their cause internationally. Gerry Adams met with US President Clinton in 1997, and in April 2003 he talked with Prime Minister Blaire and US President George W. Bush about the Good Friday Peace Agreement.

B. PIRA INFORMATION OPERATIONS TOOLKIT.

The PIRA, as a separatist terrorist organization, is attempting to forge a national identity and unite Ireland under Irish control. The PIRA leadership must have realized early on that their campaign against the British would be long (Laqueur, p.33). They appear to have learned from the drop of public support during operations from the 1930s to the 1950s, that there exists a threshold to the amount of violence the local populace will 'tolerate' and the international community will accept without losing public support. The PIRA understands that they must modulate the level of violence and the political significance of their targets so as not to provoke a massive governmental crackdown (Hoffman, p. 162). To achieve their goal, the organization has developed a 'long-war' strategy. A concept of operations focused on exploiting the perceptual domain to influence public opinion. The concept relies on information and information systems to influence the populace and hence to pressure the decision maker to negotiate and concede.

The PIRA's strategy involves a low-intensity war of attrition against British Army forces to simply wear out British commitment in Northern Ireland. PIRA active units attack targets with bombings, ambushes, sniping, and other forms of

direct attack, often attempting to intimidate British supporters or provoke a strong-handed response by the government. The PIRA strategy relies upon the response it provokes from the British government and the Irish Protestants. When the inevitable government persecution follows the terrorist attack, it draws attention to the group and allows the terrorists and their sympathizers to present themselves as victims. This increases public awareness and generates sympathy and financial support for the group (Wright, p.186).

In sum the PIRA effects-based operations in the physical domain are designed to generate a response in the physical domain. This physical response is then used to create an effect in the perceptual domain. To achieve this, the terrorists have several means available to translate the physical response into a perceptual effect. With decades of experience at their disposal, the terrorists skillfully select targets to generate the desired influence. They blend elements of IO into their operations to both enhance their attacks in the physical environment and to shape the information environment following the British response to their attack.

I. Different Audiences.

The Provisional IRA has developed several means to leverage the information environment and influence the four different audiences described by Wright in chapter III, including the opposing, uncommitted, sympathetic, and active audiences.

The opposing audience consists of several entities directly opposed to the goals of the PIRA.[18] Often the PIRA selects members of this audience (British soldiers, government representatives, and RUC police chiefs) as the primary target for physical attack. These physical attacks, which are relatively meaningless from a military or attritional point of view, are designed to provoke a counter-action that will have a major impact in the perceptual domain. By

[18] The Opposing audience includes the British government and armed forces in Ireland, the Royal Ulster Constablary (police), Protestant paramilitary groups and terrorist organizations such as the Ulster Defense Association.

targeting the active audience with physical attack, the terrorists minimize negative effects on other audiences, while maximizing the probability of violent response or oppressive legislation (Buettner,2001).

According to Wright, the uncommitted audience has two components: the general public of the country where the terrorists are operating and the international public. The majority of Irish Catholics and Protestants living in Ireland do not support the actions of the terrorists, yet are not fully in agreement with the policies of the British government. PIRA propaganda reaches the uncommitted audience primarily through channels of the mass media and Internet. Many of the PIRA pamphlets and local newspapers do not have a mass circulation; however the group does make a few of them available on the Internet.[19] The ideological appeal toward this audience is at a general level. The PIRA seeks to expose the British government as an oppressive and controlling state, disadvantaging Catholics and denying Ireland its unity. This opens the way for the terrorists to attack the credibility of the state and security forces, and to initiate a process that Tugwell calls 'guilt transfer', whereby the blame for the deaths, injuries, and destruction caused by the terrorists is put on the shoulders of the state. The PIRA actions provoke the deployment of more British security forces or the enactment of special legislation such as Internment; the terrorists present this legislation as oppressive and reactionary measures taken by the state. Hoffman contends that "one of the IRA's main aims in abandoning the February 1996 Ceasefire was to convince the British public that the government was to blame for the breakdown and thereby pressure the Prime Minister to grant favorable concessions" (Hoffman, 1998, p.147).

The sympathetic audience is comprised of those people, locally and internationally, who already have a broad historical or ideological sympathy with the terrorists' expressed political aims (Wright, 1990, p.77). The sympathetic audience provides the 'sea where the terrorists swim'. It must be cultivated and groomed with several different perspectives in order to address the rifts and

[19] An Phoblacht / Republican News is available from the Sinn Féin website.

differences in the audience. It is centered mainly on the Roman Catholics in Northern Ireland and the Irish Republic, but also includes Irish communities abroad such as Irish-Americans and Irish-Europeans. This audience helps keep the political debate on the terrorists' aims rather than on the violence. On a practical level, they provide food, money, or shelter to the active members; they also make up the majority of recruits into the organization. The PIRA portrays a savior image to the uncommitted and the sympathetic audiences, taking sides with the oppressed, disadvantaged Catholics living in Northern Ireland (Wright, 1990, p.91). Propaganda is aimed at exploiting the fact that Catholics living in Northern Ireland have gotten the bad end of the stick for a long time; the Protestant minority, supported by the British, controls the majority of the wealth in Northern Ireland. PIRA targets are often selected to mobilize the Irish community and they do so by appealing to the Irish Gaelic and Roman Catholic traditions and the hardships and oppression imposed upon them by the British. One such example involved the 1981 hunger strike in Maze prison. The PIRA used Catholic religious propaganda aimed at portraying Bobby Sands as Christ. "The iconography that they were using was of a dying Christ in the bosom of the Blessed Virgin Mary. People demonstrated wearing the prison shroud, putting on their heads the crown of thorns, which Christ had worn to Calvary. All of it was going to the very heart of Christian symbolism" (PBS, Frontline, 2003). The 1981 hunger strike is further examined later in the chapter.

The active audience is made up of those people who are actively engaged in or directly support violent actions, including those in prison. The IRA uses 'auto-propaganda' to target the active audience. The intent is to defend and protect active members from being exposed to British and Unionist propaganda. The members hear only information that is conducive to the IRA cause. The propaganda strategy attempts to "bind individuals to the cause through action, and, once they have traversed the line between legality and illegality, to keep them there" (Wright, 1990, p.140). The IRA often recites historical rally cries of fallen comrades to assist in this. A quote from Patrick Pearse, the leader of the 1916 Easter Uprising and a hallowed figure in the republican history, reads "any

Irishmen accepting anything less by one iota than separation from England is guilty of so immense an infidelity, so immense a crime against the Irish nation... that it would be better for that man (as it were certainly better for his country) that he had not been born" (Maloney, p.309). Figure 15 illustrates the PIRA audiences with the IO framework we developed in chapter III.

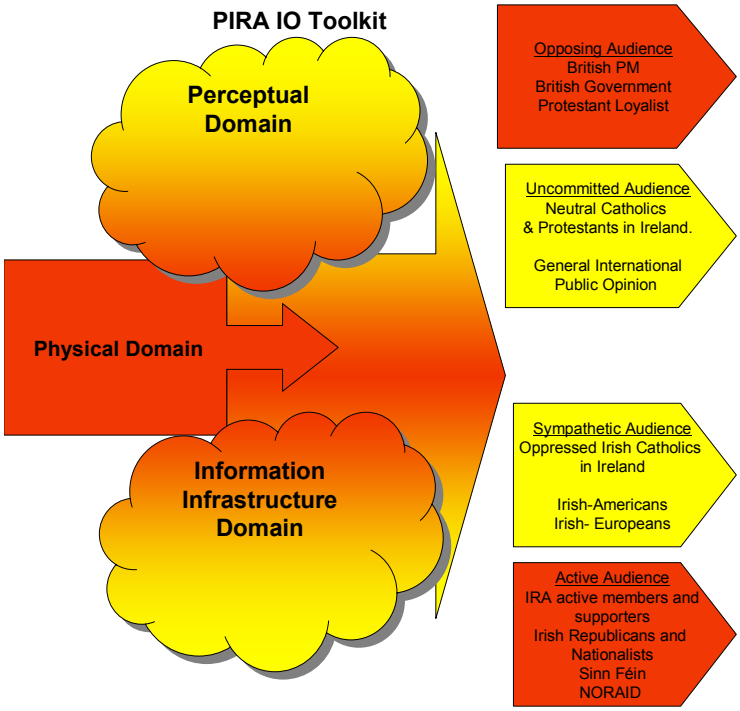

Figure 15. PIRA Audiences

2. Elements of the Toolkit.

The PIRA descended from a terrorist organization with nearly 100 years of experience. This section breaks out the elements of their tactics and techniques that we would call their IO toolkit. We provide evidence that the PIRA has evolved into a skilled practitioner of IO.

a. Psyops and Deception.

The PIRA often employs elements of IO tactically to assist in the execution of direct action missions. Operatives wear disguises and use proxies for intelligence gathering and infiltration/ exfiltration of active service units.[20] They use diversionary activities (explosions, shots, etc.) to draw British or Loyalist forces both away from PIRA operatives and toward ambushes (Gerwehr and Glenn, 2000).[21] Operatives skillfully conceal weapons, enabling them to get close to their targets.

The mortar attack on 10 Downing Street in London prior to the 1991 Gulf War illustrates the PIRA's use of deception to transport the weapons within range and the subsequent psychological operations to exploit the attack. On the morning of 7 February 1991, the PIRA moved a Mark 10 mortar concealed in a van to within 200 yards of the British Prime Minister's residence on Downing Street.[22] With a small section of the roof cut out of the van, it appeared normal to other drivers and people along the route. Bell describes the attack, "the driver parked, got out in the snow and jumped onto the rear seat of a waiting motorcycle. The short timer was running (1997, pp.623-624). Although the shells missed their mark, falling a short distance from Prime Minister John Major's residence, the attack had an enormous psychological impact on the British leadership and citizens at the height of the 1991 Gulf War. Hoffman adds that the attack "successfully elbowed the war out of the limelight and shone

[20] IRA volunteers operating in rural areas, wanting to blend in with the hedges, fields, and trees, could wear jackets, but they were not the gear for towns and villages. You had to blend in with the local population: you had to look like a mechanic, or a postman, or a bank clerk, not Fidel Castro (Gerwehr and Glenn, 2000).

[21] PIRA often employ deception in their operations. Operatives create a disturbance with the intention to attract attention. They would deliberately abandon their getaway car, setting an ambush with a hidden car bomb built into the dashboard. "The brown Mark 4 Cortina would be used as the getaway car. It would be abandoned with the aim of attracting a nosy bomb-disposal squad officer or policeman. If the glove compartment was opened, an electrical circuit would be completed which would detonate ten pounds of high explosives (Gerwehr and Glenn, 2000).

[22] The Mark 10 Mortar is constructed from three oxyacetylene cylinders and arranged on a rack with rubber collars at their base to cushion the recoil. The propellant, made from sugar and sodium nitrate, sends the projectiles in a predetermined arc; each one is packed with up to 40 pounds of industrial explosive.

renewed media attention on the terrorists, their cause and their impressive ability to strike at the nerve-center of the British government even at a time of heightened security" (p.182). An Phoblacht / Republican News and other IRA propaganda portrayed the government's inability to stop the attacks and protect their citizens.

In Northern Ireland, the terrorist leadership often staged marches, protests, and gatherings along the traditional Protestant marching routes or in parts of the city where Catholics and Protestants live in close proximity. Antagonists would create a civil disturbance to draw British forces into the area.[23] Once the British responded to the disturbance, active members then targeted the soldiers or incited them to respond with force. Often these deceptive events were staged with the intention to draw a heavy-handed response from the British. Bloody Sunday is named after the events that occurred on Sunday 30 January 1972, when British paratroopers shot dead 13 Catholics and injured 14 others. The killings took place in the predominantly nationalist city of Londonderry aka Derry to the Irish Republicans. The Northern Ireland Civil Rights Association (NICRA) had organized the illegal march to protest against internment and the ban on the right to march.[24] The PIRA induced and exploited the British physical response for perceptual purposes. Bloody Sunday strengthened local and international perception of the Irish as oppressed and deprived of basic civil rights. Additionally, the PIRA planned riots in Belfast near areas where Catholics and Protestants live in close proximity, such as the Falls Road (a Catholic area) and the Shankhill Road (predominately Protestant). These riots helped to fuel the hatred between the two communities (Bell, 1998, p.61).

[23] The Protestant 'Orangemen' have a marching calendar with two big annual events. On 12 July 1969 Orangemen commemorate the Battle of the Boyne in 1690 when the Protestant King William defeated the Catholic King James. The other big event is 12 August when Apprentice Boys march in Londonderry to commemorate the Siege of Derry in 1689 when local apprentice boys closed the city's gates against King James' army (BBC, History, 1999).

[24] The British government interned 'arrested' thousands of suspected IRA members during the 1970s. Many falsely accused suspects were jailed without trial or legal representation. The Internment, as it became known, caused great consternation among the Irish Catholics, further instigating IRA attacks and boosting recruitment.

The PIRA leaders also staged dramatic funeral processions to have a psychological effect. The funerals typically proceeded through Catholic neighborhoods to appeal to nationalistic feelings. Bagpipes, pallbearers clad in IRA uniforms, and militant ceremonial traditions create a mystical atmosphere, transforming the dead terrorists into heroes or martyrs, who died for the republic for a free and independent Ireland. The funeral procession for Bobby Sands and the other hunger strikers incited many Protestant communities along the funeral route. This example will be further explored later in the chapter.

b. Public Affairs, CMO and Propaganda.

Most terrorist organizations have recognized the importance of manipulating the media and 'spinning' a perception of the group that is favorable to their cause or detrimental to their opponents. Since its early beginning, the PIRA has been a master of propaganda.[25] The Provisionals distribute disinformation (by pamphlet, enhanced photo, radio and television broadcast, etc) to religious, cultural, civic, and military leaders in order to alienate the British and Loyalists from the noncombatant population (Gerwehr and Glenn, 2000). During the 1970s and 80s, the PIRA leaders often planned attacks (bombings or shootings) to take place in time for the evening television news. "One analysis of 60 bomb explosions in July 1974 showed that more than 80% of them were timed around four o'clock in the afternoon; this allowed maximum coverage on the television news" (Ulster Patriots, 2003). With the advent of 24-hour news, terrorists are able to carry out attacks and capture media coverage at any time.

Hoffman (1998) suggests that when the PIRA chose to abandon the February 1996 Ceasefire Agreement, the group's propagandists attempted to convince the British public that the government failed to meet the agreement and was to blame for the breakdown (p.147). In 1997, Henry McDonald, a BBC news correspondent in Northern Ireland from 1994-1996, highlighted the

[25] The British War Office noted in 1922 that Sinn Fein's mastery of publicity was unrivaled even then. "Sinn Féin's publicity department was energetic, subtle, and exceptionally skilled at mixing truth, falsehood, and exaggeration" (Laqueur p.44).

techniques of the PIRA's propaganda people. He reported that the PIRA and their apologists orchestrate a public relations campaign that imposes a 'politically-correct culture' on the reporting of both British and Irish news. It's a culture McDonald claimed "where the commentators and opinion formers blame PM John Major for resumed PIRA violence, rather than the PIRA itself" (McDonald, 1997). He contended that complaints had been voiced in Britain over the stranglehold exercised by Sinn Féin and the PIRA army council 'spin doctors' over the reporting in Northern Ireland.

The PIRA uses several different media to propagate their message; however the message theme is centrally controlled by the organization. All the Provisionals' statements and publicity is managed by the Army Council and then released to the media. There are several radio and television stations in Northern Ireland and the Irish Republic that are sympathetic to the PIRA and broadcast news and information with a republican point of view. The primary print media in Belfast is *An Phoblacht/ Republican News*.[26] The newspaper circulates in both Northern Ireland and in the Irish Republic. Electronic copies of the paper are also available on the Internet. The *Irish People* is a publication in the United States geared toward the Irish-American audience with a Republican spin (Bell, 1998, p.211). After cursory research, we discovered that the terrorists and sympathizers often exploit the Internet to distribute their propaganda through websites, chat rooms, and politically loaded newsletters (Internet Google search).

Sinn Féin, often referred to as the PIRA's propaganda machine, serves as the political voice for the organization. It is led by Gerry Adams, a former PIRA Belfast Commander. The political party provides the terrorists a legitimate public relations platform to the rest of the world. Sinn Fein maintains a dynamic website at http://sinnfein.ie, providing public affairs and perception management to local and international audiences.

[26] In 1979 the Republican News and An Phoblacht merged into one paper and relocated to 51-3 Falls Road in Belfast. The press center is equipped with the latest video and photographic technology and serves as a control center for republican news releases (Wright, p.78)

The Irish Northern Aid (NORAID) agency in America, while providing Irish-Americans a legal way to channel funds to the IRA, also serves as a distant network to propagate influential messages abroad. In Wright's book O'Ball quotes a NORAID spokesman in New York as saying "the more British soldiers who go back home in coffins the sooner it will be over" (Wright, 1990, p.161). The agency maintains a website on the Internet and produces several monthly publications. One of the primary themes of their propaganda is to discredit the British legitimacy in Ireland.[27] In 1981, NORAID placed an article in a New York magazine, announcing that many governmental and private establishments in New York had removed the British flag from view in protest to the handling of the PIRA hunger strikers. NORAID published the article in an effort to taint British legitimacy in the eyes of Americans. Subsequently, the *London Daily Telegraph* and *BBC* picked up the story and made it a front-page headline, reporting that British flags had disappeared due to Irish-American pressure. The stories incited demonstrators in London, which Lord Carrington finally had to call up police action to disperse (New York University, 2003). Other Irish nationalist publications also exploited the event. A headline from the *Irish People* read, "British Flag Down from the Mast" (22, August 1981). Although we could not find published evidence to support our assertion, it is our opinion that this action also contributed to the strong American reaction against the British treatment of the hunger strikers.

Irish-American associations have had a great impact on several aspects of American society, namely politics and entertainment. In the 1980s, Irish-Americans in Chicago influenced the City Council to intervene on behalf of the IRA. The City Council urged President Reagan to pressure PM Thatcher to concede to the demands of the IRA and stop the hunger strikes. Below is an excerpt from the Irish People.

> Be it resolved, that the Chicago City Council supports the demand of the political prisoners and strongly urges the British government to take the necessary action to prevent the tragic and disastrous

[27] NORAID publications often portray the Ulster Loyalists as obedient British puppets and tout the PIRA as freedom fighters and heroes (New York University, 2003).

> results of a hunger strike. In the name of basic human justice, we urge the British government to grant the political prisoners demands. (Chicago City Council, 21 February 1981)

IRA influences have also made their way into many Hollywood movies about the Troubles in Ireland. Nearly all the movies are made from the perspective of the Irish Nationalist, intended to either generate sympathy for the IRA's ongoing struggle for independence from Britain or draw attention to their cause.[28]

c. EW and CNO.

Although the electronic warfare capability of the PIRA is not technologically astute, the terrorists are very innovative when it comes to exploiting the electromagnetic spectrum. Early PIRA bombs were very crude and unreliable, often killing a large percentage of the PIRA bombers as they emplaced the devices. The PIRA decided to correct this so they created a bomb that would be emplaced and then subsequently detonated remotely using the remote control devises from hobby store planes and cars. During the 1980s British counter terrorist units countered PIRA remote-detonated bombings by jamming the electronic frequencies of the devises. The PIRA in turn produced a switching system, allowing the remote system to defeat the counter measure; which was again eventually defeated by the British. Persistently, the PIRA came back with a remote bomb that they could detonate using a radar gun and photographer's flash, which the British have yet to defeat (Hoffman, 1998, p.181).

Unclassified information about the PIRA's ability to employ computer network operations is difficult to find and warrants more thorough research. A cursory investigation led to several studies suggesting that the PIRA

[28] The Crying Game (1992) starring Stephen Rae; Patriot Games (1992) starring Harrison Ford & Sean Bean; Clear and Present Danger (1994) starring Harrison Ford & William Dafoe; In the Name of the Father (1993) starring Daniel Day Lewis; The Run of the Country (1995) starring Albert Finney and Matt Keeslar; Circle of Friends (1995) starring Chris O'Donnell and Minnie Driver; Braveheart (1995) starring Mel Gibson and filmed entirely in Ireland; Michael Collins (1996) starring Julia Roberts; Mary Reilly (1996) starring Julia Roberts; The Boxer (1997) starring Daniel Day Lewis; The Devil's Own (1997) starring: Harrison Ford & Brad Pitt; Bloody Sunday (2002) starring James Nesbitt.

is not capable of conducting damaging CNO at this time.[29] Rathmell, Overhill, Valeri, & Gearson's study, the *IW Threat from Sub-State Groups: an Interdisciplinary Approach*, concludes that there are a number of reasons why the PIRA may be reluctant to adopt CNO. They claim that CNO as a tactic is not consistent with the PIRA's 'macho' culture and self image. The PIRA's reputation espouses a perception of disciplined violence. They cite, "The Irish Republican movement places great store by, even glorifies in physical violence" (p.13). Secondly, they note that the sociological background and education level of the group is not conducive to use CNO. Finally, they argue that the PIRA would probably not 'contract-out' free lance hackers to do the work due to operational security. Security is of paramount importance to the PIRA survival, the terrorists are unlikely to risk their security unless the payoff is worth it. Their study suggests that the payoff is not there, yet.

Although not considered an aspect of CNO, the PIRA is more likely to use computer networks and advanced Information Technology (IT) to enable and enhance other aspects of their operations. Command and control, public affairs, and psychological operations are three such areas. Michele Zanini suggests that most active terrorist organizations are undoubtedly becoming more comfortable with advance IT. Terrorists routinely use cellular telephones and email to communicate. They gain enormous flexibility, enabling them to disperse their cells and overcome state boundaries that often create obstacles to communication and travel. Both active PIRA members and their sympathizers have established countless websites on the Internet, exploiting the world-wide connectivity of the Internet for perception management and propaganda. The Sinn Féin website at http://sinnfein.ie/ serves as the main PIRA internet site for public affairs and perception management operations (Arquilla & Ronfeldt, 2001, chapter 2).

In February 1997, British newspapers reported that the PIRA had launched a massive propaganda campaign over the internet, including

[29] The Naval Postgraduate School White Paper *Cyberterrorism* provides further evidence supporting the inability of the PIRA to employ dangerous CNO.

instructions on how to make Molotov Cocktails to maximize the effects during riots and various pointers on counter-intelligence, crafting false identifications, forging documents, and creating disguises (NYU, 2003).

d. OPSEC.

Secrecy and operations security are absolutely critical to the survival of a covert terrorist organization. The PIRA learned from experience that security originates from the organizational structure of the group. Initially the PIRA operated in 'Flying Columns', which were essentially structured like a normal hierarchical military organization. However, during what became known as the Kesh Prison Sting, the British conducted a covert deception operation, where they made the PIRA leaders believe they had been infiltrated. The success of the British deception was profound. The terrorists purged most of its top commanders and lieutenants and innovatively changed the predictable, regimented structure of their organization. This new cell structure greatly increased the terrorists' ability to operate securely and greatly diminished the British ability to infiltrate the organization. The PIRA emerged as a "smarter and more determined organization" (Bowlin, 1999, p.91). Figure 16 depicts the cell structure of the Provisional IRA.

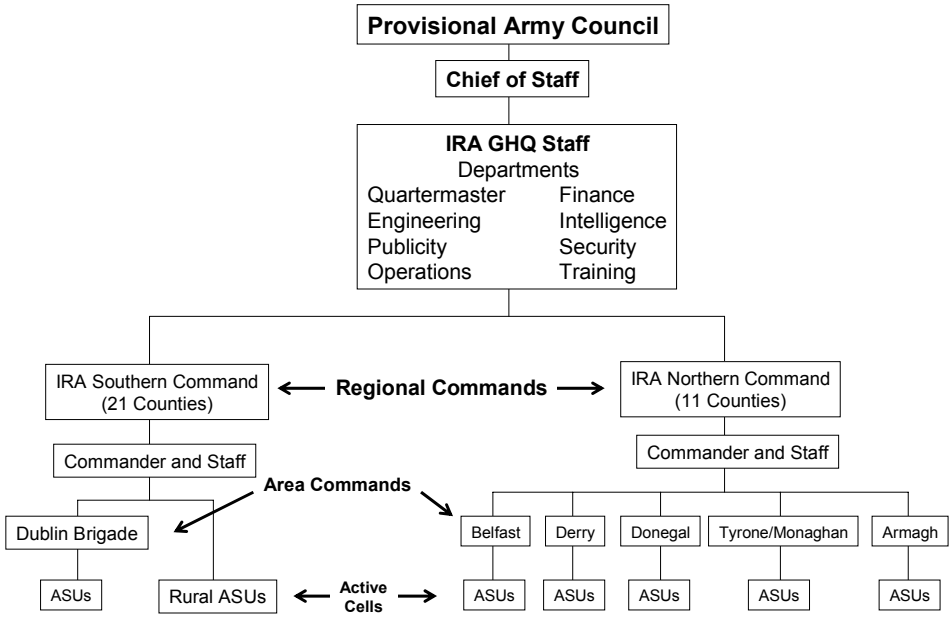

Figure 16. Provisional IRA Cell Structure by O'Brien, p.110

The PIRA compartments the inner core (PIRA Army Council, Chief of Staff, and GHQ Staff) of the secret army from the operational arms (Northern and Southern Commands). The Army Council, which is composed of seven men, authorizes, oversees, and initiates policy. The Army Chief of Staff and the commanders of the Northern and Southern Commands implement the policy directives. If a commander is arrested, a new one is immediately emplaced, which suggests that there is a pecking order among the leaders. The basic tactical Cell is called, the Active Serve Unit (ASU). Each ASU cell is comprised of four PIRA members and is controlled by the Brigade or Command in their respective area. "The cells are specialized into intelligence cells, sniping cells, executions, bombings, robberies etc" (O'Brien, 1993, p.109). The Brigades or Commands, not the cells, control the storage and movement of weapons and explosives. Covert and clandestine networks relay information, weapons, or other logistics to the ASU operatives as they near their targets. To further enhance OPSEC the Commands often order their cells to conduct operations outside their own area (O'Brien, 1993, p.109).

With the ever-present and highly technical British intelligence apparatus (MI5 and MI6) scouring Northern Ireland for possible leads on the terrorists, the PIRA depends greatly on operating in secrecy. Bell describes "secrecy as integral, not an aspect of operations" (1995, p.28). The PIRA has internalized OPSEC into a part of normal operating procedures. "A gunman's patterns' of life are changed, life becomes a cover, each word, and every reaction is adjusted. Cover is not considered a secret, not even a tradecraft, but a given" (1995, p.28). One of the more influential members, Danny Morrison served as the director of PIRA publicity. He was able to operate publicly under a legal and acceptable cover, even while he conducted covert and illicit support for the PIRA. He was finally arrested in Belfast for his involvement in the PIRA (Bell, 1995, p.37).

Lacking hi-tech solutions, the PIRA often relies on deception to assist in OPSEC. In June 1996, the PIRA attacked Crossmaglen, the British Army base in South Armagh. Being heavily fortified and guarded, the army base proved difficult to strike with the limited range of the PIRA mortars. The PIRA deceptively overcame this by concealing a MK-15 'Barrackbuster' mortar inside a hay bale. The hale bale was then placed on the back of a tractor to make a close-quarter attack on the base. The mortar was fired from a farmyard 150 yards from the base and hit a British Lynx helicopter as it landed to resupply the soldiers (Geraghty, 1998, p.196).[30] The mortar attack on 10 Downing Street in London also provides an example of deception enhancing PIRA OPSEC.

e. Intelligence.

Although Intelligence is not noted as a formal element of Information Operations, this thesis includes Intelligence as a vital enabler of IO. Without intelligence, it would be impossible to effectively attack or influence

[30] The MK-15 'Barrackbuster' was about 1 meter long and delivered more than 150 pounds of home-made explosive. The range was around 150 meters. The bomb was also used against police and army bases in Ballygawley, Newry and Osnabruck in 1996 (Geraghty, p.194).

targets. The PIRA has developed a far-reaching intelligence capability of passive and active gathers.

1. Passive Intelligence Gatherers. Bell suggests that the PIRA has established a huge intelligence network of passive supporters. He states, “their friends, neighbors, and contacts make up a huge intelligence net, a net in place of those conscious of movement priorities, those often alert, silent, working without trace…” (1998, p.196). This connection with the local populace allows the terrorists to measure the ‘pulse’ of the local audience. The PIRA is able to use the locals as a Measure of Effectiveness for the propaganda. This also allows them to tailor their attacks, so as not to inflict more damage than the public will accept. Additionally, the passive supporters provide a continual source of current information about British activity and unit locations. This information, although not always timely, is often enough to begin targeting a victim.

2. Active Intelligence Gatherers. When passive information gathering proves insufficient, especially when more information is needed on a specific target, underground leaders and decision-makers direct specific information gathering efforts in the form of active observation and surveillance (Bell, 1998, p.196). ASUs, insiders, and active members serving as spies often conduct active intelligence gathering. In the transition from passive to active information gathering, Bell notes, there are certain risks or costs assumed by the terrorist organization. First, the terrorist incurs a certain risk of exposure. Active observation may expose the nature of pending operations to the other terrorist members and the authorities as well. Second, the terrorist invites what Bell terms the “difficulty of precision,” the dangers associated with the relative lack of training and proficiency on the part of those tasked to conduct the surveillance (p.196). This places an unexpected burden on the terrorist organization. While most terrorist organizations are hampered in active observation by the relative lack of ability, many make up for it with creativity (p.200). As Bell points out, “what is impressive is that for those, ill trained or not,

who are absolutely dedicated, completely focused on particular targets, that so much useful can be found" (p.198).

An example of the IRA's intelligence capability surfaced in early 1979, when British and loyalist forces in Belfast initiated Operation Hawk, a major surveillance operation. The British employed highly sophisticated electronic equipment, covert agents, and thoroughly supported the operation with intelligence analysts to track key IRA suspects. In March of 1979, the operation received a lucky break when a Royal Ulster Constabulary (RUC) checkpoint stopped a car carrying Brian Keenan, a high-level IRA operations officer. More significant than Keenan's capture, however, was the discovery of his coded address book—a source that proved to be an intelligence windfall. In mid-June, based on analysis of Keenan's coded notes, the British and RUC raided three houses in the Belfast area. The raids were an eye-opener for the British (Bell, 1998, p. 197). To the authorities' amazement, the raid exposed a highly sophisticated terrorist intelligence operation. The Provisional IRA, it turned out, had been running its own surveillance on Operation Hawk and a number of other covert activities for more than six years. The Provos used military-style transmitters, specialized monitors, and even direction finding devices, all fabricated with components from Ulster Polytechnic and Grundig and Strathearn Audio (GSA) factories in Northern Ireland. IRA members in Belfast had also established wiretaps on several police telephones, which aided in thwarting police raids and gave them insight into future activities in the city requiring police assistance. The IRA even used equipment acquired from GSA to develop their own electronics factory, manufacturing sophisticated electronic devices and state-of-the-art radio detonators for IRA bombs (Bell, 1998, p. 198).

Figure 17 illustrates the PIRA's tactics and techniques, applied to the IO framework proposed in chapter III. Evidence indicates that the terrorists have developed significant capability in each of Waltz's information domains.

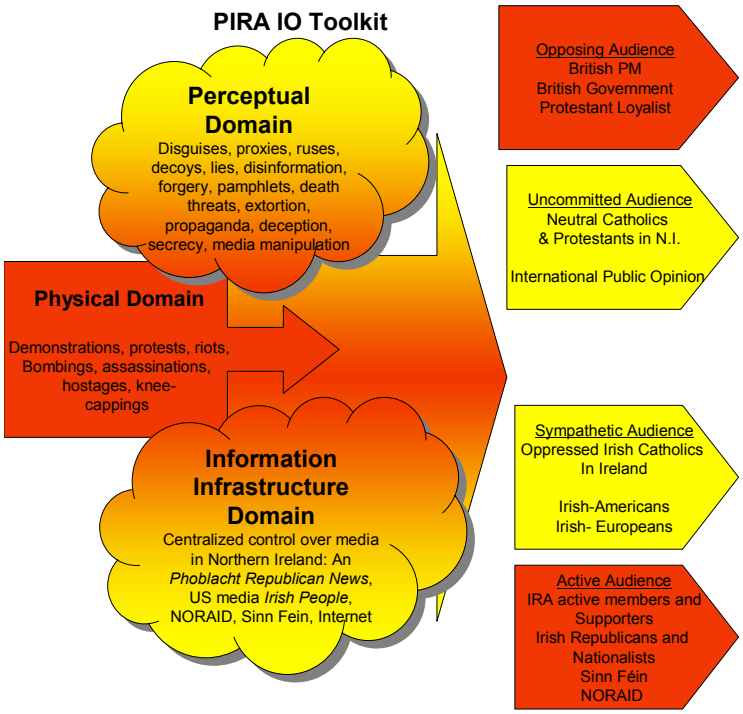

Figure 17. PIRA Toolkit and Audiences

C. BATTLE ANALYSES.

This section briefly examines three separate PIRA operations that occurred during the Troubles: the 1972 assassination of Lord Mountbatten and ambush of 18 British paratroopers; the 1981 Bobby Sands hunger strike; and the 1984 bombing of PM Margaret Thatcher. Using our proposed IO framework, this section examines the PIRA activities listed above to provide evidence of the group's use of IO. Before examining the operations, the section presents an introduction to the time period known as the Troubles.

The 1969 Battle of Bogside in Londonderry marks the beginning of the Troubles. Tensions between Derry Catholics and the RUC were high throughout the summer of 1969 as the annual Protestant Apprentice Boys March approached.[31] Sean Keenan, a PIRA veteran, knew that the Protestant marchers could be easily provoked into a fight. He created several 'street committees' with

[31] "The previous month Sammy Devenney had died from injuries he received when RUC officers battered him in his own home. As 12 August approached there was an expectation that the march would trigger unprecedented violence" (BBC, History, 1999).

seven other PIRA members. The committees then went about to plan for the defense of Bogside. “Plans were laid to erect barricades at strategic points and Keenan announced that people were to defend themselves with ‘sticks, rocks, and the good old petrol bomb” (Taylor, p.63). On 12 August, as the Protestants marched past the Catholic Bogside, an enormous crowd of Catholics converged, throwing rocks. The RUC intervened and, assisted by the Protestant marchers, charged at the nationalists. Within hours the rioting had escalated out of control. “The police were stoned and petrol bombed as they made their way in riot gear into the Bogside” (BBC, History, 1999). After 48 hours of continuous rioting the police were exhausted and British PM Wilson deployed troops to Londonderry. The British troops forcefully ended the riot, killing five Catholics.

During the Londonderry riots, the PIRA and the Irish Civil Rights Association called on Catholics to revolt in other areas of Northern Ireland[32] in order to pull RUC police and British soldiers out of Derry. “There was indeed some provocation by nationalists, since the strategy was to foment disturbances to draw police away from Derry” (Taylor, p.68). On 14 August in Belfast, several hundred Catholic protestors were struck with a massive Protestant backlash. During the ensuing mass clash of Protestants and Catholics, RUC police responded with heavy weapons (.30 Browning machine guns). Protestant crowds, shielded by British and RUC forces during the riots, emerged at night burning nearly 100 Catholic houses. As described by Bell, the aggressive and often one-sided British responses to these riots encouraged the PIRA to move from a defensive campaign to an offensive one. By employing strong-handed tactics to counter the disturbances, “the British Army largely transformed the rocks and riots of 1969 and 1970 into a very real, if low-intensity, war the following year, with snipers, car-bombs, shootouts in housing estates, and battles on the border” (1997, p.378). During the riot in Belfast, Patrick Rooney, a nine-year-old Catholic boy was hit and killed as he slept in his bed. The RUC bullet had passed through two walls of the house before striking him in the head.

[32] Rioting broke out in Strabane, Lurgan, Dungannon, Coalisland, Newry, and most seriously, Belfast (Taylor, p.68).

“From that day forth, the Protestant onslaught entered nationalist folk history as the pogrom:” full scale sectarian terror (Taylor, p.69).

1. 1972 Lord Mountbatten Assassination and Ambush of 18 British Paratroopers.

In August of 1972 the PIRA pulled off two very big operations: the assassination of Lord Mountbatten, Queen Elisabeth’s uncle and former viceroy to India, and the ambush of 18 British paratroopers along the border of Northern Ireland. This section provides evidence that both of these attacks did enable the PIRA to conduct subsequent activities in the information environment. The operations also suggest that the terrorists may select certain targets to influence specific audiences. The attacks were intended to directly influence the active and sympathetic audiences in order to strengthen the PIRA’s status among the competing terrorist groups. Evidence also suggests that the PIRA attempted to ‘spin’ the message to other audiences, but had little success in achieving influence. Figure 18 at the end of the section, illustrates the primary IO tools the PIRA employed, the target audiences, and the influence the terrorists leveraged.

On Monday morning, 27 August in Mullaghmore, the PIRA assassinated Lord Mountbatten as he “went out on his thirty-foot boat, Shadow V, with his fourteen-year-old nephew, Lady Brabourne, and a young boatman” (Taylor, p.265). The terrorists had planted a 50-pound bomb on the boat and detonated it remotely. Everyone aboard died in the blast. Since both boys and the lady were also killed during the operation, the PIRA received waves of negative publicity both locally in Ireland and internationally in Britain and the US. Nevertheless, the PIRA attempted to make the best of the attack. A Republican News article cited by Coogan had “…a photograph of Mountbatten with ‘Executed’ emblazoned across it, and a sneering half-page article signed by ‘the Brigadier’ described how the Queen took the news without a blink, merely informing the butler that ‘there would be one fewer for dinner’” (Coogan, 1994, p.361). Although the terrorist propaganda had little influence in the opposing and uncommitted audiences, Wright proposes that the intent of the target was to “produce inward-looking

propaganda" (p.161). She suggests that the assassination of Mountbatten by the Provisionals was designed to target active PIRA members and avid sympathizers. Several paramilitary groups within Ireland struggled to gain support from their perspective populations (Catholic or Protestant). Since the Irish National Liberation Army (INLA) also vies for Catholic support and had recently assassinated Airey Neave, a conservative Protestant politician within the House of Commons, the PIRA needed to trump their spectacle and gain the public's eye.

Only hours after the Mountbatten assassination, the terrorists ambushed a three-truck convoy of British paratroopers from the 2nd Battalion Parachute Regiment. The attack took place near Warrenpoint on the border with the Irish Republic and had been planned by the South Armagh Brigade under the direction of Northern Command (Taylor, p.296). "A typical ASU, acting on local intelligence, used a double-trap ambush: one explosive device was planted in a truck to hit the British convoy and another in the ground where the survivors would likely take cover" (Bell, 2000, p.229). As the convoy passed the truck, the PIRA remotely detonated the explosives, immediately killing six British paras and wounding several more. "The explosives, estimated to be half a ton, were packed in milk churns and triggered by a remote control from the IRA's vantage point across the water. The mechanism was simple: a radio transmitter" (Taylor, p.266). Under the fire of a PIRA sniper, the survivors of the blast ran for cover by the Gate Lodge of Narrow Water Castle. Only a few minutes later the second explosion ripped through the Gate Lodge, killing twelve more paras including LTC David Blair, the Commanding Officer of the Queen's Own Highlanders (Taylor, p.266).

The attack on the British paratroopers was also primarily intended to influence the active and sympathetic audiences. It was planned to avenge the deaths on Bloody Sunday when British paratroopers from the same regiment had gunned down 13 Catholic protestors in Derry. Taylor writes, "To the Provisionals it was revenge for what the Paras had done on Bloody Sunday. A slogan soon appeared on the wall opposite Sinn Féin's HQ on the Falls Road in Belfast,

'Thirteen gone and not forgotten-we got eighteen and Mountbatten" (Taylor, p.267). PIRA propaganda also sent a message to the British government and army forces in the opposing audience. Highlighting their persistence and dedication to the cause, the terrorists portrayed the attack as a continuation of the endless low-intensity war of attrition against the British. British General Glover stated about the ambush, "arguably it was the most successful and certainly one of the best planned IRA attacks of the whole campaign" (Taylor, p.266).

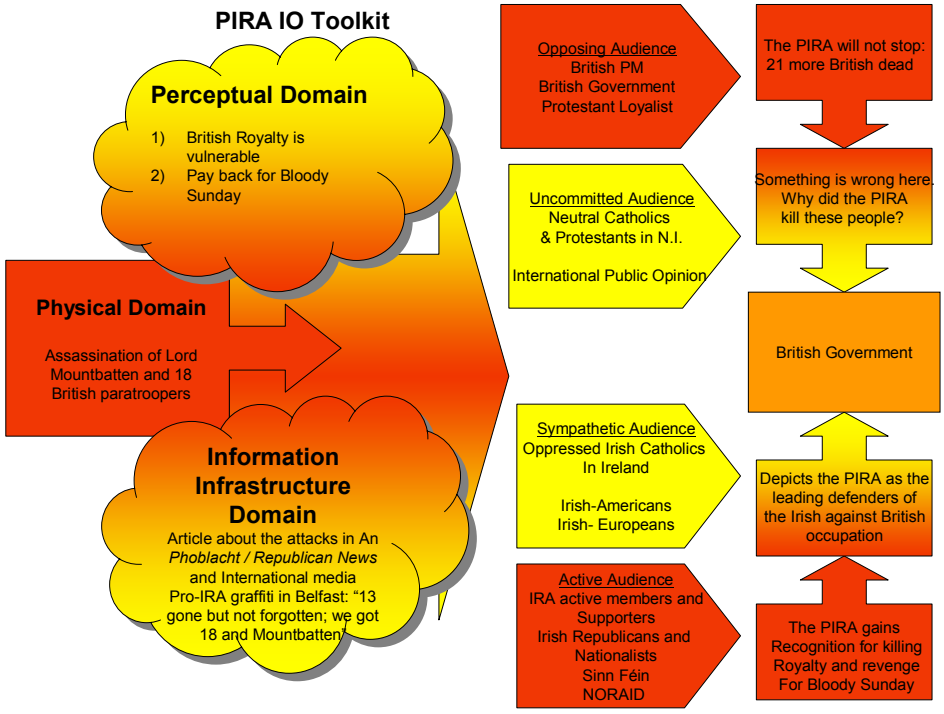

Figure 18. PIRA Mountbatten and British Paratrooper attacks

2. 1981 Hunger Strike at Maze Prison.

The 1981 hunger strike and deaths of ten PIRA prisoners in Maze prison had profound consequences for Northern Ireland and the British government. The conservative government under Prime Minister Margaret Thatcher took a hard, non-negotiable stance with the terrorists. PM Thatcher refused to talk to the terrorists under any circumstances. "Compromise was not in her vocabulary"

(Taylor, p.271). She refused to recognize the terrorists as anything more than criminals and denied them any concessions toward ending the strike. Her intransigence during the event provided the PIRA a platform from which they launched a propaganda war, transforming nine murdering terrorists into Irish icons. Bell asks, "how could the weak and criminal shape communication so that the legitimate and legal lost" (2000, p.210)?

This section provides evidence that the slow, painful death of Bobby Sands and nine other terrorist prisoners did enable the PIRA to conduct activities in the information environment. The section highlights the IRA's skillful use of perception management and propaganda to address multiple audiences, swaying not only local opinion in Northern Ireland and the Irish Republic, but also the opinion of the international community.[33] Peter Taylor quotes Gabriel Megahey, the PIRA weapons dealer in America, "the hunger strike had the effect of re-awakening an Irish American giant: an Anglophobic one" (p.10). The PIRA exploited the actions and inactions of the British government to achieve active support in the nationalist areas of Northern Ireland. After the deaths, political support for Sinn Fein dramatically increased in two elections (Northern Ireland and in the Irish Republic) transforming the party from a militant armed sect to a significant political force in Ireland.[34] Regionally, this surge in political support for Sinn Fein and the real threat that the party might overtake the Social Democratic and Labor Party (SDLP) as the main representative of the Catholic population in Northern Ireland, created great political pressure on PM Thatcher to intervene in Irish politics. As a result the British government signed the Anglo-Irish Agreement in 1985, granting the Irish republic greater political authority in Northern Ireland. Figure 19 at the end of the section, illustrates the primary IO tools the PIRA employed, the target audiences, and the influence the terrorists leveraged.

[33] The London Times reported "a survey of 73 newspapers around the world since Bobby Sands began his hunger strike on 1 March, showed the world opinion shifting toward the IRA" (Two killed in violence in ulster, Boston Globe, 1 June 1981, p.10).

[34] Support for Sinn Fein grew from zero to 13.4% of the whole vote inside Northern Ireland. They received up to 40% of the Catholic vote and seriously challenged the SDLP, the leading Irish party in Northern Ireland (http://www.pbs.org/wgbh/pages/frontline/shows/ira/conflict/hunger)

On 1 March 1981, Bobby Sands, the PIRA leader in Long Kesh 'Maze' prison, reinstated a hunger strike after the British breached an agreement to grant the prisoners special political status.[35] With no shortage of volunteers, Sands selected PIRA men, who geographically, represented the whole of Northern Ireland to join the second hunger strike. Aware of the uncompromising position of PM Thatcher toward terrorists, the PIRA skillfully exploited the agonizing deaths of Bobby Sands and the other terrorist members through an intensive perception management campaign. The PIRA selected the order that the prisoners would begin their strike at staggered intervals. Sands believed that this would incite maximum support for their cause and put pressure on PM Thatcher. As the hunger strike developed, it increasingly became a personal showdown between the 'Iron Lady' and the 'Iron Men' (Taylor, p.277). Sands refused to eat for 66 days, finally falling into coma and dying. Sands' death and the subsequent starvation of nine other PIRA prisoners became an international spectacle, capturing the attention of the world. "International interest in the hunger strike was intense. International media poured in from all over the world" (Moloney, p.209).

Sinn Fein, PIRA activists and supporters crafted an information attack using all three of Waltz's domains to influence major portions of all four audiences.

Bobby Sands exploited the physical domain by sacrificing himself for the cause. As his body deteriorated through his 66 day fast, finally falling into a coma and then death, Sands provided images (B-Roll) for the media. The images had long-lasting psychological affect on all audiences. For the active and extreme parts of the sympathetic audiences, "Sand's photograph, a flattering portrait showing a good-looking, long-haired youth, became a symbol of revolution" (Moloney, p.209). In Tehran a street was named after him, as was one in New York. For the uncommitted and opposing audiences his physical

[35] Special category or political status included five demands: the right or IRA prisoners to wear civilian clothes; the right to freely associate within a block of cells; the right not to do prison work; the right to educational and recreational facilities; and the restoration of lost remission of sentences (http://cain.ulst.ac.uk/events/summary.htm).

appearance served to protest against the treatment of PIRA members as criminals in prison; he saw his efforts other than criminal. The PIRA was able to exploit PM Thatcher's public statements stridently referring to the terrorists seeking political status as mere criminals. They were able to infer that she had absolutely no understanding of the Irish political psyche.

The PIRA exploited the information infrastructure domain through many sympathetic and uncommitted networked organizations such as: NORAID, Sinn Fein, and the US media. The Irish Diaspora (active and sympathetic audiences) all over the world became more committed to the nationalists' cause. "Demonstrations took place in New Zealand, Australia, Canada, and many cities in the US. In New York, NORAID supporters mounted a picket outside the British consulate on Third Avenue that lasted for years" (Moloney, p.209). International (uncommitted audience) interest in the hunger strike was intense. An article in the Chicago Tribune read, "Reagan should act on Ulster" urging the US President to take action against PM Thatcher (Chicago Tribune, 5 October 1981). After Cardinal Terence Cooke from New York appealed to PM Thatcher to end the hunger strike, an article appeared in the Chicago Tribune entitled "IRA brutalities, Terrorist propaganda triumphs". It reported that the IRA was winning a massive propaganda war in Northern Ireland with world opinion. The article read, "The IRA has done it. They have snookered not only Cardinal Cooke and much of the US news media, but nearly all Irish-American Catholics into backing their cause… they swallow IRA propaganda as if it were taffy" (9 May 1981)

The PIRA fought a war of perception and profoundly shaped the perceptual domain through the actions already mentioned in the physical and information infrastructure domains. The terrorists flew relatives of the hunger strikers to the US to make guest appearances on local and network television news and talk shows in New York, Chicago, Boston, and Philadelphia. The ten-year-old daughter of Joseph McDonald', one of the hunger strikers, appeared on Good Morning America to plead for Americans to help to save her daddy (NYU, 2003). The PIRA campaign successfully transformed the murdering terrorists, who had decided to kill themselves in protest, into martyrs, heroes, and

revolutionaries. The active audience gained cohesion from the event, rallying behind Bobby Sands; while the opposition British audience was ridiculed for its inhumane uncompromising actions. The uncommitted sympathetic audiences either 'swallowed the propaganda like taffy' and became actively sympathetic, or saw through the propaganda and became opposed.

Bobby Sands' funeral supplied the PIRA with their most spectacular propaganda opportunity. It was noted as the largest political demonstration in Irish history. Tens of thousands of nationalists poured in from all over Ireland to pay homage to Bobby Sands, the dead IRA man who rapidly assumed an iconic status (Moloney, p.209). The Provos organized monster demonstrations, parades, and posters; and orchestrated a symbolic funeral that successfully transformed Sands into an Irish Martyr (Bell, 2000, p.147). The PIRA actually built a grandstand for all the international photographers. At one point, CBS News had seven television camera crews in Northern Ireland reporting on the Hunger strike (PBS, 2003). In total over 100,000 people attended the funeral procession, which was led by a bagpipe and drum band with the coffin flanked by a black-clad guard of honor. The enormous funeral procession and ceremony was televised worldwide, broadcasting the event to millions of people. Newspapers, journals, and other publications added to the notoriety of the PIRA plight and English brutality. Poems and ballads enriched the already lengthy PIRA history, providing many new recruits and influencing international audiences for the Irish cause.

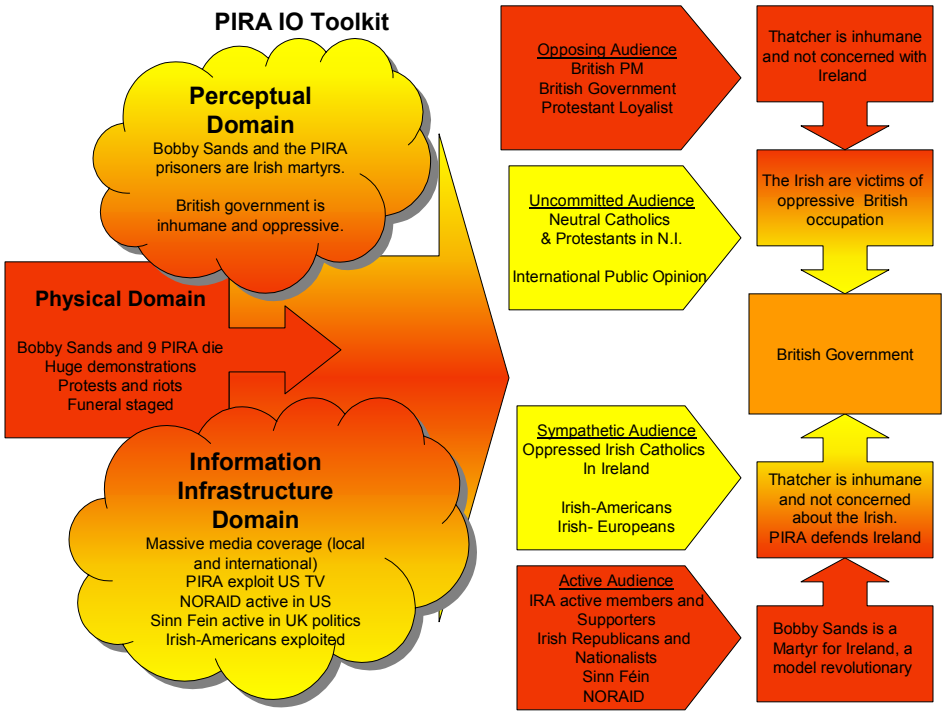

Figure 19. PIRA Bobby Sands hunger strike

3. 1984 Bombing of Prime Minster Thatcher.

In 1984, three years after the death of Bobby Sands, the PIRA attempted to get revenge. The terrorists planted a time-phase bomb in one of the walls inside the Brighton Hotel in London, where Prime Minister Thatcher and the heads of her conservative party were hosting a convention. This section provides evidence that the attack did enable the PIRA to conduct subsequent activities in the information environment. Evidence further suggests that the terrorists may select certain targets to influence specific audiences. Although PM Thatcher narrowly escaped being blown up, the PIRA skillfully exploited the story with propaganda and 'spin'. By taking the attack to the UK mainland, the terrorists specifically targeted the opposition and uncommitted audiences in Britain. PIRA propaganda attempted to blame PM Thatcher for the attack, promoting "what the British government and British people have to realize is that

what they are doing leads to this type of action" (Wright, p.94). Figure 20 at the end of the section, illustrates the primary IO tools the PIRA employed, the target audiences, and the influence the terrorists leveraged.

On 12 October 1984, the PIRA attempted to assassinate PM Margaret Thatcher at a Conservative Party convention in the Brighton Hotel. Although the attack failed to kill PM Thatcher, the deceptive bomb emplacement, technological ingenuity, and audacious target selection captured international media attention and moved the terrorists again into the spotlight (McGuire, 1973, p.62). The terrorists deceptively hid the bomb inside a wall next to PM Thatcher's room several weeks before the convention. The patchwork on the wall successfully concealed the bomb during the sweep by the British security team. The PIRA incorporated a detonation timing devise powered by a computer microchip, making the bomb less detectable and the detonation time extremely accurate. The attack provided the PIRA a platform from which to launch a very effective propaganda attack.

After the bomb detonated and the London press reported that PM Thatcher was alive but severely shaken, the PIRA exploited the physical attack with intense propaganda. A*n Phoblacht/Republican News* and other nationalist media in Ireland quickly picked the story up and provided a PIRA perspective. Directly targeting the opposing audience, the terrorists publicly warned Mrs. Thatcher and all other government officials through several news media. An article from the *Manchester Guardian International* on 21 October 1984, read, "today we were unlucky, but remember that we only have to be lucky once- you on the other hand will have to be lucky always" (Hoffman, p.182). The propaganda portrayed the vulnerability of the British security system in the UK and the determination of the Irish terrorists. PM Thatcher's 'political weight' ensured that the international media headlined the story, broadcasting the event to the rest of the world. Bell describes the IRA's influence on the opposing audience, "In Britain no cabinet member can open a hotel room door without recalling the bomb that nearly killed PM Thatcher, or drive into the parking lot at Westminster without realizing that there too a bomb went off- and killed Airey

Neave, Thatcher's representative Tory for Northern Ireland" (Bell, 1995, p.36). In an attempt to influence the perception of the sympathetic audience toward Britain, Sinn Fein blamed the attack on the British government and its continued oppressive occupation of Ireland. Gerry Adams publicly described the attack as "an inevitable result of the British occupation of the six counties" (Wright, p.94). Finally, the PIRA influenced the active audience with two primary messages. First the attack was presented as direct revenge on PM Thatcher. Many of the nationalists still held her solely responsible for the death of Bobby Sands and the hunger strikers in 1981. Second, the PIRA successfully struck the Prime Minister on UK soil. The audacity of the attack strengthened the terrorists' image, emboldening the members' belief in the organization and gaining the respect of other paramilitary groups.

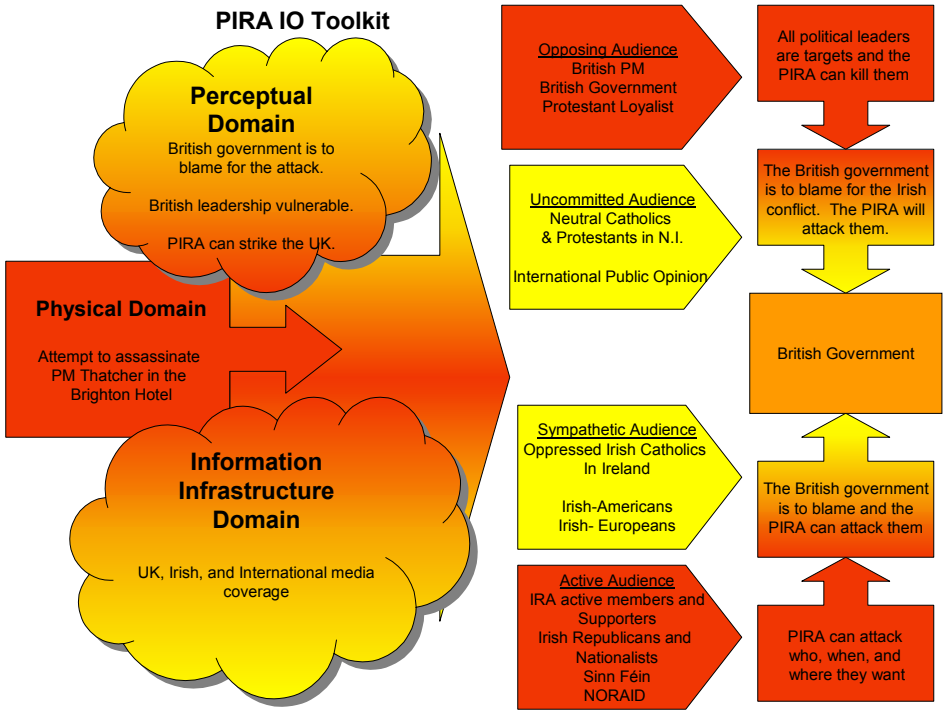

Figure 20. PIRA Assassination attempt on PM Thatcher

D. CONCLUSION.

1. Synopsis.

This chapter introduced the Provisional Irish Republican Army, a direct descendent of the Official IRA, an existing organization with decades of knowledge and experience. The brief historical overview developed a general understanding of the (Catholic-Protestant) sectarian violence and the deep-rooted hatred that many Irish Catholics have toward the British. The chapter presented the constraints and opportunities facing the PIRA operating in Ireland. Local and international opinion has created the need to moderate the amount of violence, and the terrorists apparently have successfully determined the threshold of violence that is acceptable. Since the PIRA is no where near military parity with the British, they rely heavily on actions in the information environment to achieve their objective. The terrorists' goal of re-unifying Ireland under Irish control is based on their contesting the existence of Northern Ireland. They claim that "the British guaranteed Northern Irish entity denies the Irish people their inalienable right to national self-determination" (Wright, p.227). In all aspects of PIRA propaganda the dominant theme is to portray Britain as the single and root cause of all the problems in Ireland (Wright, p.216).

2. IO Toolkit.

Evidence from the chapter suggests that the PIRA have developed a fairly diverse IO toolkit containing many of the principle elements of IO discussed in chapters II and III. The terrorists skillfully blend elements of IO into their tactical operations to help overcome British intelligence and counter-terrorist defenses. Sinn Féin is quite possibly the greatest PA / propaganda asset available to the terrorists for achieving political negotiations. Gerry Adams has legally represented the terrorists' goals and motives in negotiations with Protestant and British leaders, including British Prime Ministers. He has also entertained international leaders such as US President Clinton and George W. Bush. The front organizations such as NORAID and the Irish-American associations provide

the group direct access to the US populace and often generated sympathy for the PIRA movement. With the advent of the Internet, many legal media outlets for the PIRA (An Phoblacht, Irish Times, Irish People, etc.) have the ability to distribute their messages world wide.

3. Information Environment.

Although the PIRA's toolkit appears well-equipped, evidence suggests that they may have an even more profound understanding of the information environment. The chapter examined how the terrorists managed to 'spin' their messages to influence multiple different audiences (opposing, uncommitted, sympathetic, and active). The perceptions of each audience varied and was shaped by applying the right mix of influences in the information domains (physical, information infrastructure, and perceptual).

The Mountbatten and Thatcher operations primarily targeted the opposing audience. Oftentimes, the PIRA selected people in the opposing audience as targets specifically for the influence that their death or near death will bring about. The targets were selected to intimidate, provoke, and destabilize the audience opposing the terrorist organization.

The PIRA's operations during the civil-rights protests in the 1970s and subsequent defense of the Catholics after the Battle of Bogside, primarily targeted the uncommitted audience. The terrorists' goal was to portray PIRA as the defender of the Catholics in Northern Ireland, who were being persecuted by the Protestants and the British. The more the PIRA could force increased British and RUC responses, both armed force and legislation/policy, the more they could claim the state as oppressive and in crisis. "The provos have been waging a sectarian campaign which knows no off season and which is calculated to bring violent reaction from loyalists" (Wright, p.101).

Although the Sands' operation influenced all four audiences greatly, it dramatically affected the sympathetic audience. The broad propaganda themes directed at the sympathetic audience was intended to rally increased support for

their cause, making the ‘sea’ of sympathizers as deep as possible. By portraying themselves as political prisoners, the PIRA prevented the public from perceiving them as criminals. The terrorists presented the British uncompromising actions as wrong and unjust and thereby portrayed British presence in Ireland as wrong and unjust. Sinn Féin represented the terrorists as a popular political force in Ireland, and served as the primary conduit to the sympathetic audience. Gerry Adams appealed mainly to the “Roman Catholic communities in Belfast, Londonderry, and the border areas” (Wright, p.118).

The ambush of the 18 British paratroopers, the mortar attack on PM Major’s residence, and the Brighton bombing of PM Thatcher appealed greatly to the active audience. All three attacks attempted to avenge the deaths of PIRA members and supporters by directly striking out against British targets on UK soil. PIRA propaganda themes targeted the active audience in an attempt to isolate them from the rest of society. It attempted to reinforce the volunteers’ morale by leveraging the groups’ ethnic and religious background to counter British propaganda and by reiterating the inevitability of victory. Often the audacious attacks and advanced technology appealed to potential recruits (Wright, p160).

VI. CONCLUSION

Al-Qa'ida's attacks on September 11th shook the US from its post-Cold War slumber and introduced a new asymmetric threat to its interests and security within its borders. Nichiporuk and Builder (1995), leading Rand analysts, forecasted this new threat in his book *Information Technologies and the Future of Land Warfare*. They suggest that non-state actors may well be the enemies of tomorrow, not conventional military forces from nation-states. Nichiporuk and Builder suggest that the information revolution is changing the nature of conflict, and contends that

> "even though the revolution is a technological one, the changes it will bring to warfare will not be mostly in the form of new technology. Instead, it is altering the actors on the stage, the audience that can watch, and hence, the objectives of conflict. Non-state actors are seeing their relative strength on the international stage increase. They will certainly not be able to militarily challenge nation states on equal footing, but they also will not challenge a nation-state in the same way that another nation-state would" (p.83).

Understanding how this terrorist threat exploits information to influence US policy and decisions is crucial if the US hopes to combat this foe in the information environment. The purpose of this thesis is to analyze the use of Information Operations by two different terrorist organizations and determine how they employ Information Operations to achieve their strategic objectives. Evidence from the study suggests that terrorists, by design, rely upon an information strategy to achieve their objectives. They lack military parity with the state and therefore cannot rely upon physical attacks to achieve their objectives. The physical violence from terrorists is the most obvious form of influence they wield against states. Terrorists use this overt violence to enable operations in the information environment because they lack resources and military parity. Terrorists use IO as a force multiplier to overcome this parity and challenge a state. In this manner Information Operations serves as the supported activity to achieve the terrorists' objectives.

A. SYNOPSIS.

The thesis constructed an argument that an IO perspective has a great deal of explanatory power when examining terrorist operations. The study established this argument through a logical process. First, it integrated a generally accepted IO theory and military doctrine to form a fundamental framework. Second, the study incorporated the application of IO elements used by terrorists with the framework, developing the IO framework to be consistent with the terrorists' tactics, techniques, and procedures. Third, the thesis applied the IO framework to two different terrorist organizations as evidence that this perspective is indeed appropriate. This section provides a synopsis describing how we constructed our argument and serves to segue into the conclusions of the thesis.

1. Basic IO Framework.

Terrorist organizations do not maintain publications on how to use IO nor do they typically recognize IO as a concept of operations. Thus, the thesis explored US military doctrine and Edward Waltz's IO perspective to establish a fundamental understanding of IO to be applied to terrorist organizations. US doctrine prescribes the principle elements of IO used in the study: PSYOP, Deception, OPSEC, EW, CNO, PA, and CMO. Doctrine provides historical evidence that these elements, when incorporated into a strategy, create a synergy and can profoundly influence human decisions and actions. Next, the thesis examined Waltz's perspective of IO, first by providing an explanation of the role of information in conflict and then by exploring the three conceptual domains in his operational model of IO activities. Waltz's information models established a fundamental perspective, illustrating how elements of IO can shape the domains of the information environment and influence an adversary's perception and decisions in conflict. Figure 21 illustrates how the thesis incorporated the principle elements of IO from US doctrine into Waltz's fundamental perspective, producing a useful framework to explore terrorist organizations.

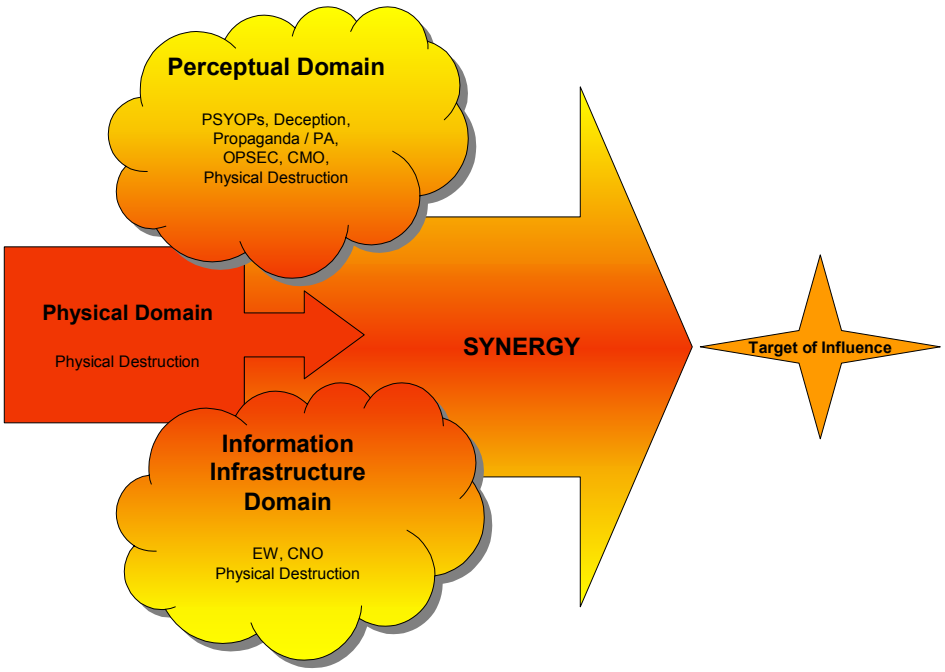

Figure 21. Basic IO Framework

2. Terrorist IO Framework.

Since terrorist organizations are illegal and covert organizations by nature and are likely to approach IO differently than the US military, the thesis further developed the framework in order to explore the terrorist case studies. To accomplish this goal the thesis examined works by several well-known terrorist authors to highlight the asymmetries of terrorist organizations that can have an impact on how terrorists employ IO. By applying insights offered by J. Bowyer Bell into the internal and external security pressures facing terrorists, the thesis highlighted the dilemma most terrorist organizations face. Terrorists must remain underground, hidden from the state's counter terrorist forces, yet they must also emerge from the underground and overtly appeal to the state and population for legitimacy and respect. Terrorist use IO to overcome this dilemma. The thesis noted three primary factors that terrorists address in their approach to IO.

a. Destruction in the Physical Environment Enables Information Operations.

The terrorists' information strategy employs limited activities in the physical environment for the primary purpose of capturing the eye of the media and the attention of their target audience. The terrorists then exploit these physical attacks with PSYOP, propaganda, and other elements of their IO toolkit. Terrorist IO serves as the supported activity (the main effort), providing the terrorist the ability to influence the perception of the local and international public and the state's decision makers. The violent action serves as the supporting activity that enables subsequent actions in the information environment. Most terrorists realize that there is a threshold of violence that the population will tolerate and accept. If the physical attack causes too much damage, the terrorists risk alienating themselves from the public and possibly causing a massive crackdown by the state. This threshold of violence in the physical environment is precisely why terrorist IO is inverted to the US military's approach to IO. Unlike the military, the terrorists lack the resources and the ability to sustain actions in the physical environment, and therefore rely on success in the information environment, where the majority of operations occur. They cannot hope to degrade the state's military enough to generate concessions from the state. Rather, terrorists must attempt to subvert the states military strength by shaping the perception of the state's populace to support their cause an by pressuring the government to negotiate.

b. Offensive – Defensive IO.

Terrorist organizations integrate offensive and defensive IO naturally to overcome the legitimacy dilemma described earlier by Bell. Terrorists employ elements of IO defensively to remain covert and ensure the group is secure. Unlike the US military, which often employs elements of OPSEC and deception as minor considerations to an operation, the terrorists have incorporated these elements defensively as part of normal operating procedures. Offensively, the terrorists integrate elements from their IO toolkit to

exploit the activity in the physical environment. Offensive IO serves as a force multiplier in the terrorists' quest to gain respect and legitimacy. The terrorist must appear legitimate and powerful in order to negotiate with the state and gain support from the populace.

c. Audiences.

Terrorist organizations that understand the power of the information environment develop what we recognize as IO tools to exploit it. This is evidenced by the PIRA's advanced toolkit consisting of political, economic, and military capabilities. Terrorist organizations employ elements of their IO toolkit to leverage information and shape the perceptions of different audiences. The primary goal is to influence the specific audience in a manner that supports the terrorist's cause. Applying insight offered by Joanne Wright (1990), the thesis outlined the four audiences available to terrorist influence: opposing, uncommitted, sympathetic, and active. Figure 22 incorporates the four audiences into the IO Framework, illustrating the power held in the information domains to influence different audiences.

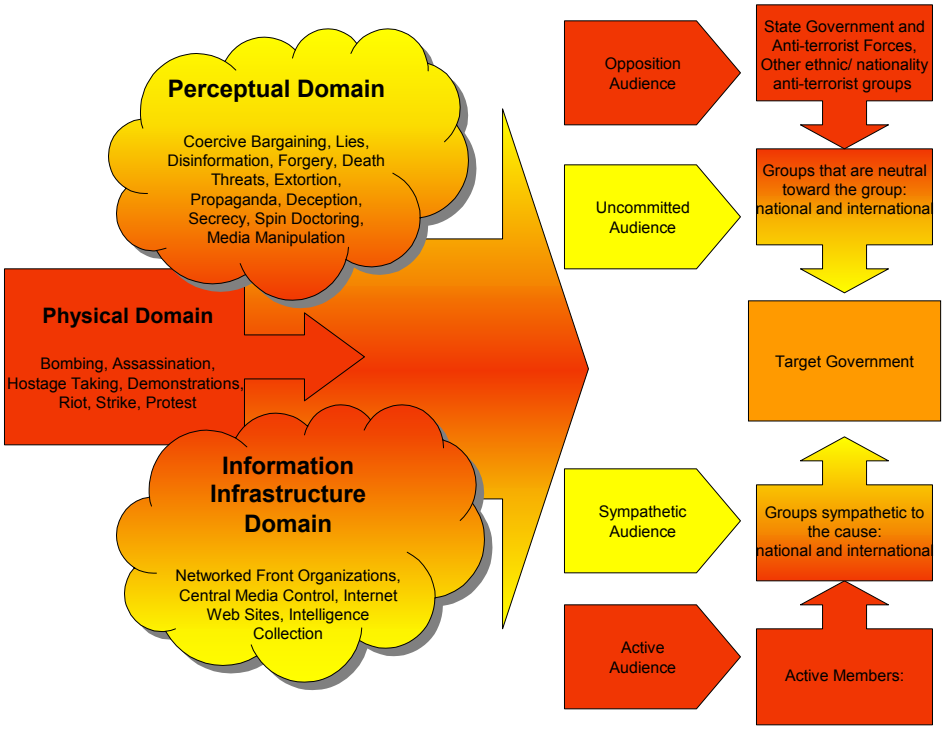

Figure 22. Terrorist IO Framework

1. Opposing Audience. Since members of the opposing audience are generally the hardest to gain support or sympathy from, they are optimal immediate targets for physical violence. Terrorist propaganda targets the opposing audience in an attempt to challenge the state's legitimacy and ability to provide safety for its citizens.

2. Uncommitted Audience. Through local and international media, terrorists capture the attention of the uncommitted audience and attempt to inform them of the terrorist's cause. Ultimately they attempt to convince uncommitted members that the state is evil and oppressive.

3. Sympathetic Audience. Terrorist propaganda attempts to gain support and backing from the sympathetic audience. The sympathizers often serve as safe havens for the terrorists and provide protection and intelligence for their operations. Most new terrorist members are recruited from the sympathetic audience.

4. Active Audience. Auto propaganda targets the active audience to ensure they remain committed to the organization. Active members are generally isolated from outside influences and hear only propaganda that supports the cause.

The terrorist's ability to target their message and successfully influence the targeted audience depends on the terrorist's intelligence network and the tools available in their IO toolkit. For effective targeting, intelligence about each audience is crucial to determine the cultural, political, and economic factors that are relevant to the audience. The intelligence network is generally comprised of active and sympathetic members living in the population. This network provides the terrorists a direct link to the populace and provides a way to measure the effectiveness of their information campaign. The terrorists IO toolkit provides the means to influence the different audiences.

3. Application of IO Framework to Terrorist Organizations.

The thesis adapted the IO framework to two terrorist organizations, Al-Qa'ida and the Provisional IRA, to provide evidence that the IO perspective is useful in analyzing terrorist operations. The study provided brief historical backgrounds, introducing the two non-state terrorist organizations. This was important to develop the goals, means, and operating environments pertaining to each group. The study then illustrated the IO tactics, techniques, and procedures of each group that made up their IO toolkit. Figure 23 illustrates the IO framework applied to Al-Qa'ida's 9/11 attack against the US and Figure 24 illustrates the 1981 PIRA hunger strike.

a. Al-Qa'ida Framework

Figure 23 illustrates the IO framework applied to Al-Qa'ida's attack against the US on September 11th, 2001. Chapter IV describes in detail how Al-Qa'ida employs elements of its IO toolkit to achieve influence in multiple audiences.

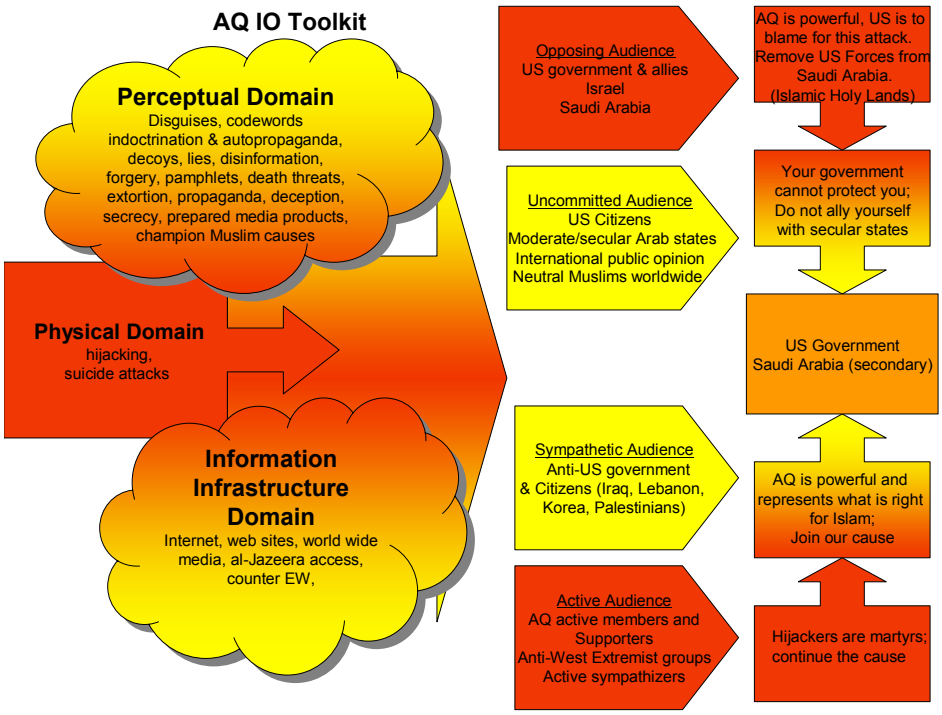

Figure 23. Al-Qa'ida's 9/11 IO Framework

b. PIRA Framework

Figure 24 illustrates the IO framework applied to the PIRA's 1981 Maze prison hunger strike. Chapter V describes in detail how the PIRA employs elements of its IO toolkit to achieve influence in multiple audiences.

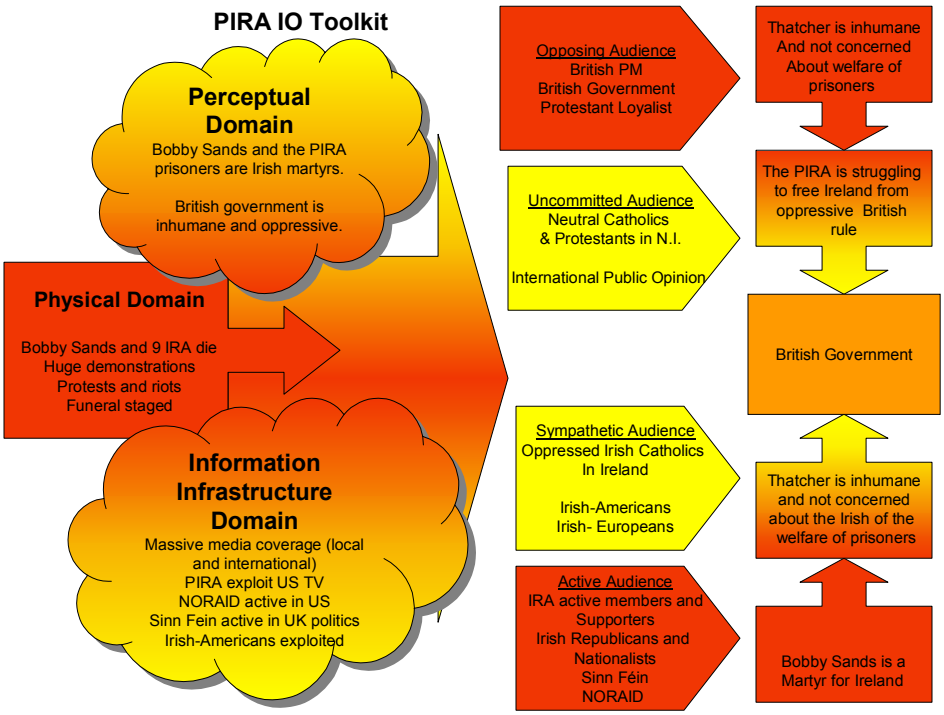

Figure 24. PIRA Hunger Strike IO Framework

B. CONCLUSIONS.

Terrorist organizations are militarily weaker than the states they face and cannot rely solely on physical attacks to accomplish their goals. Their covert, illegal nature forces them to engage in psychological warfare and drives them to using IO as their primary type of operation (a supported function).

Generally speaking, all terrorists employ elements of IO tactically to enable the success of their strategic operations. However, the terrorist's ability to manipulate information is a reflection of their understanding of the information environment and likely has direct influence on the IO toolkit they assemble.

Evidence suggests that terrorists rely upon an information strategy primarily because they don't have any other choice. Since they are not at military

parity with the state, they must attempt to subvert the state's strength by targeting its populace. However, as a terrorist organization nears military parity with a state or perceives it is nearing parity, terrorists may be likely to rely more on destruction in the physical environment as the supported activity and less on IO to shape the information environment. Terrorists may perceive themselves nearing parity through the inactions or impotence of state responses to their attacks. The operating environment and intense British presence in Ireland has prevented the PIRA from perceiving that they are nearing military parity with Britain. The terrorists therefore have continued to rely upon IO as the supported activity. Al-Qa'ida on the other hand, may have moved IO to a supporting role during their attacks on 9/11. Usama bin Laden's perception may have been shaped during the previous decade with impotent attacks by the Clinton administration. Perhaps he perceived he was invulnerable to US attack in the Hindukush Mountains, secluded in the Taliban safe haven. Usama bin Laden may have relied too heavily upon actions in the physical environment to gain his objectives.

By applying the IO framework to terrorist organizations, the thesis provided evidence that taking an IO perspective to terrorist operations is appropriate. The framework may prove useful in developing a new approach to counter-terrorism policy by showing how terrorist use IO and the extent of the synchronization of the individual elements, giving a sense of what use is deliberate or inherent. It is possible to develop a pre-emptive or minimizing counter-terrorism strategy based on the understanding of the influence process and terrorist strategy of minimal actions in the physical environment to gain maximum benefit in the information environment. A strategy could deny or degrade terrorists' benefits from their physical attacks or counter their intended influence of select audiences, essentially altering the environment the terrorist group needs to flourish.

C. AREAS FOR FURTHER RESEARCH.

As one of the first examinations of how terrorists integrate IO into their operations, this thesis merely opens the door to this subject. In doing so, however, it exposes a number of related subjects that require further study.

1. Terrorist target selection process.

This thesis highlighted the fact that terrorists often select targets for physical destruction in order to achieve influence in a particular audience. Further research may provide insight into this targeting process that terrorists use to select their targets, improving the effectiveness of defensive operations.

2. Application of IO Framework to Other Types of Terrorist Organizations.

Although we suspect our findings to be broadly applicable, further research is needed to apply the IO framework proposed in this thesis to other types of terrorist organizations such as religious sects, Leftist extremist groups, and Marist revolutionary movements. Additionally, we limited our case selection to only open-source unclassified sources. Since many aspects of Information Operations deal with relatively sensitive topics, there is presumably a wealth of information to be found from classified sources. Further research is needed to explore the classified holdings for more evidence supporting the IO perspective of analyzing terrorist operations.

3. Counter-Terrorism Strategy.

Further research using the IO framework proposed in this thesis could help to develop a pre-emptive counter-terrorism strategy based on the terrorist use of Information Operations to support their objectives. A strategy could focus on interrupting, delaying, denying, or degrading actions at critical points (i.e. physical attack, media use) in order to alter their operating environment. Alternately, specific actions in the information environment could be conducted address terrorist actions that have already occurred.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AQ-al-Qa'ida

CMO-civil military operations

CNA-computer network attack

CIA-Central Intelligence Agency

CND-computer network defense

CNE-computer network exploitation

CNO-computer network operations

DF-directional finding

DOD-Department of Defense

DDOS-distributed denial of service

DOS-denial of service

ETA- Bask Separatist Movement (Spain)

EW-electronic warfare

FARC- Revolutionary Armed Forces of Colombia

HUMINT-human intelligence

JP-Joint Publication

IE-information environment

IO-Information Operations

IR-infrared

IRA-Irish Republican Army

ISP-Internet Service Provider

IT-information technology

IW-information warfare

OPSEC-operation security

PA-public affairs

PE-physical environment

PFLP-Popular Front for the Liberation of Palestine

PIRA-Provisional Irish Republican Army

PLO-Palestinian Liberation Organization

PSYOP-psychological operations

RF-radio frequency

SIGINT-signal intelligence

SOF-special operations forces

UAV-unmanned aerial vehicle

UBL-Usama bin Laden

US-United States

WMD-weapons of mass destruction

WWW-World Wide Web

BIBLIOGRAPHY

Adams, J. (1986). The financing of terror. New York, NY: Simon & Schuster, Inc.

Adams, J. (1998). The next world war. New York, NY: Simon and Schuster, Inc.

Alexander, Y. & Latter, R. (Eds). (1990). Terrorism and the media. McLean, VA: Brassey's.

Alexander, Y. & Swetnam, M. (2001). Usama bin Laden's al-Qaida: Profile of a terrorist network. Ardsley: NY: Transnational Publishers.

Al Qa'ida (the base) (2003). [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Arquilla, J. & Ronfeldt, D. (2001). Networks and netwars. Santa Monica, CA: National Defense Research Institute, RAND.

Armistead, E. (Ed). (2002). Information operations: the hard reality of soft power. Washington D.C: National Defense University.

Attacks linked to al-Qaeda (2003, May 12). USA Today [Newspaper, article in archives]. Retrieved May 12, 2003, from the World Wide Web: http://www.usatoday.com/tech/world/iraq/2003-03-28-alaska-hack_x.htm.

BBC, History, (1999). History of IRA. Retrieved April, 10, 2003, from World Wide Web: http://www.bbc.co.uk/history/war.

Bell, J.B. & Whaley, B. (1991). Cheating and deception. New Brunswick, NJ: Transaction Publishers.

Bell, J.B. (1995). Dragonworld (II): Deception, tradecraft, and the provisional IRA. International Journal of Intelligence and Counterintelligence, 8, 21-50.

Bell, J.B. (1998). The dynamics of the armed struggle. London: Frank Cass Publishers.

Bell, J.B. (2000). The IRA: 1968-2000: Analysis of a secret army. London: Frank Cass Publishers.

Boaz, G. (15 July, 2002). Terrorism as a strategy of psychological warfare. http://www.ict.org.il/articles/articledet.cfm?articleid=443.

Bodansky, Y. (1999). Bin Laden: The man who declared war on America. Rocklin, CA: Forum.

Bomb explodes near U.S. forces in Afghanistan (2003, May 28). USA Today [Newspaper, article in archives]. Retrieved May 28, 2003, from the World Wide Web: http://www.usatoday.com/tech/world/iraq/2003-03-28-alaska-hack_x.htm.

Bowlin, M. (1999). British intelligence and the IRA: the secret war in Northern Ireland, 1969-1988. Monterey, CA: Naval Post Graduate School.

Brackett, D.W. (1996). Holy terror: armageddon in Tokyo. New York: Weatherhill.

Buettner, R. lectures 2001.

Buncombe, A. (2003, February 18). Al Qa'ida operative reveals code words. Received via email on June 2, 2003.

Campen, A. & Dearth Douglas H. (Eds.). (2000). Cyberwar 3.0: Human factors in information operations and future conflict. Fairfax, VA: AFCEA International Press.

CIA: al-Qaeda attacks likely to be small scale (2003, June 3). USA Today [Newspaper, article in archives]. Retrieved June 6, 2003, from the World Wide Web: http://www.usatoday.com/tech/world/iraq/2003-03-28-alaska-hack_x.htm.

Cialdini, R. (1991). Influence: the psychology of persuasion. New York: Quill.

Coogan, T. (1994). The IRA: a history. Niwot, CO: Roberts Rhinehart Publishers.

Crenshaw, M. (unk). The logic of terrorism. In W. Reich (Ed), Origins of Terrorism (pp. 7-24). Washington, D.C.: Woodrow Wilson Center Press.

Darby, J. (1976). Conflict in Northern Ireland: the development of a polarized community. Dublin: Gill and Macmillan.

Denning, D. (1999). Information warfare and security. New York, NY:ACM Press.

Denning, D. (2003). Lectures and various conversations.

Denning, D. & Baugh, Jr. W. (1999 Autumn). Hiding crimes in cyberspace. Information communication and society, 2.

Elliot, M. (2002, September 23). Reeling them in. Time, 29-33.

Fenton. J. (2003). Student's web site hacked by al-Qaida. Cybercrime News Archive [Newspaper, article in archives]. Retrieved June 1, 2003, from the World Wide Web: http://www.crime-research.org/eng/news/2003/04/Mess0906.html.

Fingel, Y. (2003, March 9). Falling into the al-Qaida trap again [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Gallagher, J. (1992). Low-intensity conflict: A guide for tactics, techniques, and procedures. Harrisburg, PA: Stackpole Books.

Ganor, B. (2002, July 15). Terror as a strategy [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Geraghty, T. (1998). The Irish war. Hammersmith, London: Harper Collins Publishers.

Gerwehr, S. & Glenn, R. (2000). The art of darkness: Deception and urban operations. Santa Monica, CA: RAND.

Hoffman, B. (1998). Inside terrorism. New York, NY: Columbia University Press.

Hoffman, B. (2001). Lessons of 9/11. Santa Monica, CA: RAND.

Howard, R. & Sawyer, R. (2003). Terrorism and counter-terrorism: understanding the new security environment. McGraw-Hill. Prerelease preview at http://www.mhhe.com/terrorism/ on May 16, 2003.

Hudson, R. (2002). Who becomes a terrorist and why: the 1999 government report on profiling terrorists. Guilford, CT: The Lyons Press.

Islamic hackers use student Web site to promote al-Qaeda. (March 23, 2003). USA Today [Newspaper, article in archives]. Retrieved June 1, 2003, form the World Wide Web: http://www.usatoday.com/tech/world/iraq/2003-03-28-alaska-hack_x.htm.

Jenkins, B. (1986). Is nuclear terrorism plausible? In Paul Leventhal and Yonah Alexander (eds.), The terrorism reader. New York, NY: Pergamon.

Jenkins, B. (2002). Countering al Qaeda. Santa Monica, CA: RAND.

Joint Publication 3-13. (9 October 1998). Joint doctrine for information operations. Washington DC: DoD Printing.

Joint Publication 3-51. (7 April 2000). Joint doctrine for electronic warfare. Washington DC: DoD Printing.

Joint Publication 3-53. (10 July 1996). Joint doctrine for psychological operations. Washington DC: DoD Printing.

Joint Publication 3-54. (24 January 1997). Joint doctrine for operations security. Washington DC: DoD Printing.

Joint Publication 3-57. (8 February 2001). Joint doctrine for civil military operations. Washington DC: DoD Printing.

Joint Publication 3-58. (31 May 1996). Joint doctrine for military deception. Washington DC: DoD Printing.

Joint Publication 3-61. (14 May 1997). Joint doctrine for public affairs . Washington DC: DoD Printing.

Ketcham, C. & McGeorge, H. (1986). Terrorist violence: its mechanics and countermeasures. In Neil C. Livingstone and Terrell E. Arnold (Eds.), Fighting back, Lexington, MA: Heath.

Khalilzad, Z. & White, J. (1999). Strategic appraisal: The changing role of information warfare. Santa Monica, CA: National Defense Research Institute, RAND.

Kramer, M. (unk). The moral logic of Hizzbollah. In W. Reich (Ed), Origins of Terrorism (pp. 103-130). Washington, D.C.: Woodrow Wilson Center Press.

Laqueur, W. (1999). The new terrorism: fanaticism and the arms of mass destruction. New York, NY: Oxford University Press.

Laqueur, W. (2001). The history of terrorism. New Brunswick, NJ: Transaction Publishers.

Lewis, B. (Nov/Dec, 1998). License to kill; Usama bin Ladin's declaration of jihad. Foreign Affairs Journal.

Lewis, J. A. (2002). Assessing the risks of cyberterrorism, cyberwar and other cyber threats. Center for Strategic & International Sudies, 2002, 1-12.

Liang, Q. & Wang, X. (1999). Unrestricted warfare. Beijing, China: PLA Literature and Arts Publishing House.

Libicki, M. (1995). What is information warfare? Washington, D.C.: U.S. Government Printing Office.

Moloney, E. (2003). A secret history of the IRA. New York, NY: W.W. Norton & Company, Inc.

McCormick, G. Lectures, 2002.

McDonald, H. (19 January 1997). How the BBC dances to an IRA theme. Sunday Times, London.

McGuire, M. (1973). To take arms: a year in the PIRA. London: Macmillan Publishers.

Merari, A. (Ed.). (1985). On terrorism and combating terrorism. Frederick, MD: University Publications of America, Inc.

Moody, T.W & Martin, F.X. (2001). The course of Irish history. Landham, MD: Roberts Rhinehart Publishers.

Nacos, B. (1994). Terrorism and the media. New York: Columbia University Press.

Nelson, B., & Choi, R., Iacobucci, M., & Mitchell, M., & Gagnon, G. (1999) Cyberterror Prospects and Implications. Monterey, CA: Center for the Study of Terrorism and Irregular Warfare.

New York University. (2003). Archives of Irish America. [Database posted on the Web]. Retrieved on 05 May 2003 from: http://www.nyu.edu/library/bobst/research/aia/.

Nichiporuk, B. & Builder, C. (1995). Information technologies and the future of land warfare. Santa Monica, CA: Rand.

O'Brien, B. (1993). The long war: the IRA and Sinn Fein: 1985 to today. Syracuse, NY: Syracuse University Press.

Orbach,B. (2001, December). Usama bin Ladin and al-Qa'ida: origins and doctrines. Middle East Review of International Affairs, 5, Retrieved May 06, 2003, from the World Wide Web: http:meria.idc.ac.il/journal2001/issue4/jv5n4a3.htm.

Paz, R. (2001, December 13). Programmed Terrorists [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm

PBS Frontline. (2003). The IRA and Sinn Fein [Archived database]. Retrieved April 07, 2003 from the World Wide Web: http://www.pbs.org/wgbh/pages/frontline/shows/ira/inside.

Radvanyi, J. (Ed.). (1990). Psychological operations and political warfare in long term planning. New York, NY: Praeger Publishers

Rathmell, A, Overhill, R, Valeri, L, & Gearson J. (1997). The iw threat from sub-state groups: an interdisciplinary approach. Strand, London: International Centre for Security Studies, Department of War Studies.

Ratnesar, R. (2002, September 23). Confessions of an al-Qaeda terrrorist. Time, 35-41.

Reich, W. (Ed.). (1998). Origins of Terrorism: psychologies, ideologies, theologies, states of mind. Washington, D.C.: Woodrow Wilson Center Press.

Robbins, J. S. (unk). Bin laden's war. In R. D. Howard & R. L. Sawyer (Ed.), Terrorism and counterterrorism: understanding the new security environment (pp. 358-366) McGraw-Hill. Preview chapter retrieved May 19, 2003 from the World Wide Web: http://www.mhhe.com/terrorism/sample_chap.html.

Robinson, G. E. (1997). Building a Palestinian state. Bloomington, IN: Indianapolis University Press.

Schwartau, W. (1996). Information warfare: cyberterrorism: protecting your personal security in the electronic age, 2nd edition. New York, NY: Thunder's Mouth Press.

Schweitzer, Y. (2001, June 28). Bin laden productions, ltd. [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Schweitzer, Y. (2001, October 12). Terrorism and Propaganda [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Schweitzer, Y. (2001, August 4). The "bin laden principle [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Snyder, A, Wendelken, K, and Wallace, D. (2003). IW class presentation. Monterey, CA: Naval Postgraduate School.

Taylor, P. (1997). Behind the mask: The IRA and Sinn Fein. New York, NY: TV Books, Inc.

Thomas, T. (2003). Cyber planning as a concept. Parameters, Spring 2003. Retrieved February 26, 2003, from the World Wide Web.

The Terrorism Research Center. http://www.terrorism.com/terrorism/def.shtml.

Tugwell, M. (1992). Revolutionary propaganda and possible countermeasures: an unpublished thesis. Department of War Studies, Kings College: University of London.

Tiboni, F. (2001, August). Info warfare may have averted bin laden attacks. Defense News.

Update: Investigation into the Bombing of USS Cole (2003, October 17). [Article posted on Web Site International Center for Terrorism]. Retrieved May 06, 2003, from the World Wide Web: http://www.ict.org.il/inter_ter/frame.htm.

Ulster Patriots. (2003). Propanganda war by Sinn Fein. [Article posted on the Web]. Retrieved on 03 April, 2003 from the World Wide Web: http://www.ulsterpatriots.50megs.com/Propwar.htm.

United States Army. (October 2002). Field Manual 3-13: Information operations. Washington DC: DoD Printing.

United States Army. (27 August 1996). (Approved final draft) Field Manual 100-6: Information Operations: Doctrine, tactics, techniques, and procedures. Washington DC: DoD Printing.

U.S. Embassy Kenya bombing: US vs Usama bin Laden et al., US District Court Indictment, S (9) 98 Cr. 1023 (LBS), 1998. Retrieved May 6, 2003 form http://www.terrorismcentral.com/Library/Incidents/USEmbassyKenyaBombing/Indictment/Start.html.

Vatis, M. (2001). Cyber Attacks During the War on Terrorism: A Predictive Analysis. Institute for Security Technology Studies at Dartmouth College.

Venke, B. & Ibrahim, A. (2002). Al-Qaeda tactic/target brief. Alexandria, VA: IntelCenter/Tempest Publishing, LLC.

Walcott, J. & Strobel, W. (2001, September 12). Officials suspect bin laden. Monterey County Herald. p.2.

Waltz, E. (1998). Information warfare: Principles and operations. Norwood, MA: Artech House, Inc.

Whittaker, D. (2001). The terrorism reader. New York, NY: Routledge Publishers.

White, J. (1986). Holy war: Terrorism as a theological construct. Gaithersburg, MD: International Association of Chiefs of Police.

White, J. R. (2002). Terrorism. Belmont, CA: Wadsworth Thomson Learning.

Wright, J. (1990). Terrorist propaganda. New York, NY: St. Martin's Press, Inc.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Superintendent
   ATTN: Gordon McCormick
   Defense Analysis Department
   Monterey, CA

4. Jennifer Duncan
   Defense Analysis Department
   Monterey, CA

5. 1st Information Operations Command
   Fort Belvoir, Virginia

6. Battle Lab
   ATTN: Information Operations
   Fort Leavenworth, Kansas

7. JCS Strategy and Policy
   ATTN: Deputy Director LtCol Hunigan
   6000 Defense Pentagon
   Washington D.C. 20301-6000

8. Principle Deputy Assistant Secretary of Defense (NII)
   ATTN: Dr. Linton Wells
   6000 Defense Pentagon
   Washington D.C. 20301-6000

9. National Defense University
   ATTN: Dan Kuehl
   Marshall Hall
   Washington D.C. 20319-6000