NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ON DECEIVING TERRORISTS

by

Benjamin I. Higginbotham

December 2001

Thesis Advisor:	John Arquilla
Second Reader:	Wayne Hughes

Approved for public release; distribution is unlimited

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
19Dec2001	N/A	-

Title and Subtitle On Deceiving Terrorists	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Higginbotham, Benjamin	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Naval Postgraduate School Monterey, California	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 205	

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	**2. REPORT DATE** December 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) On Deceiving Terrorists			**5. FUNDING NUMBERS**
6. AUTHOR(S) Benjamin I. Higginbotham			
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**

13. ABSTRACT ***(maximum 200 words)***

This thesis addresses the use of deception as one means available to states for dealing with terrorists. It begins by exploring the body of theoretical literature to establish the foundation necessary for a thorough discussion of deception. Next, the thesis examines the reasons for state use of deception in interstate conflict. From this list, three potential uses of deception against terrorists are suggested. Specifically, the thesis proposes that states use deception to create and exploit organizational inefficiencies and weaknesses in terrorist organizations, facilitate counter-terrorist operations, and conceal counter-terrorist capabilities and intentions. Subsequently, the cases presented herein reveal that states have in fact successfully used deception in the past with all three purposes in mind. Finally, this thesis also explores the often-overlooked subject of costs and risks, demonstrating that the use of deception is almost never without expense. Even when deception succeeds, its use inevitably incurs costs and opens the door to certain risks. Moreover, the study shows that deception—while both legal and ethical in the larger sense—might be illegal or unethical in certain applications. In the end, though, this thesis shows that deception is, indeed, a valuable tool against terrorists.

14. SUBJECT TERMS Deception, Special Operations, Terrorism, Counter-Terrorism, Intelligence, Counter-intelligence, Information Warfare			**15. NUMBER OF PAGES** 194
			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

ON DECEIVINGTERRORISTS

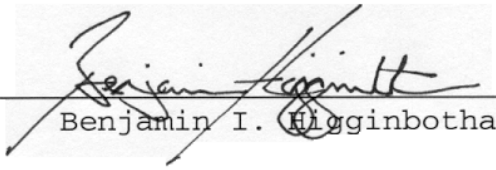
Benjamin I. Higginbotham
CPT, US Army
B.S., Texas A & I University, 1990

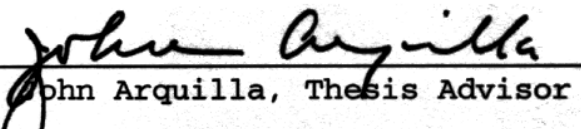
Submitted in partial fulfillment of the
requirements for the degree of

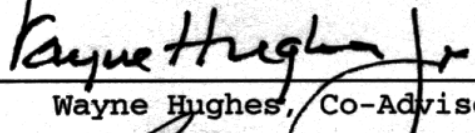
MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)

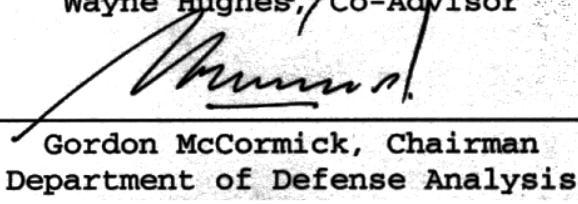
from the

NAVAL POSTGRADUATE SCHOOL
December 2001

Author: 
Benjamin I. Higginbotham

Approved by: 
John Arquilla, Thesis Advisor


Wayne Hughes, Co-Advisor


Gordon McCormick, Chairman
Department of Defense Analysis

ABSTRACT

This thesis addresses the use of deception as one means available to states for dealing with terrorists. It begins by exploring the body of theoretical literature to establish the foundation necessary for a thorough discussion of deception. Next, the thesis examines the reasons for state use of deception in interstate conflict. From this list, three potential uses of deception against terrorists are suggested. Specifically, the thesis proposes that states use deception to create and exploit organizational inefficiencies and weaknesses in terrorist organizations, facilitate counter-terrorist operations, and conceal counter-terrorist capabilities and intentions. Subsequently, the cases presented herein reveal that states have in fact successfully used deception in the past with all three purposes in mind. Finally, this thesis also explores the often-overlooked subject of costs and risks, demonstrating that the use of deception is almost never without expense. Even when deception succeeds, its use inevitably incurs costs and opens the door to certain risks. Moreover, the study shows that deception—while both legal and ethical in the larger sense—might be illegal or unethical in certain applications. In the end, though, this thesis shows that deception is, indeed, a valuable tool against terrorists.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1

A. THE TERROR WAR 1

B. THESIS OVERVIEW—SCOPE OF THE STUDY 7

C. KEY CONCEPTS 7

1. What Is Deception? 8

2. What Is Not Deception? 17

3. Why Deception Is Used 20

4. Why Deceive Terrorists? 25

D. WHERE WE GO FROM HERE—STRUCTURE OF THE STUDY . . . 27

II. HOW DOES DECEPTION WORK? 29

A. DECEPTION AS A SUM OF ITS PARTS 30

1. Simulation And Dissimulation 30

2. Negative And Positive Deception 35

3. Passive And Active Deception 36

B. DECEPTION AS A PROCESS—A MULTIDISCIPLINARY APPROACH 37

1. What Is A Multidisciplinary Approach? 38

2. Deception In Theory 42

3. Deception In Practice 45

C. WHY DECEPTIONS SUCCEED DESPITE DIFFICULTIES 49

D. DECEPTION SUCCESS FACTORS 52

1. Centralized Control, Coordination, and Integration 54

2. Intelligence 57

3. Adaptability and Feedback 60

4. Plausibility and Confirmation 62

5. Secrecy—A Fifth Success Factor? 64

III. DECEIVING TERRORISTS—ORGANIZATIONAL APPLICATIONS 67
A. INTRODUCTION 68
B. THE NATURE OF THE BEAST—BACKGROUND ON TERRORIST ORGANIZATIONS 69
1. The Difficulties Of The Dragonworld 71
2. Terrorist Intelligence Gathering 74
3. The Future of Terrorism—The Trend Toward Networks . . 83
C. DECEPTION TO CREATE AND EXPLOIT INEFFICIENCIES AND WEAKNESSES 101
1. The Prison Sting 102
2. Deception In The Philippines 106
3. The Abu Nidal Affair 110
4. Summary 115
IV. DECEIVING TERRORISTS—OPERATIONAL APPLICATIONS 117
A. INTRODUCTION—A REVIEW OF SCOPE AND METHOD 120
B. A THEORY OF SPECIAL OPERATIONS 121
C. DECEPTION TO FACILITATE COUNTER-TERRORIST OPERATIONS 124
1. Deception to Protect Counter-Terrorist Units and Missions 124
2. Deception To Create Counter-Terrorist Opportunities . . 132
D. DECEPTION TO CONCEAL CAPABILITIES AND INTENTIONS . 143
1. Capability And Intention Deception At Entebbe 144
2. Soviet Capability And Intention Deceptions 145
3. Summary 147
E. CONCLUSION 148
V. THE COSTS AND RISKS OF DECEPTION 151
A. COSTS AND RISKS OF DECEPTION 153

1. Deception Costs 154
2. Deception Risks 157
B. THE RIGHT AND WRONG OF DECEPTION 161
1. The Legal Status of Deception 161
2. The Ethical Status of Deception 164
C. SUMMARY 168
VI. CONCLUSION 171
A. SYNOPSIS 171
B. CONCLUSIONS 172
C. WHAT MIGHT FUTURE DECEPTION AGAINST TERRORISTS LOOK LIKE? 174
1. Scenario #1—Create Inefficiency In The Organization . . 175
2. Scenario #2—Exploit Security Shortcomings 176
3. Scenario #3—The Lightning Rod 178
4. Scenario #4—Deception As A Stand-Alone 179
5. Scenario #5—Going Hunting 180
D. AREAS FOR FURTHER RESEARCH 182
1. Terrorist Use Of Deception 182
2. Analysis Of Classified Cases Of Deception Against Terrorists 182
3. Empirical Analysis Of Deception Versus Terrorists 183
4. Legal and Ethical Status Of Deception Against Terrorists 183
5. Psychological Approach 183
E. PAST, PRESENT, AND FUTURE 184
LIST OF REFERENCES 185
BIBLIOGRAPHY 191
INITIAL DISTRIBUTION LIST 195

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE TERROR WAR

At 8:45 a.m. on 11 September 2001, a hijacked American Airlines flight crashed into the north tower of the World Trade Center. Eighteen minutes later, a United Airlines flight, also hijacked, crashed into the World Trade Center's south tower. The crashes set the buildings ablaze and dealt the towers a fatal blow; within two hours, both towers collapsed under their own weight. At about the same time, 230 miles away, another hijacked American Airlines flight crashed into the outermost wing of the Pentagon. Within half an hour, that portion of the Pentagon collapsed in flames. At the same time, a fourth hijacked airliner—another United Airlines flight now believed bound for a target in the vicinity of Washington, DC—crashed into the Pennsylvania countryside when passengers apparently struggled with hijackers. By 10:28 a.m., more than 3000 Americans were dead in a stunning series of coordinated terrorist attacks. Two of the most recognizable symbols of American economic and military power had either been reduced to rubble or were aflame. America found itself thrust into war.[1]

In many ways, this new war was—and remains—very different from the wars the United States has previously fought. Most notably, the United States found itself at war with a non-state actor, potentially a huge departure for a nation accustomed to thinking about war primarily in terms of inter-state conflict. This new kind of war confronted military and civilian decision-makers with a perplexing series of questions—questions for which there are no easy answers. How should the nation prosecute a war against an amorphous enemy who chooses not to face us in the symmetric, conventional manner to which we've become

---

[1] Times and details are drawn from "September 11: Chronology of Terror" [Article posted on the Web site CNN.COM]. (2001, September 12). Retrieved 23 October 2001 from the World Wide Web: http://www.cnn.com/2001/US/09/11/chronology.attack/index.html. Of course, Usama bin Laden publicly declared war on the US long before 11 September, and has been hitting American targets—the Khobar Towers, the African embassies, and the *USS Cole*—for some time.

accustomed? Is it simply a matter of sending aircraft carriers to sea, of finding the right targets to bomb with precision weapons, of applying our old way of thinking and forcing it to fit the new situation? Conversely, is a new strategy required? If so, what should that strategy be? How do we regain the initiative—to end this war in a time, place, and manner of our own choosing (to paraphrase President Bush)—if our old way of war doesn't fit?

Indeed, these questions are little different than those that have plagued men since the dawn of conflict. When faced with the perceived inevitability of armed conflict, military commanders and national leaders from Ulysses to Hannibal, and from Genghis Khan to Winston Churchill have faced a common dilemma: how does one achieve an advantage in war? The answer has varied with time and changing conditions. At times, superior strength has provided the decisive advantage. At other times, advantage has been found in superior technology, superior use of terrain, better-trained and prepared combatants, or superior leadership. These, however, have not been the only ways. Throughout the long history of military conflict, deception too has played an important role. Time and again, creative leaders have relied on stratagems in order to gain an advantage: to gain or maintain surprise; to create conditions favorable to achieving victory; or to reduce risks and costs of military action.[2] Deception has deep roots in interstate conflict and is much studied in that context; accordingly, there is much written on deception in war. There is relatively little written, however, on deceiving non-state actors. Does this mean that deception is limited to interstate conflict, or does it have a role in more unconventional forms of warfare as well?

In fact, there is considerable evidence to demonstrate that deception has played a significant role in past conflict between state and non-state actors—

---

[2] The term "stratagem," was first used in the 15th century and revived in the late 20th century by the eminent historian Barton Whaley, whose most notable work is Stratagem, an epic empirical analysis of the role of deception in warfare. A stratagem is alternately defined as "an artifice or

particularly terrorists and guerrillas.[3] As an example of this phenomenon, we need only turn to a fairly recent conflict—that between the British Army and the Irish Republican Army (IRA) in Northern Ireland. In 1974, the British Army found itself in the fifth year of a vicious campaign against terrorists. Direct military and law enforcement action against the IRA had failed to bring about either its defeat or the end of the conflict known as "the Troubles." Seeking a new tool to use in the ongoing conflict, the British reverted to a means that had proven useful in other, more conventional conflicts—military deception. The British "Prison Sting" in 1974-75 provides us an excellent example of deception skillfully and successfully executed against terrorists (see Figure 1).[4]

In 1974, the British army in Northern Ireland "recruited" two Catholic youths from Belfast—Vincent Heatherington and Miles McGrogan.[5] British intelligence (Special Branch, MI-5, and military intelligence) painstakingly trained and prepared the pair and subsequently inserted them into Belfast's Crumlin Road Prison on trumped-up murder charges. The duo's mission was to disrupt the IRA leadership from within the prison population by implicating a number of IRA members as informers, traitors, and the like, with the ultimate objective of instituting an organizational purge (Bowlin, 1999, p. 84). The Prison Sting had a firm foundation of intelligence preparation, and Heatherington fed the IRA leadership there a mixture of truths, half-truths, and outright lies; what is

---

trick in war for deceiving and outwitting the enemy, a cleverly contrived trick or scheme for gaining an end, [or] skill in ruses or trickery" (Merriam-Webster Online, 2001).

[3] The use of the term "states" can be problematic. I use it here in only the most general terms; it is not intended to describe solely the nation-state, the dominant political entity that emerged in Northwestern Europe after the 15th century, but rather any number of polities, including empires, countries, nations, commonwealths, etc. (Tilly, 1975, p. 26; Kennedy, 1987, p. xvii).

[4] This example—arguably the single best account of a deception perpetrated against terrorists—is discussed in significantly greater detail in Chapter III. I have attempted to provide only enough detail here to familiarize the reader with the story.

[5] By some accounts, Heatherington and McGrogan were coerced into participating as a result of trumped up rape charges. By other accounts, they were willing volunteers. Although versions of the method of recruitment vary in accordance with one's loyalties and preferences in the conflict, the pair was successfully recruited to aid the British military in a well-thought-out deception operation.

important is that his stories were either verifiable by the IRA, or fit existing preconceptions held by the IRA leadership.

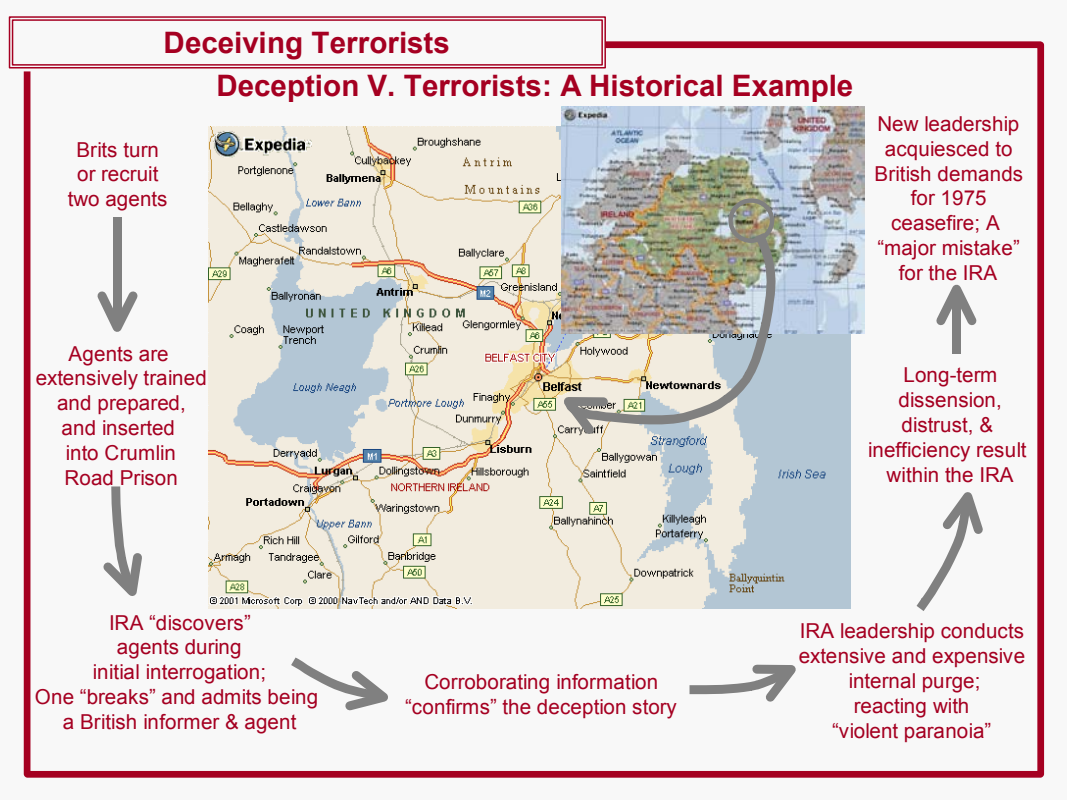


Figure 1. The Prison Sting Deception

The British used a clever method to introduce the deception story. Upon remand to Crumlin Road Prison, prison administrators would ask new prisoners which of three segregated populations they wanted to join: Republican, Loyalist, or general. The appointed leader of the respective population would then "interview" the new prisoner prior to admittance into the population. Heatherington and McGrogan indicated that they wished to join the Republican population of Crumlin Road Prison. They were immediately "revealed" as informers when Heatherington "broke" during his initial interrogations at the hands of the IRA leadership. McGrogan, on the other hand, remained calm under both initial and subsequent interrogation, adding credibility to the IRA notion that he was a British agent and "confirming" Heatherington's "admissions" (Dillon, 1991, pp. 75-76). Finally, under extreme duress, Heatherington

"admitted" that he'd been sent to assassinate key members of the IRA leadership within Crumlin Road Prison and poison was subsequently "discovered" in his cell. Heatherington's story was accepted in its entirety (Bowlin, 1999, p. 86).

The deception was a stunning success. The leaders of the IRA, both inside and outside Crumlin Road Prison, were deliberately misled. The IRA leadership ordered, and the organization undertook, specific actions that favored the British: a vicious internal purge of the organization and the negotiation of a ceasefire that was far more advantageous to the British than it was to the IRA (Bowlin, 1999, p. 91). Brutal interrogations based on Heatherington's misinformation forced many IRA members who were actually innocent to confess to being British agents. Their comrades subsequently executed these innocent men. According to one Provo leader, the IRA leadership was carried away in hysteria:

> We were had. We knew we had fallen for it. It was… clever, well planned, and brilliantly executed. The IRA knew and found it difficult to admit that British military intelligence was brilliant. They almost destroyed us. They created paranoia in the ranks and left us severely damaged. Retrospectively, you see how simply it was worked. Heatherington gave us what we wanted only after pressure was exerted. Now that was clever—McGrogan played a game designed to make us feel that he was holding back so that we could feel pleased when we were making progress with one of them… It reinforced our views. Heatherington gave us those names of innocent guys and we believed him because he also supplied us with information which [sic] supported our own theories about various incidents… The Brits and Special Branch had obviously done their homework on us because we reacted with predictability (Bowlin, 1999, p. 89).

While the operation was generally a success for the British, it is important to note that the operation had unintended consequences for them as well. The most notable of these unintended consequences concerned the evolution of the IRA. Although severely damaged by the Prison Sting, the IRA ultimately survived as a "smarter and more determined organization." This smarter organization

reorganized from its traditional battalion formations into a cellular structure and ultimately proved harder to attack as a result.

The secrecy, organization, and coordination of the "Prison Sting" were all impeccable. The deception was planned at a high-level, and was extremely centralized. Intelligence preparation was considerable as subsequent inquiries proved. The channels by which the deception was executed were controlled with extreme efficiency. A relatively high level of secrecy was maintained, protected by plausibility and confirming details. The deception was plausible and was confirmed repeatedly throughout execution. Moreover, the deception fit the target's preconceptions or cognitive biases—in other words, it encouraged the IRA to see just what it expected.

State deception against terrorists and non-state actors is neither new nor a solely Western phenomenon, however. Filipino government forces routinely used deception as part of a larger counter-insurgency strategy against the Huks in the period immediately following WW II (Leites & Wolf, 1970, pp. 142-144). The fledgling Soviet Union employed deception from the early 1920's on to marginalize and even kill anti-Communist activists both inside and outside the Soviet Union (Tugwell, 1990, pp. 17-18). More than 150 years ago, the British used deception to facilitate the defeat of the Thuggee scourge in India.[6] More than 2,000 years ago, the Romans cleverly used deception as one of several clandestine or covert means in dealing with tribes beyond the Apennine peninsula (Sheldon, 1997, pp. 300-301). The historical record repeatedly suggests that state deception been employed against terrorists and other non-state actors. Is there anything the United States can learn from this record—anything that might prove helpful in our own efforts to combat terrorism?

[6] The Thuggee were a secret cult that practiced ritual murder and robbery in India from the mid-1500's until the mid-1800's.

B. THESIS OVERVIEW—SCOPE OF THE STUDY

The purpose of this thesis is to examine the potential benefits of deception as an instrument of US counter-terrorism strategy. In order to explore this under-analyzed area, this thesis takes the following steps. First, the body of deception theory is examined to establish a general foundation for thinking about deception. Next, the general foundation of deception theory is applied to the concept of deceiving terrorists. Subsequently, the thesis explores the risks and costs of deception, particularly as they compare to the risks and costs inherent in any military operation. Next, a number of scenarios are proffered to suggest how the United States might employ deception against terrorists in the future. Finally, the study concludes with a net assessment of the benefits of deception as an instrument of US counter-terrorism policy.[7]

C. KEY CONCEPTS

Before beginning study of the potential benefits of deception as an instrument of counter-terrorism policy, we must first establish a basic foundation. In particular, four questions must be addressed. What is deception? Just as important, what is not deception: where does deception end and other elements of information warfare or command and control warfare (IW and C2W respectively) begin?[8] Why do states use deception? Finally, why try to deceive

---

[7] I do not enter into a discussion of the definition of terrorism in this thesis. In Countering the New Terrorism, Ian Lesser points out that terrorism and terrorists are terms whose use is fraught with peril: "Discussions [of what those terms mean] tend to be inconclusive…because the rapidly changing nature of the phenomenon renders many traditional definitions misleading. The fashionable and often politically charged debate about terrorism makes the definition of terrorism a highly subjective, even ethno-centric exercise… In Rand's continuing research on this subject, terrorism has generally been defined by the nature of the act, not the identity of the terrorists or the nature of the cause. 'Terrorism is violence or the threat of violence calculated to create an atmosphere of fear or alarm,' generally in support of political or systemic objectives" (1990, p. 85). Lesser's definition shows considerable common sense and proves sufficient for the scope of this study. Thus, where the term terrorism is used in this thesis, Lesser's definition is the one intended unless otherwise specified. In the same vein, the term "terrorists" applies to those who undertake such acts. Individual terrorists, such as Theodore Kaczynski, the Unabomber, are generally excluded from the scope of this work.

[8] Current US military doctrine considers deception, OPSEC, PSYOPS, electronic warfare, and physical destruction to be the five pillars of IW or C2W (Joint Publication 3-13, 1998, p. I-4).

terrorists? The answers to these questions establish the boundaries for and foreshadow the argument that plays out through the remainder of the thesis.

1. What Is Deception?

In order to arrive at a satisfactory definition of deception, it is useful to begin with a brief survey of the literature on deception. The vast body of deception-related literature can generally be broken down into four categories: historical treatments; classical works; theoretical works; and doctrinal studies.[9] The first category—historical studies—is the largest by far. Works that fall into this category typically consist of single case histories of deception, generally based on anecdote. William Breuer's Hoodwinking Hitler, a study of Allied deception operations in support of the Normandy Invasion in WW II is an excellent example; Ewen Montagu's The Man Who Never Was, an eyewitness account of the execution of the deception plan for the Allied invasion of Sicily, is another.[10]

The second category—classical works on theories of conflict and warfare—generally offers prescriptions to decision-makers on how to employ deception. Sun Tzu's The Art of Warfare and Clausewitz's Vom Kriege are the best known—and most often misquoted or misunderstood—examples.[11] Sun Tzu, on the one hand, is clearly a proponent of deception. In one of his best-known passages, Sun Tzu counsels "warfare is the art (tao) of deceit:"

Camouflage is neither a component of IW nor C2W, but is closely related to deception nonetheless.

[9] Doctrine is an official statement of a nation's policy, especially toward other nations (Webster's Dictionary). The overwhelming majority of works making up this vast body of literature focus primarily on military deception.

[10] Citations for all books mentioned in this section can be found in the List of References at the end of this thesis.

[11] Another well-known example is Machiavelli's The Prince. Machiavelli "is credited with articulating an 'operating code' for the use of deception in politics and diplomacy. 'The one who knows best how to play the fox comes out best', he wrote, 'but he must be a great simulator and dissimulator'" (Tugwell, 1990, p. 266). According to Maurice Tugwell, "While many politicians since have been accused of following his advice to the point of being Machiavellian', it is only in the 20th century that deception has been 'institutionalised' [sic] within government" (p. 266).

> Therefore, when able, seem to be unable; when ready, seem unready; when nearby, seem far away; and when far away, seem near. If the enemy seeks some advantage, entice him with it. If he is in disorder, attack him and take him. If he is formidable, prepare against him. If he is strong, evade him. If he is incensed, provoke him. If he is humble, encourage his arrogance. If he is rested, wear him down. If he is internally harmonious, sow divisiveness in his ranks. Attack where he is not prepared; go by way of places where it would never occur to him you would go. These are the military strategist's calculations for victory (Carr, 2000, p. 74).

Clausewitz, on the other hand, acknowledges the general value of deception, but recommends against its use in most cases. "The person acting in war," he suggests, "has no desire for the game of crafty agility:"

> The bitter earnestness of necessity usually forces us into direct action, so that there is no room for that game. In a word, the pieces on the strategical chessboard are lacking in that agility which is the element of stratagem and cunning. The conclusion we draw is that a correct and penetrating eye is a more necessary and more useful quality for a general than stratagem, although that also does no harm as long as it does not exist at the expense of qualities of temperament, which is only too often the case (Carr, 2000, p. 425).

While both categories of works are extremely valuable to deception research, neither is sufficient in and of itself to draw generalizations about deception. Lessons drawn about deception from one historical case may not apply in another time or conflict. Moreover, the effectiveness of prescriptions for the use of deception drawn from classical works may be limited to the context in which they were originally developed.

By way of contrast, the last two categories—theoretical works and doctrine—attempt to transcend the contextual limits of the first two. Theoretical works generally consist of attempts to break down deception in order to describe how deception works in a broad range of situations or contexts. Such treatments, particularly those taking multidisciplinary approaches to understanding and describing deception, were virtually nonexistent before 1969.

Donald Daniel and Katherine Herbig's Strategic Military Deception and Barton Whaley's Stratagem are the best examples of theoretical works. Deception doctrine, on the other hand, prescribes how the agencies of a state—generally its military forces—intend to employ deception under a wide variety of circumstances. Current US military deception doctrine is captured in Joint Publication 3-58, Joint Doctrine for Military Deception.

Of these four categories, this thesis focuses on the last two in order to develop a working definition of deception. Table 1, shown on the next page, summarizes some of the most popular definitions from the theoretical and doctrinal categories; from these we can hope to identify common threads or characteristics.

Source	Definition
Amos Perlmutter & John Gooch, Military Deception and Strategic Surprise (London: Frank Cass, 1982)	Deception is a conscious and rational effort to deliberately mislead an opponent. It seeks to create in the adversary a state of mind which [sic] will be conducive to exploitation by the deceiver. As such, deception is one of the oldest and most effective weapons of warfare... Far from being either ungentlemanly or random, [deception] is a systematic and consistent process in which success may bring substantial benefits (Perlmutter & Gooch, 1982, p. 1).
Donald Daniel & Katherine Herbig, Strategic Military Deception (New York: Pergamon, 1982)	Deception is the deliberate misrepresentation of reality done to gain a competitive advantage (Daniel & Herbig, 1982, p. 3). The immediate aim is to condition a target's beliefs; the intermediate aim is to influence the target's actions; and the ultimate aim is for the deceiver to benefit from the target's actions. Deceptions are often credited with success when only the first goal is achieved; but, to evaluate the actual impact deception has on the course of events, one should properly measure success vis-à-vis the third goal (p. 5).
Barton Whaley, "Toward a General Theory of Deception"	Deception is the distortion of perceived reality. Operationally, it is done by changing the pattern of distinguishing characteristics (charcs) of the thing (whether object or event) detected by the sensory system of the target. The task (purpose) of deception is to profess the false in the face of the real (Whaley, 1982, p. 182).
Ronald G. Sherwin, "The Organizational Approach to Strategic Deception: Implications For Theory And Policy"	The term "strategic deception" refers to instances during war or intense international competition when countries attempt to mask their diplomatic and military strategy either by confusing or misleading their opponents. The deceiver's overriding objective is to gain a strategic advantage by encouraging an opponent to respond inappropriately to the real state of affairs (Sherwin, 1982, p. 70).
Maurice Tugwell, Deception Operations (London, Brasseys, 1990)	A purposeful attempt by the deceiver to manipulate the perceptions of the target's decision-makers in order to gain a competitive advantage (Tugwell, 1990, p. 4).
Joint Publication 3-58, Joint Doctrine For Military Deception (Washington, DC: US Government, 1996)	Those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (1996, p. I-1).

Table 1. Commonly Quoted Definitions of Deception.

From these varied definitions, it is possible to identify a number of common characteristics. Deception—the distortion of reality to gain a competitive advantage—is deliberate and results in a specific action. Moreover, deception has two common variants—confusing and misleading—and appears to have utility at multiple levels. These characteristics merit some elaboration.

First, deception is a deliberate act—never an accident. As Whaley points out in his "Typology of Perception," part of his seminal "Toward A General Theory Of Deception," unintentional deception is not deception but rather misrepresentation (Whaley, 1982, p. 180; see Figure 2).[12] This is significant because it implies that deception requires both intent and effort on the part of the deceiver to deceive. Without intent and effort on the part of the deceiver, an adversary may still draw the wrong conclusions or may be surprised, but those outcomes are not the result of deception.

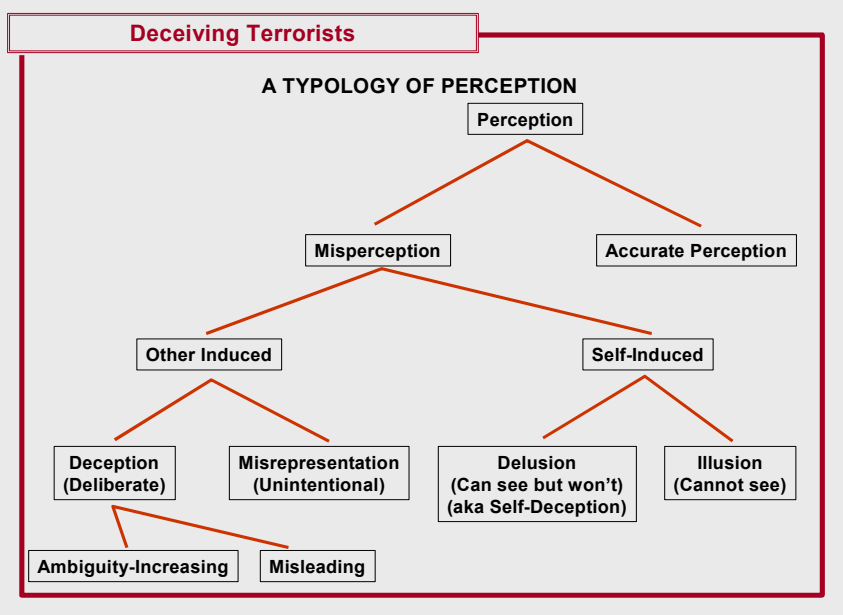


Figure 2. A Typology of Perception (after Whaley, 1982, p. 180).

[12] Barton Whaley points out that deception is but one type of human perception, and is distinguishable as such from misrepresentation, delusion, and illusion. According to Whaley, "All deceptions are applied psychology—the psychology of misperception" (Whaley, 1982, p. 179).

Intent to deceive without some specific resulting action on the part of the deceived party is generally pointless, however. As Maurice Tugwell points out, deception "succeeds only when the victim acts in the manner intended" (Tugwell, 1990, p. 398). Thus, the second characteristic of deception is that it is undertaken with the intent of producing or provoking a specific action (or the lack thereof); generally, this specific action is ultimately in our best interests and hurts the adversary's interests (although the latter is not clear to the adversary at the time). For this reason, deception normally targets adversary decision makers—those who have the authority to direct the intended reaction—rather than the whole of an adversary's forces or people.[13]

The third characteristic of deception that merits attention is the fact that virtually all deceptions can be distinguished as one of two variants: ambiguity-increasing or misleading (Daniel & Herbig, 1982, p. 5). These variants produce somewhat different effects and operate in different ways. Ambiguity-increasing deception "confuses a target so that the target is unsure as to what to believe" (p. 5). Such deceptions seek to ensure that "the level of ambiguity always remains high enough to protect the secret of the actual operation" (p. 5). Operation Fortitude, the strategic deception and cover plan for the invasion of Normandy in WW II, is one example of ambiguity-increasing deception (See Figure 4).

[13] Maurice Tugwell points out that it may be a mistake to view only key government or military elites as decision makers. "When an electorate or faction has in its power to influence or dictate [a desired] policy,' says Tugwell, "that group may become the 'target's decision-makers,' even though it holds no official executive position" (Tugwell, 1990, p. 4).

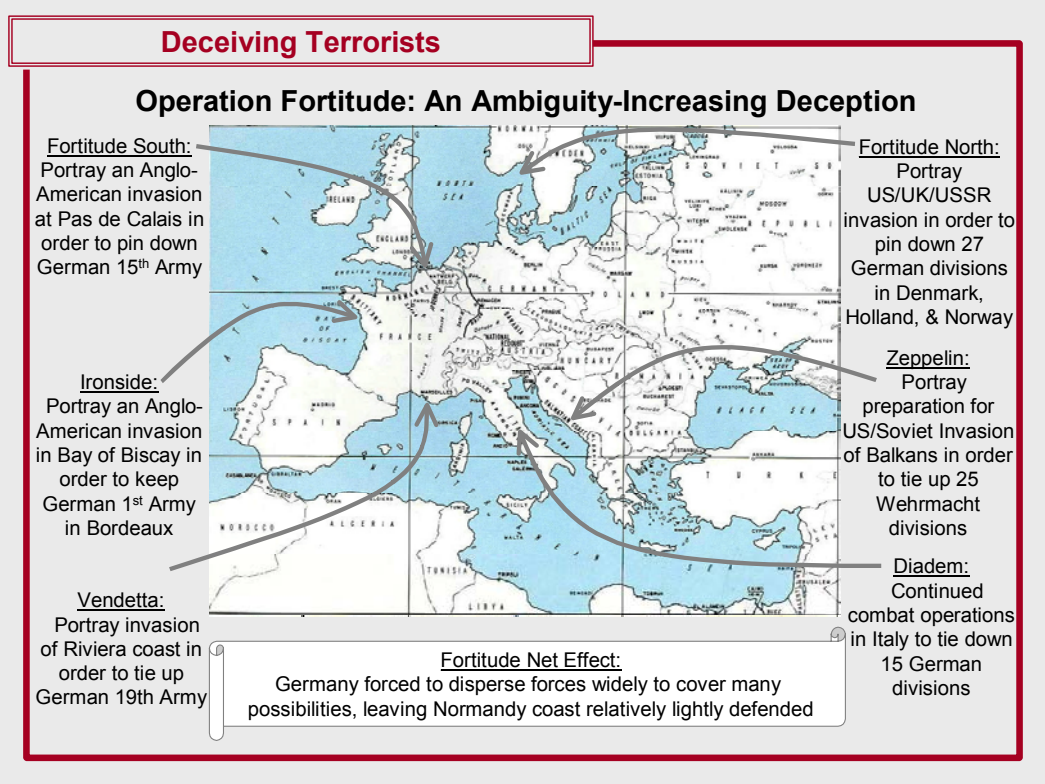


Figure 3. Operation Fortitude: An Example of Ambiguity-Increasing Deception (After Breuer, 1993, p. 101)

Misleading deceptions, on the other hand, reduce ambiguity by "building up the attractiveness of one wrong alternative" (Daniel & Herbig, 1982, p. 6). The ultimate goal of such deceptions, according to Barton Whaley, "is to make the enemy quite certain, very decisive, and wrong" (1969, p. 135). Misleading deceptions thus encourage an adversary to focus or concentrate on a single contingency, thereby increasing the deceiver's chances for success in others. Barbarossa, the extensive Nazi campaign to deceive the Soviet Union prior to the invasion of the latter on June 22, 1941, is one example of a misleading deception. Operation Mincemeat, an elaborate scheme to convince the Axis that the Allies' Mediterranean invasion would come at Sardinia as opposed to Sicily, is another WW II example of misleading deception (see Figure 5).

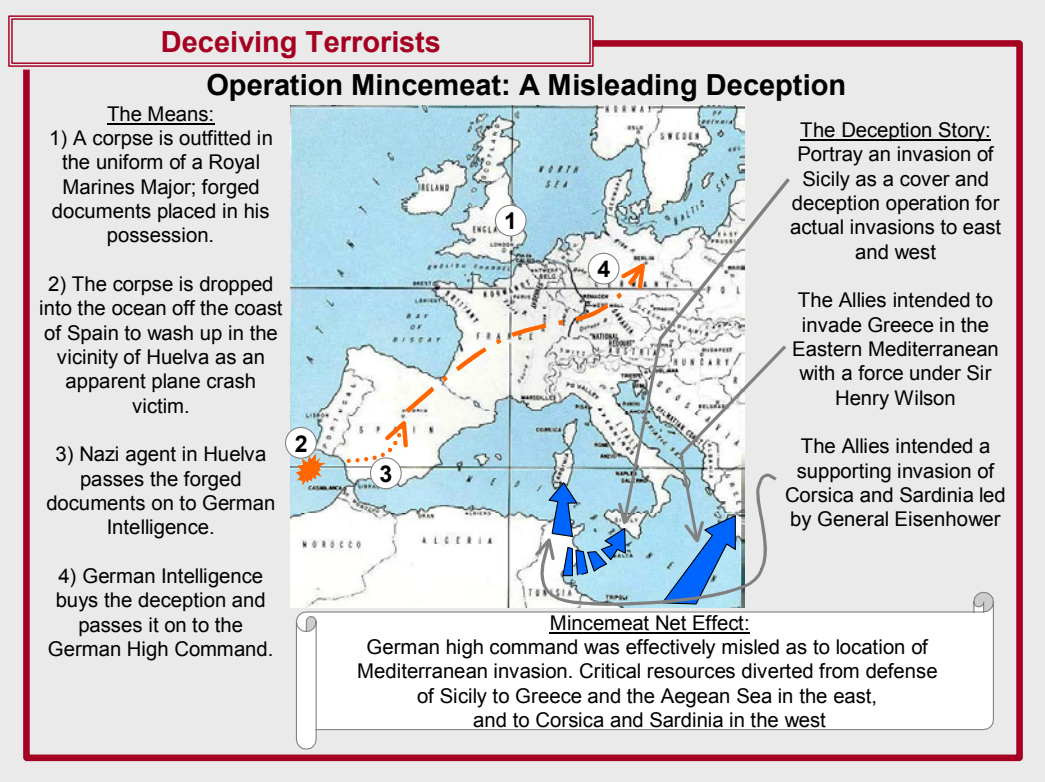


Figure 4. Operation Mincemeat: Example of Misleading Deception (After Montagu, 1996).

In practice, most elaborate deceptions tend to employ deception ruses of both the ambiguity-increasing and misleading variants. As Daniel and Herbig point out, although ambiguity-increasing and misleading deceptions "are conceptually distinct and can be initiated with different intentions in the deceiver's mind, in practice their effects often coexist or shade into one another as the deception evolves" (Daniel & Herbig, 1982, p. 7). Daniel & Herbig further suggest, "it may be most useful to consider the outcomes of the two variants as a continuum between convinced misdirection at one pole and utter confusion, in which all looks equally likely, at the other" (p. 7).

The final critical characteristic of deception that merits attention is that it tends to have utility at more than one level, with different aspects at each level. Most theoretical authors distinguish at least two levels of deception: strategic and

tactical.[14] According to Daniel and Herbig, strategic deceptions "involve large numbers of individuals and organizations as perpetrators and victims of deception, including the national command authorities on both sides of the deception interaction (1982, p. xi). Moreover, strategic deceptions "are relatively long-term deceptions, recurring over the course of weeks or months" (p. xi). Ronald G. Sherwin expands on this definition in "The Organizational Approach to Strategic Deception: Implications for Theory and Policy." Sherwin suggests that strategic deception usually involves a much wider array of deception means than tactical deception, "using diplomacy, economics, espionage, intelligence, and virtually every conceivable dimension of modern international conflict" in order to deceive (Sherwin, 1982, p. 70). Finally, the stakes of strategic deception tend to be much higher than other deceptions, since strategic-level deceptions "can affect the outcome of wars or large-scale front-level campaigns" (Daniel & Herbig, 1982, p. xi).

Tactical deceptions, on the other hand, are generally much more narrow in scope, generally limited to "the outcome of battles or local engagements" (Daniel & Herbig, 1982, p. xi). For the most part, smaller numbers of individuals and groups are typically involved, and the targeted decision makers are local rather than at the national command authority level. Moreover, tactical deceptions tend to be shorter in duration and the means used to carry them out are usually much more limited.

Despite these differences, however, strategic and tactical level deceptions are frequently intertwined. Tactical deceptions are often undertaken as part of strategic deceptions; strategic deceptions, in turn, may constrain or bound tactical deceptions. One way of looking at the relationship between various levels of military deception is suggested by Figure 6.

---

[14] US military doctrine, on the other hand, distinguishes five categories of military deception: strategic, operational, tactical, service, and deception in support of OPSEC (JP 3-58, 1996, p. GL-4;

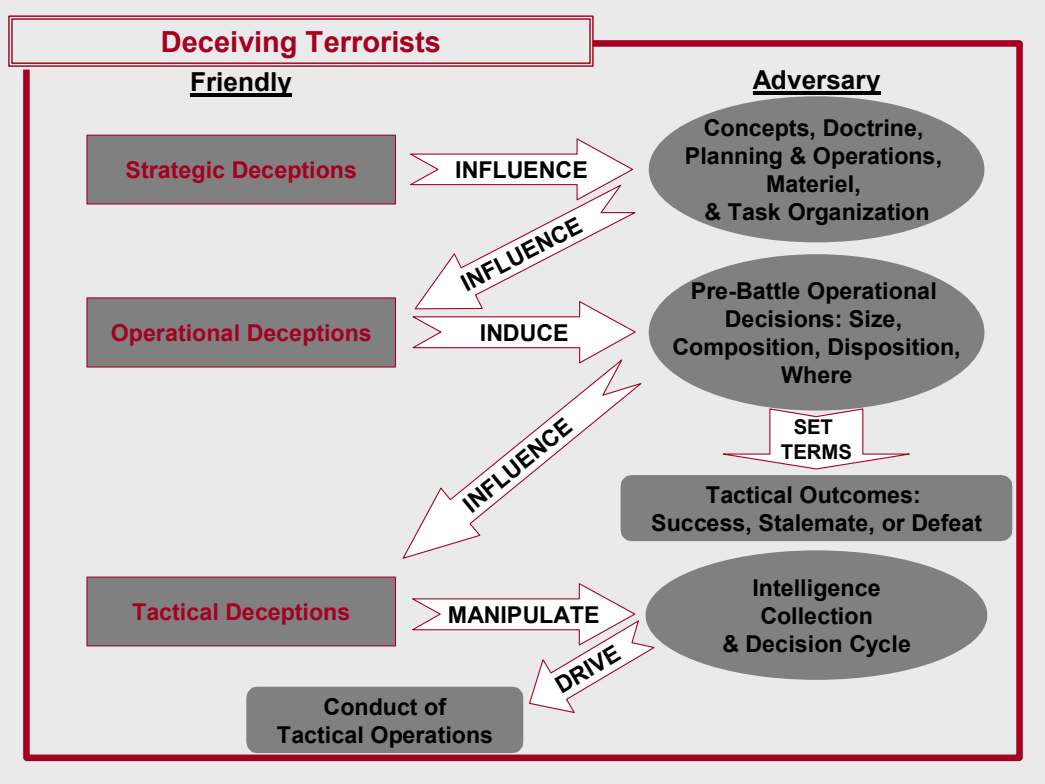


Figure 5. Relationship of Levels of Deception

(After Figures 2-3 and 3-1, FM 90-2, 1988, pp. II-10, III-4)

For the purpose of this study, therefore, the following definition of deception is proffered, synthesizing three of four of these common threads:

> Deception consists of actions taken during periods of conflict or intense international competition to deliberately confuse or mislead enemy decision-makers. The ultimate goal of deception is to gain a decisive advantage by provoking a specific action (or the lack thereof) on the adversary's part.

2. What Is Not Deception?

Because of the close relationship between deception and the other four elements of IW or C2W, deception is often confused with those other elements. However, although it may be closely related, deception is not synonymous with propaganda, psychological operations (PSYOPS), operations security (OPSEC),

and camouflage.[15] Still, these concepts quite often support or go hand-in-hand with each other. As Joint Publication 3-58 points out, "deception is done in conjunction with the overall C2W effort," with deception reinforcing and being reinforced by the aforementioned concepts (Joint Pub 3-58, 1996, p. II-2).[16]

According to Maurice Tugwell, propaganda is "any information, ideas, doctrines, or special appeals disseminated to influence the opinion, emotions, attitudes or behaviour of any specified group in order to benefit the sponsor either directly or indirectly" (1990, p. 7). Propaganda may be classified according to source as white, gray, or black. White propaganda emanates from a source that is what it proclaims itself to be (p. 7). Gray propaganda emanates from unidentified sources—"a voice on the radio without station identification, or a pamphlet published anonymously" (p. 7). Black propaganda comes from sources pretending to be other than what they really are—"a newspaper claiming independent editorial control" but in fact "funded and directed by a foreign intelligence service" is one example (p. 7).

As Tugwell points out, however, propaganda isn't intrinsically deceptive.[17] Rather, propaganda "is 'loaded', meaning that it tends to select the facts it chooses to expose, and the interpretations it places upon them, to support preconceived bias. It may give a one-dimensional view of the world without actually telling lies" (p. 7). Propaganda may conceal the truth while propagating the false, conceal or falsify the source from which it emanates, or some combination of the two (p. 7). Thus, propaganda may be used to perpetrate deception in certain situations, particularly when the deception target is a faction or group with the power to influence or dictate a desired action:

---

[15] Propaganda is not an element of IW or C2W under US military doctrine.
[16] There is a movement afoot today to revise these concepts somewhat under the guise of Information Operations, both with the Joint Publication 3-13, dated October 1998, and the Army's Draft Field Manual 3-13, currently undergoing final revisions. It is unlikely that the changes will significantly alter the descriptions or relationships offered here, however.
[17] Propaganda does often deceive nonetheless, sometimes by design, and sometimes by default.

> When the 'target decision-makers' comprise a mass audience, such as an electorate, deception channels may be expanded beyond the covert and specialist routes typically used in war to broader means of communication such as propaganda. (Tugwell, 1990, p. 7).

Like both deception and propaganda, PSYOPS represent a systematic process of conveying tailored messages to a specific audience to influence perceptions. Unlike deception and propaganda, however, PSYOPS generally promote specific themes that it is hoped will result in desired attitudes and behaviors conducive to friendly efforts and objectives. PSYOPS normally target large groups that do not necessarily have any decision-making power, whereas deception typically targets specific individuals or groups empowered to make decisions. Still, the distinction between propaganda and PSYOPS is a fine one, often depending on one's perspective. If the target is general perceptions and the message is the truth, the appropriate means is probably PSYOPS. If the target is general perceptions and the message consists of selected truths or even lies, the appropriate means is probably propaganda.[18] If the target is specific or narrow perceptions, decisions, and resulting actions, the appropriate means is probably deception. Despite these differences, however, there is "opportunity for mutual support if deception and PSYOPS are carefully coordinated" (Joint Publication 3-58, 1996, pp. II-3-4).

Secrecy, in this case, is the process of denying adversaries information about capabilities and intentions by identifying, controlling, and protecting the evidence of planning and executing sensitive activities. In the US government lexicon, much of secrecy falls under the rubric of OPSEC. According to Joint Publication 3-58, OPSEC seeks to limit an adversary's ability to detect or derive useful information from friendly activities (usually open) called indicators. By way of contrast, deception generally seeks to increase the likelihood of an adversary's

[18] An additional distinction sometimes made between PSYOPS and propaganda is audience. By DoD regulation, American PSYOPS is never used to influence a domestic audience; propaganda may be (LTC Paul Mullin, personal communication, 5 November 2001). Other nations may not observe this distinction.

detection of only certain indicators, usually while hiding others, in order to paint an ambiguous or misleading picture. The relationship between OPSEC and deception is thus a close one, since both generally require the management of indicators (Joint Publication 3-58, 1996, p. II-4). As Handel points out, "any breach of [secrecy in the attempt to deceive]…will of course lead to failure and probably to self-deception" (Handel, 1982, p. 126).

In terms of guarding capabilities, deception "can be used to protect the development, acquisition, and deployment of physical destruction systems," as well as to "mislead an adversary as to the true capabilities and purpose of a [new] weapon system" (Joint Publication 3-58, 1996, p. II-5; Axelrod, 1979, pp.231-232). Likewise, deception and secrecy can work hand-in-hand to conceal intentions—"the actual goals and plans of the deceiver" (Handel, 1982, p. 126).

Finally, camouflage consists of efforts by individuals and units to hide, blend in, or disguise in order to prevent enemy observation. Camouflage is, by its definition, conceptually distinct from deception; the goal is almost invariably protection as opposed to provoking a desired response, while the target is an enemy's sensors (from eyes to high-technology sensor systems) as opposed to enemy decision makers.[19] Nonetheless, camouflage protects deception, particularly at a tactical level, by disguising evidence of the deceiver's actual courses of action (Field Manual 90-2, 1988, p. V-2). The German use of camouflage at the tactical level to conceal the preparations for the 1941 invasion of the Soviet Union and the 1944 offensive into the Ardennes is an excellent example of the symbiotic relationship between camouflage and deception.

3. Why Deception Is Used

Why do states use deception at all? After all, "As a form of trickery [deception] has acquired a pejorative connotation: just as 'gentlemen do not open

[19] Chapter II will introduce Barton Whaley's theory that every act of deception consists of both simulation and dissimulation. Camouflage is one means of dissimulation; hence, camouflage may be viewed in some cases as a subset of deception.

each other's mail,' so decent people should not engage in what is sometimes seen as an indecent activity," according to Perlmutter & Gooch (1982, p. 1). Still, there is considerable evidence that states routinely employ deception in intrastate conflict. At first glance, weak states seem to use deception to help defeat strong states. Strong states, on the other hand, seem to use deception to reduce their risks and costs. John Van Vleet, Barton Whaley, and Ronald Sherwin suggest that states (or, more to the point, their military forces) employ deception during armed conflict in order to gain or maintain surprise, to create conditions favorable to victory, and to reduce risks and costs. Maurice Tugwell suggests that states use deception for at least two other reasons in situations short of armed conflict: to mobilize groups and to protect legitimacy. Moreover, there is considerable evidence that states use deception in both periods of war and peace to conceal capabilities and intentions.

Van Vleet, Whaley, and Sherwin based their observations on the value of deception in gaining or maintaining surprise on empirical analysis of a large number of battles between the armed forces of states. Based on an empirical analysis of more than 160 battles fought between 1914 and 1973, Van Vleet observed deception provided "a high return in that it [had] at least an 80% chance of yielding surprise" (Van Vleet, 1985, p. 27). Barton Whaley and Ronald Sherwin calculated an even higher probability of achieving surprise and victory through stratagem, albeit in an analysis of a smaller (and different) group of 93 cases (Sherwin & Whaley, 1982, pp.187-189). [20]

One must keep in mind, however, that the surprise value of deception is relative. Michael Handel points out that surprise is "only rarely complete or total" (1982, p. 149). In fact, says Handel, "In most cases of sudden attack, the surprised side normally had enough information and warning signals to indicate

[20] In fact, one extremely interesting conclusion of the research of Whaley, Sherwin, Van Vleet, and others is that military deception that employs two or more strategic ruses is virtually always met with success (Sherwin & Whaley, 1982, p. 188). The degree of success is relative, of course, but the implication is stunning nonetheless.

the possibility of a forthcoming attack—its timing, place, direction, and the like" (p. 149). Moreover, "In many successful surprise attacks, the attacker achieves only a partial degree of surprise" (p. 149).

Still, states that employ deception in intrastate conflict in order to gain surprise are routinely rewarded. Nazi Germany employed deception to achieve surprise on the strategic and tactical levels during the 1941 invasion of the Soviet Union. The Allies returned the favor by employing deception against Nazi Germany in order to achieve surprise during the invasion of Normandy in 1944.

Van Vleet also points to the value of deception in creating conditions favorable to achieving military victory. Van Vleet suggests "deception itself can also induce the enemy to make inefficient use of his own resources by causing him to make mistakes in timing or utilization" (Van Vleet, 1985, p. 28). While Van Vleet does not provide the same kind of empirical evidence to support this observation, his argument is nonetheless seductive. Handel certainly concurs with Van Vleet's suggestion, arguing that:

> Effective deception will cause the adversary to waste his resources, to spread his forces thinly, to vacate or reduce the strength of his forces at the decisive point of attack, to tie considerable forces up at the wrong place at the worst time; it will divert his attention from critical to trivial areas of interest, numb his alertness and reduce his readiness, increase his confusion, and reduce his certainty (Handel, 1982, p. 143).

The aforementioned use of deception in Operation Mincemeat is but one of many examples of deception to create conditions favorable to achieving victory. With a Mediterranean invasion all but a foregone conclusion, the Allies persuaded Hitler and his senior military advisors to waste invaluable resources in areas that the Allies had no intention of attacking—Corsica, Sardinia, and Greece. Furthermore, the Allies encouraged the Germans to spread their forces thinly, tying up considerable forces far from the field of battle in a "force divisor effect." Finally, the Allies certainly caused the Axis to divert attention to trivial

areas of strategic and tactical interest—at least from the Allied perspective (Montagu, 1996, p. 134).

In much the same way, says Handel, deception reduces the risks and costs of interstate conflict. Deception, he contends, is a powerful "force multiplier," magnifying "the strength or power of the successful deceiver" (1982, p. 122).[21] "When all other elements of strength are roughly equal," Handel suggests, "deception will further amplify the available strength of a state—or allow it to use force more economically—by achieving a quicker victory at a lower cost with fewer casualties" (p. 122). "Reducing the cost for the deceiver," he contends, "implies increasing the cost for the deceived" (p. 143).

Van Vleet certainly agrees with Handel on this point, observing that "surprise multiplies the chances for a quick and decisive military success, whether measured in terms of explicitly sought goals, ground taken, [or] casualty ratios" (pp. 27-28). Moreover, Van Vleet's analysis seems to lend credence to Handel's observation. In the analysis, the average casualty ratio suffered by the military forces of states that used deception (59 cases) was 1:6.3. The average casualty ratio in cases involving either no surprise or no attempt to deceive (45 cases), on the other hand, was 1:2 (Van Vleet, 1985, p. 26; Whaley, 1969, p. 195).

The case can be made very effectively that the deception operations supporting the 1944 Allied invasion of Normandy reduced the risks and costs of that operation. As in the case of the Mediterranean invasion in 1943, invasion was a foregone conclusion. Operation Fortitude, however, reduced the costs of the invasion for the Allies by amplifying German uncertainty and thus increasing the costs for the Nazis.

Maurice Tugwell suggests that states have also used deception in periods of intense international competition to mobilize groups and to protect legitimacy.

---

[21] An observation echoed by Perlmutter & Gooch (1982, p. 2).

Mobilizing deceptions “have the goal of persuading the target to commit itself in support of a cause. Sometimes, deception is used to break an existing commitment; in other cases deception provides the illusion that old and new causes are compatible” (Tugwell, 1990, p. 396). In this respect, mobilizing deceptions may target groups as often as they target individual decision-makers. Mobilizing deceptions play a key role in ideological conflicts, and were used extensively by both the Soviet Union and the United States during the Cold War era (p. 397).

As one example of mobilizing deception, Tugwell cites the successful efforts of the North Vietnamese communists during the Vietnam War:

> By creating false pictures of: a democratic, non-communist, indigenous Southern insurrection; an American military employing criminal deeds and genocide as a matter of policy; and a benevolent North Vietnamese regime with no ambitions towards the domination of the South, the Vietnamese communists succeeded in mobilizing many American and much Western and Third World opinion against the war and the United States (Tugwell, 1990, p. 396).

In the eyes of many observers, including Tugwell, these mobilizing deceptions thus played a critical role in the eventual “victory” of the North Vietnamese.

States employ legitimacy deceptions, according to Tugwell, to achieve, maintain, or restore perceived legitimacy. The goal of legitimacy deceptions is almost invariably perception management. “Typically, these take place prior to, during, or after some political or military action; they are defensive, even apologetic, in their style (Tugwell, 1990, pp. 397-398). Legitimacy deception operations are more often “directed at publics [than individual leaders], with domestic audiences as first priority,” since “legitimacy starts at home and it is this base that must be protected at all costs” (p. 398). As evidence of legitimizing deceptions, Tugwell cites two examples: Soviet information operations in the aftermath of the 1983 shoot-down of Korean Air Lines (KAL) Flight 007, and the “American cover-up that followed the U-2 incident” in 1960 (p. 398).

Finally, as mentioned in the section on the relation of deception to other elements of IW and C2W, there is considerable evidence that states use a combination of deception and secrecy in both war and peace to conceal capabilities and intentions. In conjunction with secrecy, deception has tremendous utility "to protect the development, acquisition, and deployment of physical destruction systems," as well as to "mislead an adversary as to the true capabilities and purpose of a [new] weapon system" (Axelrod, 1979, pp.231-232). Likewise, deception and secrecy can work hand-in-hand to conceal intentions—"the actual goals and plans of the deceiver" (Handel, 1982, p. 126). The American concealment of the fledgling Corona "spy" satellite program in other space exploration development programs is one example of the use of deception to conceal capabilities. The German strategic deception carried out throughout the 1930's regarding the capabilities of the Luftwaffe—well chronicled by both Barton Whaley and Michael Mihalka—is an example of the use of deception to conceal both capabilities and intentions.

The historical record clearly indicates that states routinely use deception, both during periods of armed conflict and during periods of intense international competition short of armed conflict. The reasons for the employment of deception are also clear: deception promises potential benefits for those who practice it.[22]

4. Why Deceive Terrorists?

While the reasons states employ deception in conventional conflict may be relatively clear and straightforward, the same cannot be said about the potential reasons to use deception against terrorists. Still, it seems possible to identify three potential benefits or utilities of deception as a counter-terrorist tool. Deception may be used to:

- Create and exploit inefficiencies and weaknesses in the terrorist organization;

[22] The reasons that states use deception may not be shared by non-state actors, who also use deception in times of both conflict and relative peace.

- Facilitate counter-terrorist operations; and
- Conceal counter-terrorist capabilities and intentions.

Deception may offer one means to create inefficiencies and weaknesses in terrorist organizations. Clandestine organizations—and many terrorist organizations are clandestine organizations—generally struggle to balance organizational efficiency with operational security. Increased organizational efficiency—the ability to commit acts of terror—is only purchased at the expense of operational security (McCormick & Owen, 2000, p. 186; Bell, p, 27). By targeting a terrorist organization's confidence in its operational security, a deceiver may, for a time, be able to affect the terrorists' organizational efficiency. Furthermore, deception may be used to target the trust bonds upon which cellular or network-type terrorist organizations are founded; deception operations have been used in the past to cause and exploit organizational dissension in these kinds of groups (Bowlin, 1999, p. 89; Garreau, 2001, p. C01). Moreover, deception may offer a means to exploit existing organizational inefficiencies and weaknesses once they are created or identified (McCormick & Owen, 2000, p. 186).

Deception may also prove useful to facilitate counter-terrorist operations in two ways. First, deception may be used to protect operational counter-terrorism units and missions. While direct action is certainly preferred by many as the blunt instrument of choice in many counter-terror operations, the special mission units that conduct them are generally valuable assets with extremely limited recuperability.[23] Deception can be used to give those units a greater chance of operational success and the survivability that goes with it just as other "commando" units have used it in the past to create relative superiority (Hoffman, 1985, p. 22). Second, deception may also be used by special operations or counter-terrorist units to create operational & tactical opportunities where none

[23] A Delta squadron, if such a thing exists, cannot be reconstituted quickly if a majority of the unit is lost on one mission. The organizational capabilities and individual experience such a unit would theoretically possess would take years to replace.

otherwise exist (Hoffman, 1985, p. 22). Finally, as discussed in the preceding sections, deception has been employed throughout history to conceal strategic, operational, & tactical capabilities and intentions in general. In theory, deception can certainly be used in the same way against terrorists (Jones, 1979; Handel, 1982, p. 148).

At this point, however, these utilities—these potential benefits of deception as a counter-terrorist tool—are merely assertions. In order to determine whether any of these assertions holds value, the theory or theories underlying each use must first be examined in greater detail. For each assertion, it seems prudent to try to unearth historical examples to support those theories. Finally, each historical example must be examined in detail in order to determine whether there are any significant lessons to be learned or conclusions to be drawn from those examples. Only then can we claim with any confidence that these utilities hold promise as real-world counter-terrorism applications.

D. WHERE WE GO FROM HERE—STRUCTURE OF THE STUDY

With a basic understanding of what deception is, we can turn our attention to other questions that are fundamental to understanding the potential benefits of deception as an instrument of counter-terrorism policy: how deception works, why states have deceived terrorists, the risks and costs of deception, and what deception against terrorists might look like in the future. Chapter II takes on the first of these—the question of how deception works—from two complementary perspectives. The chapter first looks at deception as an activity consisting of its component parts. Then, a brief, multidisciplinary study of deception as a process, both in theory and in practice, is undertaken.

Chapters III and IV turn to the issue of applying deception against terrorists. Chapter III explores the use of deception to create and exploit inefficiencies and weaknesses in terrorist organizations. Chapter IV explores the use of deception to facilitate counter-terrorist operations and to conceal capabilities and intentions. The theories underlying each potential utility are

examined in detail and case studies or historical examples are offered to support each utility. Finally, the chapters examine a number of cases of deception against terrorists and other non-state actors in varying degrees of detail, in order to see what common lessons may be drawn from them.[24]

A significant line of questioning scarcely addressed by existing studies on deception concerns the potential risks and costs incurred by its use. Chapter V tackles this subject in two parts. The first part offers a summary of the risks and costs of deception. The second part of the chapter, in turn, offers a summary of the ethical and legal status of such deceptions.

Finally, Chapter VI summarizes the concepts of deception both in general and of terrorists in particular. Then the chapter addresses the question "how might the US employ deception against terrorists in the future?" Chapter VI offers a series of five loosely connected scenarios depicting a deception campaign against a terrorist organization—in this case, Usama bin Laden's al Qa'ida network.[25] Each scenario includes necessary background information, a detailed narrative, and an examination of the risks, costs, and benefits of each deception operation. These scenarios are not meant to be taken literally, but rather to spur thought on how deception operations might be employed as a part of American counter-terrorism policy. The chapter offers a number of questions for further research and closes with final assessment of the idea of deceiving terrorists.

Having established a road map of where we are and are not headed with this thesis, our journey thus begins with the logical next step, in the form of a question. How does deception work? Chapter II delves into this question.

---

[24] Specific cases of deception of terrorists are often shrouded in considerable secrecy, as Barton Whaley notes in Stratagem (1969, p. vii). While this secrecy complicates the study of deception in general, and deception of terrorists in particular, the work of Whaley and others shows that it is possible to pierce the veil of secrecy. I discuss this phenomenon in detail in Chapter III,

[25] Although the American media commonly uses the transliterations "Osama bin Laden" and "Al Qaeda," I employ the Arabic transliterations "Usama bin Laden" and "al Qa'ida."

II. HOW DOES DECEPTION WORK?

Everything should be made as simple as possible, but not simpler.

Albert Einstein

One of the most common human failings is to examine a complex phenomenon from only one perspective and claim to make definitive conclusions based on that limited perspective. The parable of the blind men and the elephant, excerpted below, makes that point:

> It was six men of Indostan to learning much inclined,
> Who went to see the elephant (though all of them were blind),
> That each by observation might satisfy his mind.
>
> The first approached the elephant, and happening to fall
> Against his broad and sturdy side, at once began to bawl:
> "God bless me! But the elephant is very like a wall!"
>
> The second feeling of the tusk cried, "Ho! What have we here,
> So very round and smooth and sharp? To me 'tis mighty clear
> This wonder of an elephant is very like a spear!"
>
> The Third approached the animal, and happening to take
> The squirming trunk within his hands, thus boldly up he spake:
> "I see," quoth he, "the elephant is very like a snake…"
>
> …And so these men of Indostan disputed loud and long,
> Each in his own opinion exceedingly stiff and strong,
> Though each was partly in the right, and all were in the wrong!
>
> (Saxe, 1968)[26]

The lesson of the parable and its relevance to our topic is this: in order to gain a thorough understanding of a complex phenomenon like deception, one needs to examine it from different perspectives. One means of gaining perspective into how deception works is to break it down into its component parts, defining those activities which, when taken in sum, make up the act of deception. An alternate means is to employ a multidisciplinary approach to

[26] This is, of course, only one version of a very ancient parable with an uncertain origin. The fifth, sixth, and seventh stanzas are omitted here for the sake of brevity. For those interested, the fourth man thought the elephant was a tree, the fifth a fan, and the sixth a rope.

describe deception as a process. In this way, deception can theoretically be "mapped" and further analyzed to draw relevant lessons concerning its use. Those approaches, respectively, are the basis for the first and second sections of this chapter. The remaining sections draw from the first two to explain why deceptions succeed and what factors contribute to deception success.

A. DECEPTION AS A SUM OF ITS PARTS

As mentioned above, one way to gain perspective into how deception works is to look at the lesser acts, or categories of acts, which make up the larger act of deception. This is the approach taken in the past by Barton Whaley, R.V. Jones, and Michael Handel. Whaley broke the act of deception down into two subordinate acts—simulation and dissimulation. Jones provided us another way of looking at how deception works—as a combination of positive and negative acts. Handel, on the other hand, characterized all deceptions as either active or passive. What we have, in the end, are three wise men, all astute students of deception, who each describe the "elephant" in slightly different but nonetheless complimentary terms. Each description merits further examination.

1. Simulation And Dissimulation

Barton Whaley offers a detailed dissection of deception into subordinate components. According to Whaley, "Every deception operation, whether of man or nature, is comprised of only two basic parts: dissimulation and simulation" (Whaley, 1982, p. 183).[27] Simulation, on the one hand, is that overt, part of a deception presented to the target. The task of simulation is to "pretend, portray, profess" the false: to tell one's adversary a story sufficiently believable and compelling to cause him to ultimately take some action that will lend the deceiver a competitive advantage (p. 183). Dissimulation, on the other hand, is "hiding the

[27] Whaley points out that the systematic analysis of these two terms—simulation and dissimulation—goes back as far as the early 17th century, with Sir Francis Bacon's essay "On Simulation and Dissimulation." The first application of the concept of simulation and dissimulation to military theory, however, was made by the head of British camouflage operations in WW I, Solomon J. Solomon, in Strategic Camouflage (Whaley, 1982, p. 191).

real" (p. 183). According to Whaley, "it is covert, that part of a deception concealed from the target" with the purpose of concealing or at least obscuring the truth (p. 183). Operationally, dissimulation is accomplished by hiding one or more of the characteristics that make up the unique pattern of an object or activity (p. 183). Whaley further notes, "Both simulation and dissimulation are always present together in any single act of deception. Nothing is ever 'just' hidden; something is always shown in its stead, even if only implicitly" (p. 183).

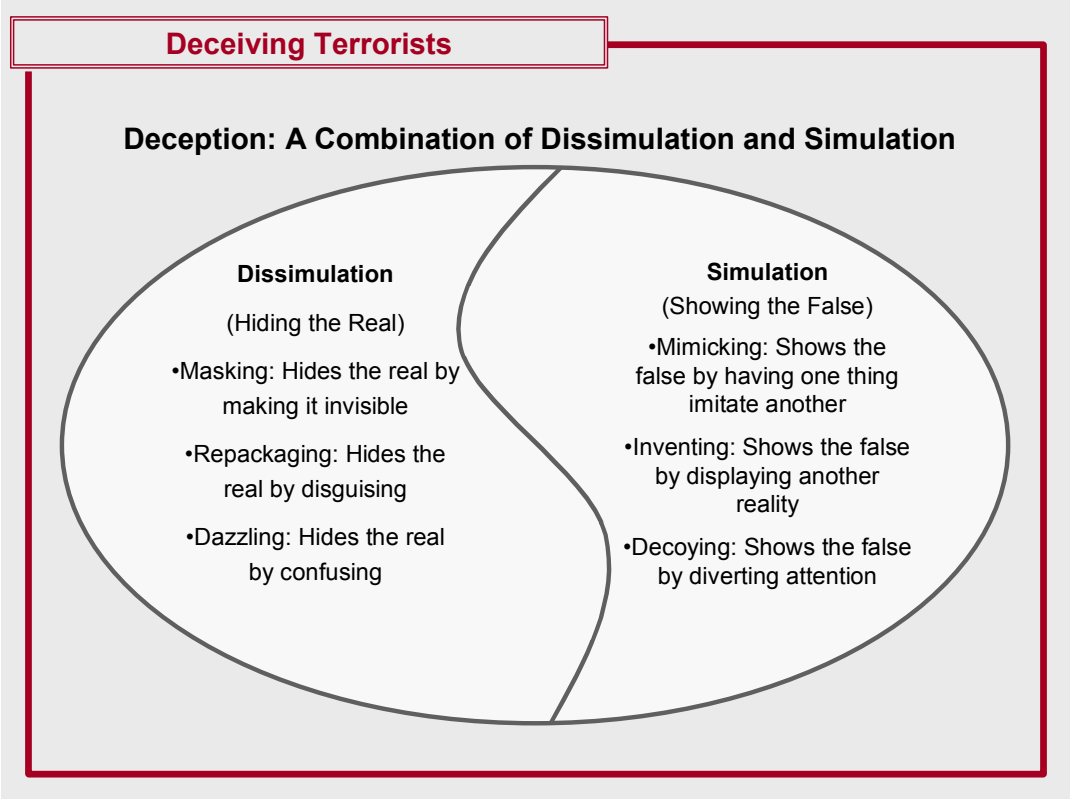


Figure 6. Simulation and Dissimulation

The acts of simulation and dissimulation are themselves each comprised of three subordinate categories of activities (See Figure 7). "The three procedures by which false things are shown [simulation]," says Whaley, "are mimicking, inventing, or decoying" (1982, pp. 184-185). Mimicking typically misleads the observer and "shows the false by having one thing imitate another" (p. 185). Mimicking is accomplished by duplicating a sufficient number of the distinctive characteristics of the object or activity to be imitated to passably

approximate its distinctive pattern. The ideal example of mimicking, contends Whaley, is the use of the double, or doppelganger (p. 185). One of the better-known examples of mimicking deception is a WW II operation code-named Copperhead. Lieutenant Clifton James, a Royal Army Pay Corps officer, convincingly portrayed General Bernard Montgomery in a scheme to convince the German high command that an invasion was due in southern France about the same time as the Normandy invasion (Breuer, 1993, pp. 169-172). A lesser-known example of mimicking deception was the use of pseudo-gangs by the British in the Mau Mau uprising in Kenya, as well as by the Rhodesian Selous Scouts during the Rhodesian War. Pseudo gangs were groups consisting of soldiers and former insurgents who adopted insurgent dress and behavior, contacted actual insurgent gangs, and passed themselves off as insurgents in order to glean information necessary to conduct effective counter-insurgent direct action (Thompson, 2000, pp. 1-2). More recently, Saddam Hussein and Usama bin Laden have both purportedly used doubles in mimicking operations designed to ensure their own safety.

Inventing, the second means of simulation, "shows the false by displaying another reality" (Whaley, 1982, p. 185). As opposed to mimicking, in which one object or activity imitates another already existing, inventing "creates something entirely new, albeit false," by crafting enough new characteristics "to create an entirely new pattern" (p. 185). The "amphibious operation" portrayed by a SEAL platoon using pyrotechnics on the beaches of Kuwait at the initiation of Operation Desert Storm is one excellent example of an inventing deception, but it is hardly the first time that the United States used a false amphibious landing to carry out an inventing deception. In September 1950, an ad hoc commando-style detachment of more than 100 soldiers, under the command of COL Louis B. Ely, invented an invasion near the Korean city of Kunsan. This highly successful ruse, supported by carrier-launched air strikes and PSYOPS leaflet drops, was a key part of the deception plan for MacArthur's Inchon landing on 15 September (Whaley, 1969, pp. A-483-484).

Decoying, the third means of simulation, “shows the false by diverting attention” (Whaley, 1982, p. 185). Decoying is accomplished by “creating alternative false characteristics that give an additional, second pattern” (p. 185). In this manner, decoying is “a matter of feints and diversions, literally misdirection” (p. 185). One example of a successful decoying deception can be found in the historical account of the US invasion of the island of Tinian on 24 July 1944. The US 4th Marine Division was faced with the daunting task of invading an island whose Japanese defenders were fully alert, fully prepared, and forewarned of the precise date of the invasion. To make matters even worse, the island of Tinian had only three beaches, one of which was not negotiable with existing amphibious equipment. The Marines solved the problem by using modified landing craft to seize the “untenable” beach, while simultaneously conducting a convincing decoy operation at one of the “good” beaches at the opposite end of the island. The deception was so successful that the Marines pinned down all of the Japanese reserves at the site of the decoy operation and lost less than twenty Marines and sailors in the first sixteen hours of the invasion (Whaley, 1969, pp. A-394-395).

The three methods or procedures by which objects or activities are dissimulated, on the other hand, “are masking, repackaging, or dazzling” (Whaley, 1982, p. 183). The act of masking “hides the real by making it invisible” (p. 183). Masking, according to Whaley,

> Either interposes a screen, shielding [the real object or activity] from senses (and any intermediate sensors) of the ‘deceivee’ so it is truly covert, or integrates it with its environment so it is unnoticed, blending into its background, literally overlooked, hiding in plain sight” (pp. 183-184).

In many ways, masking incorporates the activities traditionally referred to as camouflage. Whaley cites as an example a little known WW II deception in which German aircrews “hid” in captured B-17’s to “spy close-up on US bomber formations” (p. 184).

In contrast, repackaging, the second means of dissimulation, “is simulated metamorphosis,” which works to hide the real by disguising it (Whaley, 1982, p. 184). Repackaging modifies the appearance of an activity “by adding or subtracting characteristics to transform them into a new pattern that resembles something else” (p. 184). The Soviet portrayal of the buildup to the invasion of Czechoslovakia in 1968 as “training maneuvers” is one outstanding example of repackaging on a strategic scale (Whaley, 1969, pp. A-607-609; Valenta, 1982, pp. 53-54). A lesser-known example of repackaging is the Israeli use of a Ugandan-flagged Mercedes as the lead assault vehicle during the commando raid on 3-4 July 1976 to free hostages held at the Entebbe airport (McRaven, 1995, pp. 339-340).

Dazzling, the third method of dissimulation, “bewilders, confounds, baffles, perplexes, reducing certainty about the real nature of a thing” in order to hide the real by confusing the observer (Whaley, 1982, p. 184). This is accomplished by “randomizing or otherwise partially obscuring the characteristics of an object (its precise location, size, color, etc.) or an event (its exact timing, method of operation, etc.) in order to blur their distinctive pattern” (p. 184). If all works as planned, the resulting modified pattern creates ambiguity by conveying less certainty than the real but underlying pattern (p. 184). The former Soviet Union used dazzling extensively throughout the Cold War to deceive the Americans and NATO about the true capabilities of the combined Soviet strategic, land, and naval forces. As a result, Western leaders viewed the Soviet forces as “a foe of towering capabilities;” this ongoing deception had a definite impact on East-West relations throughout the Cold War (Bell and Whaley, 1991, p. 347). Much earlier, Gideon used trumpets and torches to dazzle the Midianites—one of our earliest examples of tactical dazzling.

According to Whaley, there is no textbook combination of simulation and dissimulation procedures to optimize the probability of deception success. Masking may be accompanied, for example, by mimicking; alternately, inventing or decoying may accompany masking just as easily (and profitably). Whaley

does conclude, “Masking and mimicking are not only overwhelmingly the most common methods used for dissimulation and simulation respectively,” but are also “the two used most often in combination” (1982, p. 187). Still, he acknowledges, “In practice as in theory, all three ways of hiding the real can accompany the three ways of showing the false in any of their possible combinations” (1982, pp. 186).

2. Negative And Positive Deception

R.V Jones approaches the task of describing how deception works in a manner similar to that employed by Whaley: as a whole comprised of two parts. In his essay “Intelligence, Deception and Surprise,” Jones observed that every deception consists simultaneously of both negative and positive acts (Handel, 1982, p. 148)(A summary of Jones’ classification of positive and negative deceptive activities, expressed in terms of their objectives, is found in Table 2).[28] Negative deceptive acts are essentially dissimulation: acts undertaken to “prevent the enemy from deducing” the deceiver’s true capabilities and intentions (p. 148). John Van Vleet subsequently expanded on Jones’ observation: “The negative side of deception is the protection of certain portions of the real operation and plans for future operations” (1985, p. 15).

[28] Jones presented “Intelligence, Deception and Surprise” at the 8th Annual Conference of the Fletcher School of Law and Diplomacy—Tufts University International Security Studies Program in April 1979. The essay can also be found in Raanan, Pfaltzgraff, and Kemp (Eds.), (1981), Intelligence Policy and National Security, London: MacMillan.

Negative Objectives Prevent the enemy from deducing at least one of the following:	Positive Objectives Persuade the enemy to deduce:
1. Where you are	1. You are somewhere else
2. What weapons and forces you have at your disposal (Capability)	2. Your weapons and forces are different from what they are (Capability)
3. What you intend to do (Intention)	3. You intend to do something else (Intention)
4. Where you intend to do it (Intention)	4. You intend to do it elsewhere (Intention)
5. When you intend to do it (Intention)	5. You intend to do it at a different time (Intention)
6. How you intend to do it (Intention)	6. You intend to do it in a different manner (Intention)
7. Your knowledge of the enemy's intentions and capabilities (Capability)	7. Your knowledge of the enemy is either greater or less than it actually is (Capability)
8. How successful his operations are.	8. His operations are either more or less successful than they actually are.

Table 2. Positive and Negative Deception Objectives (After Jones, 1981; Handel, 1982, p. 148)

Positive deceptive acts, on the other hand, are similar to what Whaley characterized as simulation. Positive deceptive acts "persuade the enemy to deduce" something other than the ground truth concerning the deceiver's capabilities and intentions (Handel, 1982, p. 148). According to Van Vleet, these acts thus incorporate "the presentation of the false tale, the deception story…[which] leads the enemy away from the truth" (1985, p. 15).

3. Passive And Active Deception

Michael Handel approached the task of describing how deception works in a somewhat different way. Rather than characterizing deception in the same manner as Whaley and Jones, as a whole comprised of two parts, Handel characterized two distinct types of deception—passive and active. "Passive deception," says Handel, is based primarily "on secrecy and camouflage, on hiding and concealing one's intentions and/or capabilities for the adversary" (1982, p. 133). By way of contrast, "active deception normally involves a calculated policy of disclosing half-truths supported by appropriate 'proof' signals

or material evidence" which must be picked up by the adversary's intelligence network (p. 134). According to Handel, the former frequently receives less attention from casual observers:

> Some experts view passive deception as inferior and not likely to succeed against any competent intelligence organization. This, as we have already seen…is not necessarily true. While measures of secrecy do not have the same aura of romance and intellectual excitement as that associated with active deception, they can frequently be as effective as any more elaborate type of deception operation. *Moreover, active types of deception are dependent on the success of passive deception*.[29] What is even more important, passive deception can tremendously complicate and therefore increase the costs of intelligence work [for the deceived] (pp. 183-184).

Handel's view of deception as either an active or passive proposition, although conceptually distinct, is not inconsistent with the perspectives adopted by Whaley and Jones. Whereas in the descriptions of Whaley and Jones two activities work together to achieve one effect, in Handel's description two distinct activities accompany each other more often than not. The difference is minor at best. Accordingly, if we take all three views in sum, we have adequate reason to conclude that deception is a complex activity that works by simultaneously doing two things: hiding indicators of the deceiver's true capabilities and intentions and showing false capabilities and intentions in their place. Furthermore, in Whaley's theory we find valuable conceptual categories to catalog the subordinate activities by which a deceiver may hope to accomplish these two tasks.

B. DECEPTION AS A PROCESS—A MULTIDISCIPLINARY APPROACH

The first method this thesis described to gain perspective into how deception works, while insightful, has limits in what it can tell us. Although this approach give us an idea of some of the most important sub-activities of the act of deception, it tells us little or nothing about the deceiver, the deceived, their

[29] Emphasis is from the original.

environment, and the interactions between all three. A basic understanding of these various elements, Van Vleet points out, is absolutely critical:

> Deception is not easy to plan. It requires an understanding of a complex process. The enemy is an uncooperative part of that process. The enemy organization and the entire system must be understood in order to control deception signals and project a coherent deception story. Human behavior cannot be predicted, but patterns of behavior can be predicted. The prediction of those enemy human behavior patterns requires an understanding of the nature of the deception process (Van Vleet, 1985, p. 206).

1. What Is A Multidisciplinary Approach?

To gain some perspective into those areas, it is necessary to adopt a multidisciplinary approach similar to the one first taken by Donald Daniel and Katherine Herbig in Strategic Military Deception. In 1979 and 1980, Daniel and Herbig adopted a multidisciplinary approach in "an effort to go beyond the typical single case history of deception based on anecdote" (1982, p. xiii). Observing that there were "as yet few basic concepts established with which to think systematically about deception," the group's aim was to adopt "a more theoretical approach" in order to generate "theories that hold promise for encompassing deception without violating its complexity" (p. xiii). "It is consistent with this research tactic," Daniel and Herbig noted, "to divide the concept of strategic deception into intellectually manageable components and, where possible, apply principles from other disciplines in hopes of gaining theoretical leverage on the concept" (Sherwin, 1982, p. 71).

The resulting multidisciplinary approach combines elements of organizational, systems, and communications theories, along with perspectives into human perceptual and cognitive processes, to attempt to explain how deception works. Organizational theory focuses on the intelligence or information-processing organizations that are on the opposing sides of the deception process. Once the "discrete properties [of these organizations] which remain relatively constant regardless of the personnel who belong to the

organization" are understood, it is theoretically possible to manipulate those factors to perpetrate deception (Van Vleet, 1985, p. 57).

Systems theory focuses on the interaction of the two organizations and their respective and combined environments (Van Vleet, 1985, p. 63). As Van Vleet points out, the environment "is a third part of the [overall] system which [sic] introduces stimuli into sensing capabilities of the two opposing organizations" (p. 64). This environment is dynamic in that it may either "be changed by the actions of either organization or by factors which are out of human control. Unpredictable behavior of the system may be generated by random or unaccountable events caused by the environment or by imperfect knowledge of the predictable events" (p. 64). In order for deception to succeed, this unpredictable behavior must "be adjusted for," according to Van Vleet, since "deception requires the ability to predict future behavior of the system and influence it" (p. 64). Systems theory thus explains the impact of the environment on the deception process, as well as the role of feedback (p. 64).

Communications theory, in turn, describes the flow of information throughout the system, "from a source through an encoder, channel, and decoder, to a destination" (Van Vleet, 1985, p. 46). By mapping and analyzing this linear progression of information, communications theory identifies some of the problems of transmitting deceptive information between a sender and a receiver (p. 46). Among these problems are the introduction of "noise" and its resulting effect on deception efforts.

Finally, psychological theories on perceptual and cognitive biases help to further illuminate understanding of the process of deception. The reason for this is simple, as Richards J. Heuer, Jr. points out: "To be successful, deception must achieve a desired impact on the thinking of the deception target" (1982, p. 31). Theoretically, the more a deceiver understands about the thought processes of the target leaders or analysts, the greater the chance of deception success.

Perception is the process of constructing reality based on the clues the mind receives. Perception is not simply a passive process of seeing, hearing, smelling, tasting, or feeling, but is an active process by which we construct rather than simply record "reality" (Heuer, 1982, p. 33; 1999, p. 19). "Perception answers the question: what do I see?" (Dahl, 1996, p. 10). Cognition, on the other hand, tackles the subsequent question: what does it mean? (Dahl, 1996, p. 10; Heuer, 1982, p. 34). In both processes, "the mind follows certain rules of convenience, sometimes called biases, which are not always optimal ways of sorting out information. Often these biases favor the deceiver" (Daniel and Herbig, 1981, p. 35). Perceptual biases "result from the way the world is perceived and they limit the accuracy of [subsequent] perceptions" (Van Vleet, 1985, p. 81). Cognitive biases "result from the way the mind works," and tend to hinder accurate interpretation (Van Vleet, 1985, p. 81; Dahl, 1996, p. 10). Moreover, "they influence the way that a person treats evidence, attributes causality, and estimates probability" (Van Vleet, 1996, p. 81). Taken together, theories on perceptual and cognitive biases may offer an explanation for how and why deceptive messages are ultimately interpreted the way they are. If deceptions can be designed to take advantage of enemy perceptual and cognitive biases, the target will theoretically do much of the work of deception for the deceiver (Van Vleet, 1985, p. 91). Some common perceptual and cognitive biases are listed in Table 3.

Common Perceptual Biases	Common Cognitive Biases
Expectations influence perceptions. More information and more unambiguous information is required to recognize an unexpected phenomenon than an expected one.	Probability estimates are influenced by availability—how easily one can imagine or remember instances of an event.
Perceptions are quick to form but resistant to change, even in the face of new contradictory evidence.	Probability estimates are frequently anchored by some natural starting point and adjusted incrementally; normally, they are not adjusted enough.
Initial exposure to ambiguous information interferes with subsequent accurate perception, even after more and better information becomes available.	Observers place more confidence in flawed conclusions drawn from a small body of consistent data than more valid conclusions from a larger body of less consistent information.[30]
We tend to perceive our own actions as the result of circumstance; we tend to perceive the actions of others as dictated by motive rather than circumstance or chance.	

Table 3. Examples of Common Perceptual and Cognitive Biases Relevant to Deception (After Heuer, 1982, pp. 62-63; Van Vleet, 1985, pp. 90-91)

These summaries of systems, organizational, communications, and psychological theory only scratch the surface of the respective fields. None does full justice to the intricacies of the theoretical field it summarizes; each description could certainly be expanded in almost infinitely greater depth. That, however, is not the descriptions' purpose. Rather, the point of these cursory descriptions is to demonstrate that each of these theoretical fields is, in effect, a microscope that allows us to examine one part of the bigger picture of the workings of deception. What each of these theoretical fields offers is its own more-or-less simple model that can be applied to gain a better understanding of how various elements of the deception process work.

[30] A phenomenon discussed in great detail by Amos Tversky and Daniel Kahneman in "Belief in the Law of Small Numbers," Psychological Bulletin, 76, pp. 105-110 (1971).

Each of the simple models, however, is inadequate in and of itself to describe the whole of the deception process. As Van Vleet, himself a proponent of the multidisciplinary method, noted, "The overall deception process is more complex than [any one of] the simple models" (1985, p. 101). Hence, in-depth analysis and understanding of deception "requires a thorough understanding of all of the processes involved so that the necessary signals" of a deception "reach the enemy [decision-maker] to result in the correct interpretation and desired action" (p. 101). Taken together in one multidisciplinary approach, each of these disciplines allows us to craft the bigger picture—to describe the elephant, as it were—out of the descriptions of its various parts.

One note of caution is due, however, before we look at the resulting "big picture." As Handel points out, "deception is a creative art and not an exact science or even a craft" (1982, p. 136). Thus, the picture of deception that results from this multidisciplinary approach, no matter how accurate, is still analogous at best. This is the shortcoming of any picture, of course, so—understanding this potential limitation—we drive on.

2. Deception In Theory

The multidisciplinary approach allows us to map deception as a process in a manner typical of a traditional systems model (See Figure 8). At one end of the process are the deceivers. "The deceiver's side," according to Daniel and Herbig, "consists of decision-makers, planners, and implementers. Regardless of who had the inspiration, a deception does not begin until a decision-maker agrees to it" (1981, p. 15). Decision makers generally direct appropriate organizations to plan and execute deception operations in order to induce an adversary to take a certain action favorable to the deceiver. This direction is generally stated in the form of a deception objective that "states the action or nonaction [sic] that the target must take to bring about the desired situation" (Field Manual 90-2, 1988, p. IV-6).

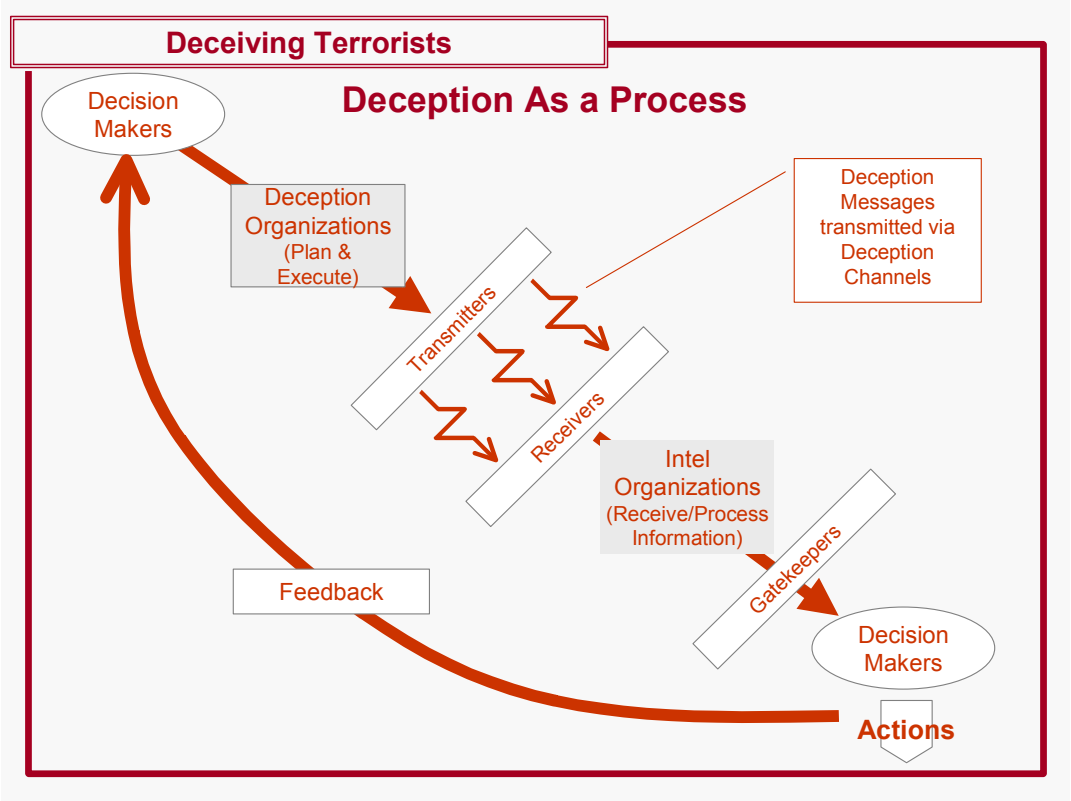


Figure 7. The Theoretical Process of Deception[31]

The deception planner then devises a scenario based on "what he wants the target to think about the facts or event, precisely what it is they should perceive" in order to provoke the desired action (Whaley, 1982, p. 188). Subsequently, the deception planner "must decide specifically what is to be hidden about those facts or impending events and what is to be [simultaneously] shown in their stead" (pp. 188-189). Next, he analyzes the pattern of the activity or object to be hidden to identify the distinguishing characteristics that must be masked, repackaged, or otherwise obscured by dazzling. Moreover, the planner does the same thing for the object or activity to develop a "pattern that plausibly mimicks [sic], invents, or decoys" (p. 189).

[31] This figure is synthesized from the works of a number of different observers, including Donald Daniel & Katherine Herbig (Daniel & Herbig, 1981, pp. 17-21; 1982, p. 8), William Reese (Reese, 1982, p. 99), and Paul Moose (Moose, 1982, p.137).

Once he has identified all of these things, the deception planner determines the means necessary to transmit the scenario. If sufficient means are unavailable, the deception planner has no option but to "return to the drawing board and develop a new scenario that is capable of being transmitted using the available means (Whaley, 1982, p. 189). Once a scenario suitable for the means has been developed, "in the military and intelligence fields, the deception planner usually hands over to operational units to present ('sell') the effect" (p. 189). The message is then "encrypted" into a form that may be transmitted to the adversary's observers and subsequently transmitted through a variety of actions (Daniel & Herbig, 1982, pp. 8-9).

Although Whaley focuses on military and intelligence "operational units," in actuality the transmitter of deception may range from an Army maneuver brigade to a Foreign Service diplomat, from a web page designer to an international businessman. Transmitters may be willing, knowledgeable participants in the deception plan or may alternately be unwitting accomplices carrying out instructions that they believe to attend a different purpose altogether. Moreover, each potential transmitter has its own strengths and weaknesses, its own potential or actual biases, and its own vulnerability to deception and manipulation (Heuer, 1999, p. 88).

Deception messages, in turn, may be the actions of a military unit, the content of a diplomatic message, the content of a web page, or the actions of the businessman; the array of possibilities is virtually limitless, bounded only by the imagination of the deceiver, the "channels" available and the information-gathering abilities, organs, and tendencies of the deception target. Moreover, the messages themselves may be conduit, clues that convey some greater meaning, or content, wherein the deception message is not disguised in any way but is, in fact, the actual intended message.

On the opposite side of the field from the deceiver is the adversary—the target of the deception. Virtually every group seeks information in numerous

ways in order to conduct its normal functions. Thus, the deception adversary potentially gathers (receives) deceptive messages through a variety of receivers. Adversarial intelligence organizations receive, decrypt, and process raw information and analyze it in order to convert it into intelligence (Reese, 1982, pp 105-110). The various resulting messages are, theoretically at least, collated and subsequently passed to gatekeepers—key individuals who screen incoming information and analyses and control the resulting flow of information to adversary decision makers (Daniel & Herbig, 1982, pp. 8-9; Sherwin, 1982, p. 76). Gatekeepers, in turn, "make decisions that affect whether or not the information processed at one level is allowed into the next level of the hierarchy" (Sherwin, 1982, p. 76). Finally, decision makers apply perceptual and cognitive processes to the decoded deception message. "Presumably relying on information received, these leaders make the strategic or tactical decisions that the deceivers seek to influence" (Daniel & Herbig, 1982, p. 9).

Once adversary decision-makers direct action based on these decisions, the deceiver monitors the resulting communications and actions in order to derive feedback as to the effectiveness of the deception. The deception story and subsequent messages are adapted as necessary, and the deceiver adjusts his overall concept of operations accordingly (Whaley, 1982, p. 189; Reese, 1982, pp. 112-113; Moose, 1982, p. 147).

3. Deception In Practice

In practice, however, the process of deception rarely functions as smoothly as Figure 1 and the narrative suggest (See Figure 9). Given the complex nature of the deception process, Herbig and Daniel note, "There are many points at which deception can in theory fail. It is a fragile and risky enterprise" (1981, p. 27). On the deceiver's side, the deception objective and story, though perfectly clear to the deceiver, may be unclear to the adversary upon transmission (Jervis, 1976, pp. 473-474). As with any operation, the transmitters may fail to carry out their orders, may be unconvincing in their actions, or may go unnoticed by the adversary's observers and receivers.

Moreover, actions on the part of the deceiver—as the result of his interaction with the environment, interactions with the adversary, or of the dynamic interactions of actors within the deceiver's organization—may either compromise the deception or render the deception effort pointless.

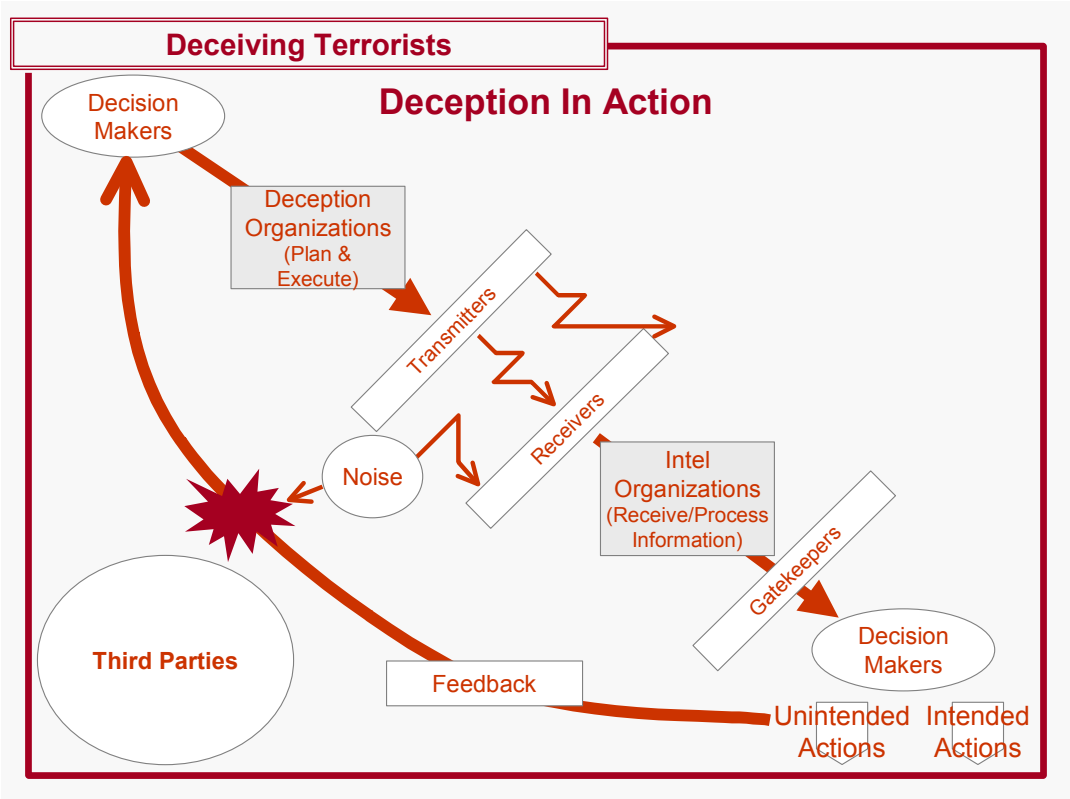


Figure 8. The Practical Process of Deception[32]

In transmission, the various deception messages, in turn, may be distorted in transmission or reception, may be lost or interdicted, or may be ignored, with the target receiving a different signal than intended (Herbig & Daniel, 1982, pp. 9-11; Jervis, 1976, p. 474). Noise may interrupt the deception message as it is transmitted, or may alternately interrupt feedback as the deceiver receives it

[32] Like Figure 8, this figure is synthesized from the works of a number of different observers, including Donald Daniel & Katherine Herbig (Daniel & Herbig, 1982, p. 8), William Reese (Reese, 1982, p. 99), and Paul Moose (Moose, 1982, p.137). Although I do not cite them parenthetically, I certainly acknowledge their influence.

(Reese, 1982, pp. 99-102).[33] Alternately, noise or competing signals of various types may overwhelm the transmission. The message may be lost in transmission and never reach the target.

On the target's side of the deception equation, the target intelligence organizations may receive the transmission, but analysts may garble the transmission or may dismiss the message as trivial or irrelevant. Additionally, analysts may not interpret the deception messages as they were intended, may misperceive other actions taken by the deceiver, or may see through the deception (Jervis, 1976, pp. 474-478). Moreover, "The ever-present possibility of deception always introduces [artificial] 'noise' into the collection and analytical work of intelligence and weakens the clarity of the signals received" (Handel, 1982, p. 143). The transmission may be received and interpreted correctly but a gatekeeper may not allow the information to pass on to decision makers for one reason or another. In turn, adversary decision makers may take no action at all, or may take any of a variety of unanticipated actions. Finally, the transmission may be received and interpreted correctly, only to be ignored by the decision-maker; alternately, it may be received and interpreted correctly, only to prompt the decision-maker to take unintended actions (Herbig and Daniel, 1981, pp. 28-32). In short, even if the target "buys" the deception message, he may do something entirely different than what the deceiver wants and intends; every deception thus may have unintended consequences.

Even if all goes well in the exchange between the deceiver and his target, third parties may take actions that cause a deception to fail or to be altered. On the one hand, third parties may interject their own messages that interrupt, overwhelm, modify, or contradict the deceiver's signals. Moreover, third parties may see through and unmask the deception either intentionally or unintentionally.

---

[33] Although Reese very narrowly defines the concept of noise, he acknowledges the much broader interpretation reached by Roberta Wohlstetter in Pearl Harbor: Warning and Decision. (Stanford, CA: Stanford University Press, 1962). The concept of noise that I apply here is based on both interpretations.

Finally, third parties may be deceived themselves and take unintended actions as a result (Reese, 1982, pp. 99-102; Moose, 1982, pp. 137-138).

Finally, other environmental factors may undo or alter the deception. As time passes, the situation may change and become something quite different. The original deception signals, however convincing and appropriate they might have originally been, “may not elicit the expected action if events overtake them in the meantime” (Daniel and Herbig, 1981, p. 33). Additionally, chance, in the form of bad weather, misplaced orders, bungled execution by any participant, or any of a virtually limitless number of possibilities, may “intervene to prevent action otherwise intended” (p. 33).

Potential Deception Outcomes
Target receives and interprets the signal as intended and takes the desired action
Target receives and interprets signal correctly but the decision-maker ignores it
Target decision-maker receives and interprets the signal as intended but takes an unintended action
The message is lost in transmission and never reaches the target
A competing signal or noise overwhelms the message in transmission
The "clue" is modified or garbled in the channel; the target receives a different signal
The transmission is received but competing signal(s) overwhelm it in interpretation and replace it
Target receives the transmission but analysts garble the interpretation
Analysts receive and interpret signal correctly but dismiss the message as trivial or irrelevant
The transmission is received and interpreted correctly but a gatekeeper prevents it from reaching the decision-maker
Third parties receive deception signal and take unintended action
Third parties interfere with target taking desired action
The situation may have changed and become quite different
Chance—bad weather, misplaced orders, bungled execution of orders by either side, etc.—may intervene

Table 4. Summary of Potential Deception Outcomes[34]

C. WHY DECEPTIONS SUCCEED DESPITE DIFFICULTIES

Obviously, deception seems to be a process fraught with potential pitfalls. These might lead one to conclude that deception seldom succeeds. In reality, though, quite the opposite is true: the historical record suggests that deception often succeeds despite the milieu of potential problems (Daniel & Herbig, 1981,

[34] This list is not exhaustive; rather, it merely illustrates that deception has a wide range of potential outcomes.

p. 33; 1982, p. 10). One reason for this, of course, may be due to the fact that "bungled deceptions rarely appear in a deceiver's historical record" (Daniel and Herbig, 1981, p. 33). Nonetheless, Daniel and Herbig concluded that deception frequently succeeds despite the difficulties for three reasons.

First, every "competitor"—whether a state, organization, or informal group—actively seeks information. This ultimately favors even the clumsy deceiver. Because each competitor does seek information, each is forced to open up communications channels to the outside. Generally, an enormous amount of raw information about the enemy and the situation flows in through these channels in a variety of forms. Even in this deluge of information, a large number of the deceiver's "signals reach the target largely unscathed" (1982, p. 10). Furthermore, a competent intelligence structure or organization tends to evaluate and put together the signals that are received and then fill in the blanks—using intuition—to complete the picture (Heuer, 1999, pp. 35, 90-91). Thus, the target tends to work around the problem of missing information. As a result, not all of the signals making up a particular deception need get through, only enough for the adversary to complete the picture.

Moreover, even given the deluge of raw information, highly reliable information is scarce. As a result, a competitor does not have the luxury to simply dismiss information that appears to be plausible and warns of serious consequences for the receiver. According to Daniel and Herbig, "This puts the benefit of the doubt about the validity of such information on the side of the deceiver, for it ensures his deceptive clues a hearing by his target" (Daniel and Herbig, 1981, p. 34). In such a case, ambiguity is increased for the target even if he is not ultimately misled.

Second, the processes of human perception and cognition tend to conspire against the deceiver. As Daniel and Herbig note, the deceiver "is more often betrayed than served by his own processes of thought" (1981, p. 34). Several biases in particular "converge to put a target of deception at the mercy of

his initial impressions," especially if reinforced by a deceiver as part of a deception (p. 34):

> Expectations shape what we in fact perceive; perceptions are quick to form but resistant to change; initially ambiguous perceptions delay the ability to clarify an assessment even when clear-cut evidence becomes available; estimates of the probability of some future events cluster around an initial starting point and resist radical alteration; and even after evidence has been completely discredited, the impressions based on it often persist and shape one's thinking (Daniel and Herbig, 1981, p. 36).

The effect of these biases on analysts, gatekeepers, and decision-makers alike is fairly evident. Deception targets unknowingly and unwittingly "help" deceptions along through the maze of potential problems. As a result, deceptions often succeed despite what appears to either the deceiver or the detached observer to be obvious and overwhelming contradictory evidence.

Third, the inherent uncertainties of international conflict tend to forgive or cover up many of the deceiver's mistakes. Even in peacetime, "traditional diplomatic and other forms of verbal communication are extremely susceptible to twisting, misconstruction, and even honest misunderstanding" (Arquilla, 1993, p. 171). In periods of conflict, this phenomenon is magnified. According to Daniel and Herbig, "Especially in competitions where virtually all data are ambiguous and to some degree suspect, so often the case in war, the situation forgives most of the mistakes a deceiver makes" (1981, pp. 36-37). Contradictory actions and "even leaks which come from well-placed sources" that the target trusts "or over channels which are usually reliable" must compete against the range of alternatives that the target's hypotheses and evidence suggest (p. 37). Furthermore, even these contradictory pieces of evidence are susceptible to many of the same outcomes as the deception signals themselves. As a result, "What seems to the deceiver a glaringly bright give-away often seems to the target either too good to be true or only one more among his many grey-colored clues" (P. 37).

D. DECEPTION SUCCESS FACTORS

A number of well-meaning observers have approached deception, usually from a historical case study perspective, and attempted to divine some resulting set of simple maxims, list of rules, or compilation of lessons learned for those who would practice deception. Invariably, however, the vast majority of these maxims, rules, and lessons prove to be either overly simplistic or wrong.[35] Moreover, such maxims and rules may actually do more harm than good; if one attempts to practice deception without a detailed understanding of how it works, cookie-cutter instructions will almost certainly lead to failure.

A more beneficial approach is to look at how deception works to see what qualities or factors seems to contribute to successful deception, regardless of situation or context. In the last quarter of the Twentieth-century, a number of observers took this alternate approach (for a summary of deception "success factors," see Table 5). One such pair of observers already quoted in detail in this work, Donald Daniel and Katherine Herbig, identified "Five Factors Conditioning the Success of Deception" (1982, p. 15). Another observer, Major Donald Bacon, in a study of World War II deception operations, noted "seven primary factors [that] enabled successful…deception operations" (1998, p. 13). More recently, Roy Godson and James Wirtz suggested four components of "a successful denial and deception campaign" (2000, pp. 426-427).

---

[35] One example is Charles A. Fowler and Robert F. Nesbit, who, in 1995 issued six "rules" for successful tactical deception. Although there is much of value in their article, their rules can be misleading to those who do not fully understand deception. The first of these rules was, "To be effective, a deception operation must be one that causes the enemy to believe what he expects" (p. 41). Richards Heuer, Daniel and Herbig, Van Vleet and others have proved that this is simply not the case.

Daniel and Herbig	• Secrecy, organization, and coordination; • Plausibility and confirmation of the lie; • Adaptability of deception; • Target predispositions; and, • Strategic initiative (1982, pp. 15-25)
Godson and Wirtz	♦ ♦ perceptual context ♦ ♦
MAJ Donald Bacon	• Control key channels; • Intelligence preparation and intelligence feedback are critical; • Need high-level and centralized deception planning; • Sound deception execution: plausible stories and preexisting beliefs, conditioning, and putting the puzzle together; • Deception supports strategic and operational objectives; • Maintain secrecy; and, • Deception requires time (1998, p. 13).

Table 5. Observations on Deception "Success Factors"

The twin luxuries of academic comparison and hindsight allow us to pare this list of potential "success factors" down somewhat, as well as to add one that has previously been overlooked. As a result, four factors in particular can be identified as integral to the success of deception: centralized control, coordination, and integration; intelligence; adaptability and feedback; and plausibility and confirmation.

1. Centralized Control, Coordination, and Integration

The relative complexity of the deception process dictates that centralized control and detailed coordination are essential components of successful deception operations. Centralized control and detailed coordination contribute to the success of deception by facilitating mutual support between deceptions and actual operations. This mutual support subsequently contributes to the likelihood of success by insuring against compromise of the deception, by facilitating protection of limited resources, and by facilitating positive control.

The mutual support afforded by centralized control and detailed coordination is a critical underpinning of simultaneous simulation and dissimulation. To successfully deceive, "The overall activity must not only provide believable indicators of the false operation, but must deny believable indicators of the real operations" (Fowler and Nesbit, 1995, p. 44). To achieve mutual support, Fowler and Nesbit advise, "Deception must be integrated with [actual] operations" (p. 44). "The deception plan should never be created independently from the operations plan," they observe, but rather, "operation and deception plans must complement and support each other" (p. 44). "The two plans," Van Vleet notes, "must be mutually supporting if the deception is to be optimized" (p. 200). Deceptions are "well coordinated," he suggests, "when directed from one central point—that being the highest headquarters" or lead agency controlling assets "directly benefiting from the deception" or when the activities of the various agencies are coordinated sufficiently to prevent the compromise of the deception (Van Vleet, 1985, p. 19). This ensures that "all instruments of power are integrated into deception planning, and all actions are consistent with the deception story" (Bacon, 1998, p. 17). Moreover, Bacon adds, "high-level centralized planning ensures that critical information, which otherwise might remain compartmentalized, can be shrewdly exploited for deception purposes" (p. 17).

Centralized control and detailed coordination, while certainly necessary for any deception, is especially important for higher-level deception operations, according to Godson and Wirtz:

> [High level deception and denial] campaigns require coherent, if not coordinated, action from many departments, agencies, or ministries. Public statements, press articles, and Internet communications must [all] be shaped to support the goals of the nation intent on deception (Godson and Wirtz, 2000, p. 426).

The mutual support achieved by centralized control and detailed coordination additionally contributes to the likelihood of deception success by insuring against the possibility of compromise. "Deception must be well organized and well coordinated," notes Van Vleet, "else leaks may occur and deception unravel" (Van Vleet, p. 19). Deceptions, especially high-level deceptions, may be compromised by either security leaks or by the incongruent activities of other agencies and organizations. In practice as well as ultimate effect, there is little difference between the two. If, for example, the CIA and the State Department "expose" a strategic military deception by their incongruent activities, the outcome is virtually the same as if a secret had been inadvertently slipped.[36] Current American military doctrine attempts to institutionalize this concept. Joint Publication 3-58 offers six principles of military deception; the third of the six is centralized control. In explanation, JP 3-58 states, "a deception operation must be directed and controlled by a single element" in order to avoid confusion, compromise, "and to ensure that the various elements involved in the deception are portraying the same story and are not in conflict with other operational objectives" (1996, p. I-3).

It is necessary to mention at this juncture that herein lies one of the more notable paradoxes of deception. While centralized control and detailed

---

[36] American practitioners of strategic deception should, of course, observe that there is a considerable amount of "incongruence" or friction in the various, day-to-day activities of the United States government. A deception in which all the activities of the US government were seamlessly synchronized (admittedly not a likelihood), might appear too good to be true.

coordination are necessary to avoid compromise, they may also be sources of compromise. The more individuals and agencies that are brought into "the know" on a particular deception, the greater the risk of exposing the deception by some kind of security breach. Thus, the need for centralized control and detailed coordination must be balanced on a case-by-case basis with the potential risk of compromise of deception operations.[37]

Centralized control and detailed coordination also protects limited resources. Competition for finite resources is a dilemma that every commander faces at one point or another. Even for a resource-rich nation such as the United States, there are rarely enough resources for a decision-maker or commander to do all that he would like to do. As John Van Vleet points out, "Competition for resources…is such that the requirements [to carry out deception] will have to be filled using the existing force structure. Any proposal for how to do that will have significant drawbacks and will produce many reasons that it cannot be done" (Van Vleet, p. 229). Centralized control and detailed coordination is the mechanism by which conflicts over scarce resources can be resolved.

Finally, Richard Schultz captures a fourth potential contribution of high-level, centralized control in The Secret War Against Hanoi, his history of covert operations during the Vietnam War. Since the Vietnam War, Schultz suggests, American presidents have routinely mixed eagerness "to employ covert methods [including deception] to accomplish specific policy objectives, " with apprehension "over the trouble they could cause if exposed" (Schultz, 1999, p. 336). The political and strategic risks of exposure are very real concerns for high-level decision-makers. High-level, centralized planning and detailed coordination facilitate the oversight required by the inevitable combination of "interest and caution" (p. 336).

---

[37] Some Pentagon staffers refer to a "feel the magic phenomenon" that exists around sensitive operations such as deceptions or special operations direct action missions. Such operations are being planned, it seems, many individuals who have no real need-to-know (but who are otherwise

2. Intelligence

Good intelligence is an integral part of every successful deception operation from inception to completion. As Daniel and Herbig observed, "Accurate intelligence on what the adversary is intending and how he is reacting is one of the basic goals in any competition, but for deception it has particular importance" (1982, pp. 20-21). "Knowledge of what the enemy will accept as plausible and what degree of confirmation is necessary before he will believe," says Van Vleet, "is a firm requirement for a successful deception" (1985, p. 191). "Knowledge of the enemy organization," in turn, "is the key to prediction of how the enemy will react to the information he receives" (p. 191). Bacon concurs, expanding on the significant role of intelligence:

> Deception planners need intelligence to identify enemy perceptions, channels of information, and susceptibility to deception. Planners also need methods to gather feedback. Allied intelligence successfully provided such information [during WW II], whereas Germany's intelligence failed. The Allies won the intelligence war[38] and the impact was most prominent with Allied deception efforts (Bacon, 1998, p. 16).

Intelligence performs five critical roles in the planning and conduct of deception. First, it allows identification of adversary decision-makers and assessment of their vulnerability to deception (JP 3-58, 1996, p. II-2). Second, it facilitates determining the adversary's preconceptions of friendly capabilities and possible courses of action (p. II-2). Third, intelligence permits the development of estimates of adversary actions under various friendly actual and deception scenarios (p. II-2). Fourth, it makes it possible to identify adversary information gathering capabilities and communication systems to determine the best conduits for a particular deception (pp. II-2-3; Sherwin, 1982, pp. 79-80). Finally, it

---

understandably motivated by curiosity) appear out of the woodwork wanting to "feel the magic" of knowing what is going on.

[38] While the Allies unquestionably won the intelligence war, there are some historical indications that they had help from inside Germany's intelligence organizations. For a more detailed history,

facilitates the establishment and monitoring of feedback channels to evaluate the effectiveness of the deception operation by observation of the adversary's reaction (JP 3-58, 1996, p. II-2). This, in turn, facilitates the adaptability of deception to the changing situation. Moreover, intelligence preparation allows the deception planners to develop reliable measures of effectiveness (MOE) to gauge deception effectiveness.

The role of intelligence in allowing deception design to be based on enemy preconceptions is especially significant. "To be successful" at deception, suggest Godson and Wirtz, "the deceiver must recognize the target's perceptual context to know what (false) pictures of the world will appear plausible (2000, p. 426). Once a target's preconceptions and cognitive biases are known, a deceiver may customize a deception in three ways. First, the deceiver has the option to devise a deception story that "fits" and thus capitalizes on the target's preconceptions. The American invasion of Tinian, discussed earlier in this chapter, capitalized on Japanese expectations. The Japanese defenders of Tinian were deceptively encouraged to believe that the scenario that they thought most likely was, in fact, coming true (Whaley, 1969, pp. A-394-395). By the time the Japanese realized their error and were able to respond to the actual operation, the Marines had established a solid beachhead on the island.

Alternately, the deceiver may be forced to devise a deception that goes against the target's preconceptions. Van Vleet, Heuer, and Daniel and Herbig have all theorized that to do so—to convince the enemy that what he doesn't expect is, in fact, true—is harder to carry off than deceptions that fit the target's preconceptions. The literature on perceptual and cognitive biases tells us that to do so generally requires "a considerable and concentrated shock" to the target's system (Daniel & Herbig, 1982, p. 23). The Mincemeat deception, discussed in Chapter I, is one example of a deception that successfully challenged the target's

---

see W.B. Breuer, Hoodwinking Hitler: The Normandy Deception, Westport, CT: Praeger Publishers, 1993.

initial preconceptions. The introduction of a windfall of authoritative evidence proved to be sufficient catalyst to induce Hitler and his high command to change their notion of where the Allied Mediterranean assault would come.

Finally, if the target has no observable preconceptions regarding a particular activity or if sufficient intelligence information is not available to ascertain the target's preconceptions, it is possible to create certain expectations on the part of the target. "Here, the deceiver sets up the target for a future surprise by conditioning him to expect something he hadn't considered before" (Daniel and Herbig, 1982, p. 24). In early 1942, the Germans used this concept to cover the escape of the destroyers Scharnhorst, Gneisenau, and Prinz Eugen from the barricaded port of Brest. Over the course of several weeks, the Germans conditioned the British to expect a certain amount of radar jamming at the same time every day in the area. Ultimately, the British came to attribute this jamming to atmospheric interference. On 12 February 1943, the Germans again jammed the British radars; this time, however, the three destroyers used the deceptive jamming cover to slip to sea without being noticed or engaged by the British Navy (FM 90-2, p. I-5).

The connection between intelligence and successful deception is hardly confined to the modern era of warfare, however. Although intelligence staffs, agencies, and organizations as we know them today are arguably a Twentieth-century phenomenon, the link between intelligence and deception is much older (Van Creveld, 1985, p. 4).[39] J. Bowyer Bell and Barton Whaley observed that the Mongols recognized the importance of intelligence more than 750 years ago:

[39] Of course, successful generals and rulers have always sought intelligence, employing a variety of means. Van Creveld's point—and mine—is that large, standing intelligence organizations like the Central Intelligence Agency (CIA) or the Komitet Gosudarstvennoy Bezopasnosti (KGB) are twentieth-century inventions.

> Mongol strategic intelligence was superb. Their campaigns were planned and launched only after detailed and political military information had been obtained, information that gained them many bloodless victories through bribery, treason, or alliance.[40] This fine intelligence also enabled the Mongols to design highly effective strategic psychological warfare programs, by means of which they panicked, demoralized, and terrorized their prospective victims, again sometimes inducing surrender without battle (1991, p. 30).

Intelligence—particularly intelligence preparation and feedback—has proven to be a critical success factor in deceptions throughout history. There is every indication that this trend will continue.

3. Adaptability and Feedback

"A deception campaign," Godson and Wirtz tell us, "is a dynamic enterprise" (2000, p. 427). The situation of both deceiver and target is in constant flux. The resulting implication for deception, Van Vleet points out, is that "the simple deception plan that has only one explanation may deviate from the system reality too soon to receive confirmation" (1985, p. 192). Accordingly, notes Van Vleet, "The deception must be able to change as reality changes" (Van Vleet, p. 191). "Cover stories, communications channels, and specific initiatives require fine tuning to take advantage of unforeseen opportunities or problems" (Godson and Wirtz, 2000, p. 427). As a result, adaptability is a necessary component of every successful deception. "An adaptable deception," in turn, "requires the ability to react to change and also requires knowledge about when to react. The ability to react to change is a function of planning and execution flexibility," as well as of "coordination and intelligence" (p. 192). Adaptability allows the deceiver to continue deceptions for a longer time, to react to unforeseen changes in the situation, to take advantage of unforeseen or unpredictable enemy actions and reactions, and to protect valuable intelligence

[40] The Mongol campaigns made extensive use of "feints, demonstration attacks, camouflage by raising dust clouds to conceal movement or exaggerate strength, stuffed dummies on spare horses, false campfires, ambushes, and especially the carefully rehearsed feigned flight intended to lure the enemy into a precipitate charge" (Bell & Whaley, 1991, p. 30).

and deception resources by ending the stratagem if the deception wears thin or is compromised (Daniel and Herbig, 1982, p. 21; Sherwin, 1982, p. 80). Furthermore, adaptability provides some degree of "insurance" against intelligence shortcomings or failures. As Van Vleet points out, "Alternative planning does not reduce the demands for quality intelligence, but it does provide more security against the possibility that the intelligence is wrong or that it becomes 'fogged'" (Van Vleet, p. 227).

If adaptability is a necessary component of every successful deception, feedback is the mechanism that makes adaptability possible. "The ultimate asset that allows deceivers to adapt their scenarios" to changing situations, Daniel and Herbig point out, "is feedback from the target" (1982, p. 20). Feedback is necessary, notes Van Vleet, "if the deception planner is to know if the enemy has interpreted the signals in the desired manner so that the deception…can continue as planned or so that the execution can be modified to produce the desired effect (1985, p. 194). Godson and Wirtz point out: "To pursue a course of action that relied on deception if the target failed to 'take the bait' would be foolhardy. Alternatively, if an initial deception plan failed, the feedback mechanism could activate backup [deception and denial] campaigns" (Godson and Wirtz, 2000, p. 427).

Reliable measures of effectiveness (MOE) are a key component of feedback. The deceiver must develop MOE that tell him whether the adversary has taken notice of the deception, found the deception relevant or irrelevant to his own concept of operations, formed the intended hypothesis about the meaning of the deception and taken the appropriate action, taken some other unintended action, or failed to detect the deception (Whaley, 1982, p. 189). MOE must be flexible enough to shed light on alternative explanations for enemy perceptions and actions. Furthermore, in order to be truly effective, MOE must allow sufficient time both for the deception to work and for the deceiver to adapt his plans if the deception does not work.

The deceiver has three basic options when feedback indicates that the situation has changed and the original deception is in danger of failing. The deceiver's first option is to abandon the deception. While this option has the advantage of preserving key resources for later use by the deceiver, it may also increase certainty for the target about the deceiver's true course of action. The second option open to the deceiver is to continue the deception in hopes of producing or increasing ambiguity for the adversary. Even if this option succeeds, however, it may ultimately reduce the deceiver's flexibility by committing him to an operational concept or course of action that is untenable. The deceiver's third option is to attempt to adapt the deception to fit the new reality. The final course of action is generally also the most desirable, although often the most difficult, (Van Vleet, pp. 191-192). Regardless of which course of action the deceiver chooses, "It seems reasonable that when a change must be made, that change should be to adopt an alternative that has been carefully evaluated" (Van Vleet, p. 215).

4. Plausibility and Confirmation

One of the most basic problems of deception is creating a story and indicators that the target will accept as valid (Reese, 1982, p. 107). Plausibility, therefore, is a prerequisite for deception success. Citing the conclusions of both SHAEF and German planners from World War II, Daniel and Herbig note that in order for a deception to succeed, "the lie must be plausible" (1982, p. 17). One of the key components of plausibility, Van Vleet points out, is enemy perceptions regarding the deceiver's capabilities and intentions: "An important consideration in deciding whether the enemy will accept the plausibility of the deception story is determining whether the deception plan might be acceptable" to the enemy as the real plan (Van Vleet, 1985, p. 190).

The historical record suggests that deceiver decision-makers often reject deception concepts not because of their relative costs, but rather because the concepts seem implausible to the decision-makers. Simply put, decision-makers often believe, based on the insights afforded by virtue of their own privileged

positions, that because a particular course of action is either not possible or not feasible, the target will reject it as a deception. Roger Hesketh and Ewen Montagu both note their own experiences with this phenomenon as deception planners during WW II (1982, p. 236); Hesketh also notes that this is a logical fallacy.[41][42] "What is or is not possible" from the deceiver's point of view, notes Hesketh, "matters less than what the enemy believes is possible" (p. 236). Hesketh goes on to point out that "One is always inclined to credit the enemy with knowing as much about one's own affairs as one does oneself" (p. 236). In fact, he suggests, "A reasonable and straightforward story, even if it involves maneouvres which cannot in reality be performed," is preferable to "a more complex one which is capable of execution," but whose objects and activities the adversary is much less likely to discern (p. 236).

A key component of plausibility is confirmation. "A lie is made more plausible," according to Daniel and Herbig, "when it has been confirmed by a variety of credible sources" or means (1982, p. 18). Confirming details are necessary because virtually every target of deception continues to seek information to support his conclusion. "The usual [proximal] targets of deceptions, intelligence organizations," according to Daniel and Herbig, demand "that all claims be confirmed and evidence evaluated and ranked according to its estimated reliability" (p. 18). Given the role of perceptual and cognitive biases, a target is far more likely to accept data that confirms his hypotheses: "the target is likely to ignore, twist, or explain away those details that do not fit, and often those

---

[41] Montagu describes in great detail an incident in which the British Chiefs of Staff rejected a deception intended to convince the Germans that an invasion would come at the Bay of Biscay. Although Ultra suggested that the Germans greatly feared such an operation, the Chiefs of Staff knew that an invasion in this area was beyond the range of fighter aircraft support. The Chiefs of Staff reasoned that certainly the Germans would know this as well. In fact, the Germans either did not know or did not seem to care, but the deception was scrubbed nonetheless (Handel, 1982, p. 135).

[42] Roger Fleetwood Hesketh served as the head of the "Intelligence" or "Special Means" subsection of OPS (B), the section of the Chief of Staff Supreme Allied Commander (COSSAC) designated to handle strategic deception, from April 1943 until the end of World War II. Among Hesketh's responsibilities were the coordination of the actual Allied operations, physical

are the incongruities on which the deception hinges" (p. 19). If there is no confirming data, however, the target is likely to receive sufficient contradictory information to overcome his cognitive biases and see through the deception more easily.

5. Secrecy—A Fifth Success Factor?

Finally, the nature of the complex process that is deception suggests that deception success requires maintenance of a certain threshold of secrecy. Daniel & Herbig cite a review of German cover and deception by General Hans von Greiffenberg: "knowledge that cover and deception is [sic] being employed must be denied the enemy" (Daniel & Herbig, 1982, p. 16). "'If the strictest secrecy is not observed,' says von Greiffenberg, 'all deception projects are condemned to failure from the very start'" (p. 16). Daniel & Herbig conclude that there are two levels on which such secrecy must be maintained. "One tries to protect the truth about what a side [actually] intends to do in an impending operation," while the other tries to "protect the truth about the existence of the deception itself" (p. 17).

There is considerable evidence, however, that secrecy—although important—need not be absolute. Daniel & Herbig point out, "Total security is an elusive, usually unattainable goal even in the best organized and coordinated operations" (1982, p. 16). As a result, "Breaches of security…need not be fatal to deception's success. Some leaks may not catch the target's attention, and, if they do, may only increase his ambiguity[43]. A target's predispositions may cause other leaks to be ignored or misinterpreted as to their true significance" (Daniel & Herbig, 1981, p. 37; 1982, p. 17). Furthermore, so long as the deception is planned to reinforce the target's existing preconceptions, "the target's propensity to rationalize discrepancies commonly offsets security leaks and uncontrolled

---

deception means, and the controlled leakage of information using double agents (Hunt, 1982, p. 225).

[43] What Daniel & Herbig do not point out is that increased ambiguity, coupled with increased risks, may make an adversary more unpredictable, rather than less so (Jervis, 1968).

channels of information" (Daniel and Herbig, 1981, p. 37; 1982, p. 16). Furthermore, Whaley's empirical analysis suggests that deception has a "high probability of achieving surprise even though a warning has been given" (Sherwin & Whaley, 1982, p. 192). In fact, Sherwin and Whaley's analysis implies that the probability of achieving surprise *despite* warning is more than 90% (p. 192).

Since absolute secrecy is likely to prove elusive or overly expensive to attain, a more reasonable goal for deception might be relative secrecy, coupled with plausibility and confirmation of the deception. These qualities are interrelated. Relative security prevents *significant* indicators of either the deceiver's actual operational concept or of the existence of deception. Confirming details from a variety of sources augment plausibility, a necessary component of deception; together, these work to mitigate minor security leaks.

Having addressed what deception is and how it works, this thesis now transitions to its central theme—deceiving terrorists. Chapter III addresses that theme.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DECEIVING TERRORISTS—ORGANIZATIONAL APPLICATIONS

At the beginning of December 2001, a fresh wave of violence rocked the Middle East.[44] Late in the evening of 2 December, a pair of serious-looking young Palestinian men walked into Jerusalem's Zion Square shopping complex and blew themselves up. The initial explosions killed nearly a dozen—including the two bombers—and wounded almost two hundred, the vast majority of whom were marked as victims simply because they happened to be Israeli citizens. Just as in a hundred other instances, the well-practiced Israeli emergency response system swung into action immediately following the initial explosions. Rescue workers were just beginning to arrive at the scene a few minutes later when a third explosion—this one a car bomb—targeted the emergency responders themselves. Less than twenty-four hours later, a third young Palestinian man boarded a bus in Haifa, quietly paid his fare, and took his seat. Moments later, he detonated the bomb strapped to his body, killing himself and a number of his fellow passengers and turning the bus into a moving fireball. The burning bus careened across the centerline of the road, slamming into another crowded bus. More than a dozen people died and nearly three dozen were injured in this latest incident.

Chairman Arafat of the Palestinian Authority quickly denounced the attacks, but Hassan Abdel Rahman, Palestinian representative to the United States, suggested that the attacks were the result of "the conditions that are created by Israel that makes the Palestinian people very angry and very frustrated" (CNN, 2001). These latest suicide attacks, however, were not merely the coincidental acts of a trio of disillusioned young Palestinian men indignant at a system that repressed them, as Rahman claims. Such an explanation, although certainly containing strong strands of truth, is misleading. With only a few exceptions—most notably Ted Kaczynski and Tim McVeigh—terrorism is

[44] Admittedly, these acts represented the latest round within the second Intifadah. Thus, in a larger sense, they represent neither beginning nor end.

predominantly the deliberate act of groups rather than disgruntled individuals. "The brutal, sometimes criminal, activists who do [terror's] bidding," Gerald McKnight points out, "are simply instruments. Behind every act of planned terror and clandestine revolt is a brain, highly specialized and tuned to guerrilla warfare" (1974, pp. 68-69). If McKnight is correct, then some counter-terrorism measure is necessary that targets not just the individuals who carry out the violence, but also the brain behind the violence. Deception, it seems, is one potential means of striking at that brain.

A. INTRODUCTION

The historical record suggests that deception has considerable counter-terrorism potential. In particular, states may use deception to create and exploit inefficiencies and weaknesses in terrorist organizations, to facilitate counter-terrorist operations, and to conceal counter-terrorist intentions.

The purpose of this chapter is to explore these potential uses of deception in greater detail. In order to determine whether any of these potential utilities holds value, some discussion of the concept or theory underlying each use is necessary. Next, it is essential to try to unearth historical examples to support those theories. Finally, each historical example must be examined in detail in order to determine the lessons to be learned or conclusions to be drawn from the examples. Only then can we proclaim with any confidence that these utilities hold promise as real-world counter-terrorism applications.

The study of state use of deception, particularly deception against terrorists, does not promise to be a simple process. As Maurice Tugwell pointed out, "By its very nature, deception is very difficult to research and document. The most successful examples presumably delude us and remain undetected. Many others so muddy the waters that the truth and falsehood remain indistinguishable" (1990, p. 20). This is certainly the case concerning counter-terrorism deception. Because the "war against terrorism" is not over, secrecy continues to shroud many of the counter-terrorism operations and campaigns of

the last half-century or so.[45] Only occasionally is the veil of secrecy pulled back to reveal the mysteries underneath. As a result, Ronald Sherwin noted, "there are few [well-documented] empirical cases from which to draw generalizations and data, and the available data may be filtered to protect national security interests" (1982, p. 71). In the end, however, there may yet be enough glimpses behind the veil to allow us to draw solid conclusions about the potential utility of deception.[46]

B. THE NATURE OF THE BEAST—BACKGROUND ON TERRORIST ORGANIZATIONS

Before the discussion about deceiving terrorists is joined, there are three questions that must first be addressed concerning the nature of terrorist organizations. While these observations most directly affect the efficacy of the first kind of counter-terrorist deception, they have some relevance across the spectrum of such deceptions. First, what is the general nature of the organizations that occupy the lower right side of the process diagram established in Chapter II (see Figure 10)? Do these organizations possess any unique characteristics that may be exploited for the purposes of deception? In theory and in practice, a general understanding of this nature seems vital for those who would deceive terrorists.[47]

Second, how do terrorists and terrorist organizations undertake those activities shown in the center of the diagram—specifically, how do they gather

---

[45] The vast majority of details of Allied deception during WW II remained secret for more than a quarter of a century after that war ended. Only in the 1970's did information begin to surface about the scope and nature of those operations. Details about Soviet deception and disinformation campaigns against activist Russian émigrés only emerged in the period following the collapse of the Soviet Union. Given these perspectives, it is understandable that there may as yet be a lack of solid information concerning recent deception operations against terrorists.

[46] The veil of secrecy is not limited to recent deception operations against non-state actors. Rose Mary Sheldon has noted that accounts of Roman deception against tribes and other non-state actors, though suggestive, are conspicuously deficient in detail. She suggests that the one-sided nature of the literary evidence, coupled with the "official" Roman line disdaining "anything that appeared artificial or disingenuous," is to blame (1997, p. 300).

[47] On this point, it seems particularly important to heed Sun Tzu's advice to know the enemy's "way"—*tao*—in order to gain the strategic advantage—*shih* (Carr, 2000, pp. 73-74).

and process information? Is there anything in those processes and procedures that the deceiver can exploit to gain a competitive advantage? The answers to this question, in turn, may suggest the means by which deception may be "transmitted" to the target.

Finally, is the general nature of terrorist organizations changing, and, if so, what are the potential implications of those changes? If one hopes to establish any general theory about deceiving terrorists, something akin to Whaley's general theory on deception, one must understand not only what the historical record holds regarding how terrorists have operated in the past, but also what the future appears to hold.

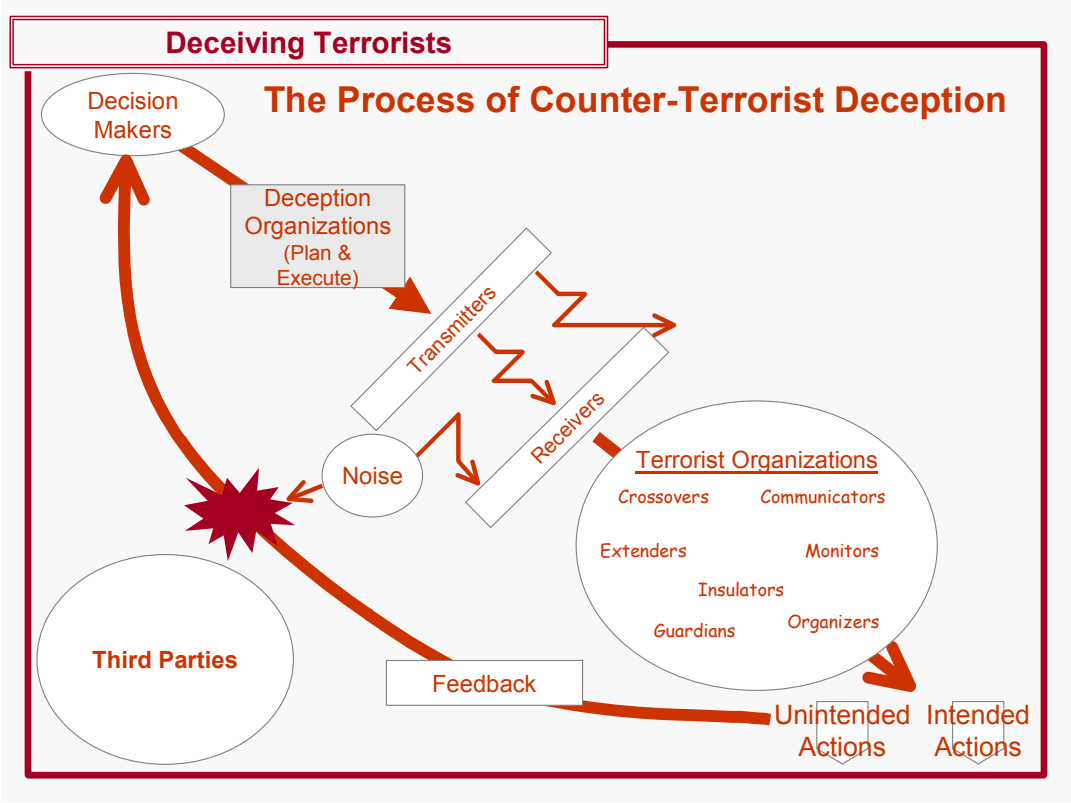


Figure 9. Another Glimpse Of The Process Of Deception

1. The Difficulties Of The Dragonworld[48]

Making universal proclamations about the general nature of terrorists and terrorism is, of course, risky business, academically speaking. That is certainly the case when one talks about the potential complications that terrorists face on a day-to-day basis and how terrorist and insurgent organizations gather information. It is extremely difficult to reach conclusions that apply equally to the overwhelming majority of cases. This is due in no small part to the enormous differences that may exist in terms of terrorist ideology, goals, means, size, membership, and organizational structure. Still, for more than a quarter of a century, one historian—J. Bowyer Bell—has made detailed studies of the nature of terrorist, guerrilla, and insurgent organizations that generally "get it right."[49]

a. The Dragonworld

Bell suggests that the terrorist operates in a world and with a sense of reality that is far different from that of the vast majority of "civilized" people. Bell dramatically and figuratively describes the world of the terrorist as "a world filled with monsters, a Dragonworld" (1999, p. 61). Bell's terrorist Dragonworld "is 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). The terrorist generally seeks legitimacy for himself and his cause; this legitimacy is only purchased at the risk of exposure to direct counter-terrorist action (1990, p. 200).

---

[48] This discussion of the general nature of terrorists and terrorist organizations is admittedly cursory. Countless volumes exist on terrorism; the discussion offered here only touches on one aspect of terrorist organizations. For more on the subject, see the works of Hoffman, Crenshaw, Bell, and Reich listed in the Bibliography.

[49] Bell has not merely studied terrorism from the "ivy-covered walls" of his office at Columbia University, but has been a frequent and long-term eyewitness to conflicts in Beirut, Belfast, Aden, Gaza, Ethiopia, Central Africa, Italy, Cyprus, and others. While Bell's work does have its shortcomings, most notably a tendency toward lengthy, flowery phrases and sweeping generalizations, few scholars can truthfully claim to have been offered a ride on a car bomb, to have been kidnapped by revolutionaries, or even to have assisted in the medical treatment of wounded guerrillas. The fact that Bell can claim all of these things, coupled with his knack for generally "getting it right," generally excuses his shortcomings.

One of the defining aspects of this terrorist ecosystem, according to Bell, is inefficiency. "A revolutionary organization engaged in an armed struggle is inherently inefficient," he writes, "a price paid for the capacity to persist" (1990, p. 193). To accomplish even the simplest task, Bell suggests, the terrorist must overcome the always-present "enormous penalties in the covert, a myriad of obstacles to action, and obstacles always increasing" (1990, p. 194). "It is impossible to overstress the penalties paid by those on the run," Bell tells us, "who must survive, appear normal, and still operate. Error or bad luck is almost always irreversible. The simplest task," he says, "is complex. The strain is constant. The covert support mechanism is always stretched" (p. 194).

b. The Efficiency-Security Tradeoff

Perhaps the single most dominant characteristic shared by clandestine organizations, Bell repeatedly suggests, is the inherent tradeoff between security on the one hand and operational efficiency on the other: "As a general rule, the greater the secrecy, the greater the inefficiency of the organization or operation; absolute secrecy assures absolute chaos" (1990, p. 203). Even for an organization that seeks armed confrontation, secrecy is a must. The "typical" terrorist organization cannot afford to waste limited resources on haphazard meeting engagements; rather, the terrorist organization must husband these assets to be used when and where they can achieve the greatest effect.

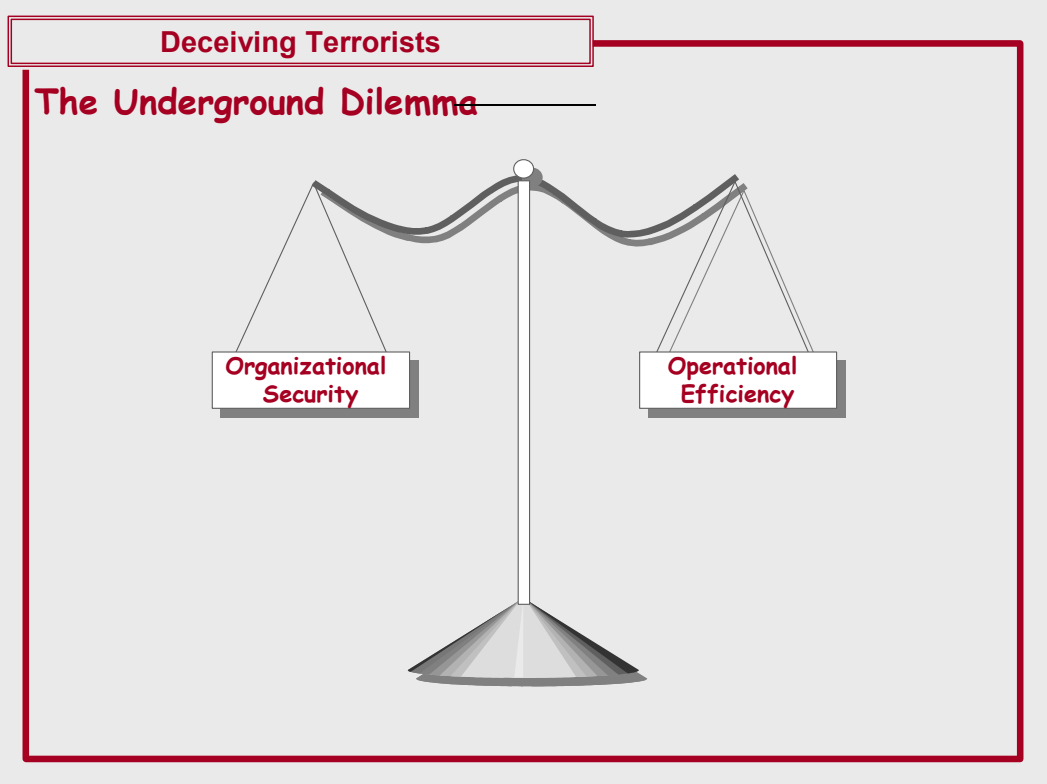


Figure 10. The Traditional Underground Dilemma—Security Versus Efficiency

Gordon McCormick and Guillermo Owen have expanded on Bell's concept of the security-efficiency balance. Every clandestine group, they observe, faces a critical tradeoff "between its operational capacity on the one hand and its level of operational security on the other" (2000, p. 190). According to McCormick and Owen,

> This tradeoff is a defining characteristic of underground (and other secret) organizations which, in distinction to their "above ground" counterparts, must worry about minimizing their risk of exposure, even as they worry about the competing need to maximize their capacity to operate (p. 190).

The implication of this characteristic for counter-terrorism is this: security is a pressure point, to one extent or another, for every terrorist organization. Theoretically, measures leveraged against that pressure point, if applied effectively, will force the terrorist organization to sacrifice operational

efficiency for organizational security. The theoretical implication of this characteristic for deception, in turn, is that deception measures leveraged against that pressure point, if applied effectively, will force terrorist decision-makers to take actions that will ultimately cause the terrorist organization to sacrifice operational efficiency for organizational security. Some terrorist organizations will ultimately prove much more resilient in this aspect than others, but every terrorist organization must nonetheless deal with the tradeoff.

2. Terrorist Intelligence Gathering

How do terrorists and other non-state actors gather information and process it into usable intelligence? This question, frequently overlooked by those who study and write about terrorists and terrorism, is of utmost importance to those who would deceive them. The information necessary to facilitate terrorist operations doesn't just come to terrorist decision-makers in the form of sudden revelations from above—the claims of some millennial or religious terrorists notwithstanding. Every terrorist organization gathers information. In some cases, the information is the result of the casual observations of sympathizers. In other cases, information is gleaned from the Internet and other media sources. Operatives may be tasked by the organization to gather specific information. Finally, information may come from not just one but a combination of sources. Like a state target of deception, the terrorist organization collates the information flowing in from a variety of sources. All of it is analyzed, even if only superficially and informally, and some or all of it is passed along. The gatekeepers who protect terrorist decision-makers, in turn, receive and filter the incoming information, allowing varying amounts of it to reach those decision-makers. Ultimately, the decision-makers do something with the information, whether choosing to act upon or ignore it.

The problem for every terrorist organization, then, is one of information gathering and processing. Some groups tend to do the former very well, only to falter at the latter. Some groups are just the opposite, on the other hand, making up for weaknesses in information gathering by excelling at analysis—making the

most of the limited information that they do receive. There is, however, a third group as well. This group tends to establish good processes and procedures for both gathering and analyzing information. If these groups can match operational capabilities to their intelligence capabilities, then they theoretically have the potential to be the most dangerous (Arquilla, personal communication, 29 November, 2001). Only by understanding a terrorist organization's processes, procedures, strengths, and weaknesses can a deceiver realistically hope to deceive a terrorist, inducing a desired response on the part of his target.

a. J. Bowyer Bell On Underground Intelligence

In The Dynamics of the Armed Struggle, J. Bowyer Bell suggests that terrorists gather information in two ways: passive observation on the one hand and active observation and surveillance on the other. All of the members of a clandestine organization, says Bell, "and often 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—and, of course, often without result" (1998, p. 196). From this passive observation net, Bell points out, the terrorist organization is able to gather very basic information on "targets and routines, habits and adjustments, vulnerabilities, secrets, and intentions" (p. 196). While the information that flows from many of these passive sources may be erratic and unrefined, it is nonetheless sufficient, if used correctly, to enable terrorist operations. According to Bell, "A little intelligence can go a long way—and does" (p. 206).

When passive information gathering proves insufficient, especially when more information is needed on a specific subject, underground leaders and decision-makers direct specific information-gathering efforts in the form of active observation and surveillance (Bell, 1998, p. 196). 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 rank-and-file terrorists and the authorities alike. 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 perform 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, however, 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).

One example that highlights the ability of terrorists to overcome the dangers Bell describes comes from the Troubles in Northern Ireland. In early 1979, British and loyalist forces in Belfast initiated Operation Hawk, a major surveillance operation employing highly sophisticated electronic equipment, covert operations, and thorough supporting intelligence analysis 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 GHQ operational officer. More significant that 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 position-fixing devices, all fabricated with components from the Ulster Polytechnic and Grundig and Strathearn Audio factories.[50] The Belfast IRA had even established surreptious wiretaps on the

[50] The IRA even used equipment acquired from Grundig and Strathearn Audio to develop their own electronics factory, manufacturing sophisticated electronic devices and state-of-the-art radio detonators for IRA bombs (Bell, 1998, p. 198).

British Telecom telephone network, including the private line of the general officer commanding the Dunmurry army garrison. Even more importantly, the IRA had been able to crack the codes being used for Operation Hawk; as a result, they were able to move their own people around to avoid observation and turn the tables on their observers (Bell, 1998, pp. 197-198).

Just as significant was the fact that the IRA had been keeping its own detailed files on the authorities, "just as a real intelligence operation would generate" (Bell, 1998, p. 198). The IRA files included minute detail on the houses, cars, and lifestyles of civil servants, security personnel, and judges. Moreover, IRA files contained numerous clandestine photographs and endless pages of transcripts of secret security force transmissions. The IRA case is important for two reasons. First, it suggests that some terrorist organizations are able to overcome shortcomings in capabilities and experience to develop sophisticated intelligence apparatuses. Second, it suggests that terrorists can mitigate the risk of exposure through discipline and sound security measures.

Underground organizations, according to Bell, seek to fulfill three basic categories of intelligence needs with passive and active means: strategic intelligence, tactical intelligence, and counterintelligence. Bell downplays the importance of the first: "Strategic intelligence is data accumulated to give substance to the rebel vision and has, once the killing has begun, almost no further role to play except as exhortation" (p. 192). Of much greater and enduring importance, he suggests, are tactical intelligence and counter-intelligence. In terms of tactical intelligence, Bell notes, "what is next needed [are] the most mundane operational details. Since most rebel operations are small, the tactical is often actually technical" (p. 192). The hijackers who carried out the 11 September attacks, for example, didn't require detailed strategic-level intelligence but rather simple tactical and technical information on airline in-flight procedures, flight times to cruising altitude, and the like.

The details emerging concerning the planning, preparation, and execution for the hijackings suggests that the perpetrators conducted very rigorous clandestine intelligence gathering, analysis, and sharing at a tactical level. For example, during the months of May through August 2001, the would-be hijackers traveled on a number of cross-country commercial flights to actively gather a wealth of information ranging from airport security procedures to flight crew practices. On virtually all of these reconnaissance flights, the hijackers traveled in the first class cabins. From the less crowded first class seats, the terrorists had a much better view of the cockpit and of airline procedures than they would have had in coach. After each series of cross-country flights, the terrorists gathered in a Las Vegas Econo Lodge, where investigators believe that they analyzed and shared the intelligence that had been gathered to that point (Zernike and Van Natta, 2001, p. A1).

Tactical intelligence is frequently only of secondary importance to terrorists, however. One of the greatest collective fears of every terrorist organization, according to Bell, is the fear of penetration or betrayal. As a result, the greatest intelligence efforts of most terrorist organizations tend to be devoted to counter-intelligence, "the search for conspiracy and spies, informers and heretics" (Bell, 1998, p. 194). The fear of penetration or betrayal is not merely focused on attempts by the state forces to penetrate the terrorist organization, however. Bell contends that terrorist organizations also have a closely related collective fear of internal divisiveness:

> Rebels yearn for a single road to salvation, a single crusade, control of the faith and the faithful by the elect. Sometimes there are internecine conflicts over the faith, the movement, the organization or the secret army—a shooting war to solve ideological problems. These problems may arise from all sorts of reasons, personality clashes, communications problems, agenda differences or real theological problems but are always seen once the shooting begins as a struggle not between variables but over the control of the truth (1998, pp. 203-204).

In short, an organization of rebels must always be conscious of a rebellion inside the rebellion. Bell's observations on terrorist counter-intelligence are significant for two reasons. First, they suggest that terrorist organizations are likely to have a motivated bias toward information regarding penetrations and betrayals, whether that information proves to be true or not. Second, they suggest that tactics designed to promote divisiveness in terrorist organizations may prove particularly useful. A deception that can convincingly portray any of the "reasons, personality clashes, communications problems, agenda differences or real theological problems" that Bell mentions, therefore, promotes internal dissension, potentially turning the terrorist organization in on itself (1998, pp. 203-204). Since many terrorist organizations are effectively "trust networks," deception can be used effectively to "sow dissension in the organization," further undermining operational efficiency (McCormick, personal communication, May 11, 2001).

b. A More Detailed View Of Insurgent Intelligence

In many ways, Bell's treatment of terrorist intelligence gathering, while generally informative on a macro- level of understanding, gives only a broad-brushstroke view of actual terrorist intelligence activities. Lincoln B. Krause, an intelligence officer with the Defense Intelligence Agency, notes that this phenomenon is all-too-common:

> Practitioners and theorists of insurgent warfare agree on the critical importance intelligence plays in the survival and success of insurgent movements. Yet, almost no *specific* writings on guerrilla intelligence exist. Especially lacking are works from those who imply the centrality of intelligence but almost never deal with its nuts and bolts: its requirements, sources, and organization. The lack of detailed literature on this type of intelligence stands in curious contrast to the critical role that it plays in guerrilla operations (1996, p. 291).

To remedy this shortcoming, Krause offers his own detailed analysis of insurgent intelligence activities. While there are conspicuous differences between terrorists such as bin Laden's al Qa'ida organization on the one hand, and insurgents such as Nicaragua's Sandanistas on the other, there

are numerous, sufficiently close parallels to find utility in Krause's description of insurgent intelligence. As a preface, Krause acknowledges that every insurgency is differentiated by local conditions, goals, strategy, and organization. Despite these differences, however, "most insurgencies do share common traits" (1996, p. 291). As a result, Krause has mapped out the "typical" intelligence needs, sources, and organizational requirements associated with each phase of insurgency (see Table 6).[51]

Krause's categorization is useful because it suggests the potential intelligence activities of terrorist organizations at various stages of group development. Well-established terrorist groups tend to fit passably (with some exceptions) into the guerrilla warfare category of Krause's framework. Usama bin Laden's al Qa'ida, for example, appears to be in the guerrilla warfare phase.[52] Although there is much ambiguous information on the organization, it is apparent that al Qa'ida has passed through the organizational phase and is relatively well developed. The organization is undertaking actions equivalent to guerrilla warfare against its enemies, but has yet to achieve its goal of open warfare between Islam and the West. There are indications that the network gathers basic operational information on its enemies, information on an ever-expanding area of operations, and basic tactical intelligence on a wide variety of potential targets using both passive and active means. Evidence further suggests that the various groups that comprise the al Qa'ida network task a wide variety of potential sources, from operatives living abroad to infiltrators or sympathizers in the militaries and intelligence agencies of Islamic governments, and from

---

[51] Krause suggests that insurgencies progress through at least three common phases—the organizational phase, the guerrilla warfare phase, and the conventional warfare phase. Not all insurgencies pass through all of the phases, nor do all insurgencies spend the same amount of time in each phase. Yet, the needs of insurgents are common in each of these phases.

[52] A terrorist or insurgent group, such as al Qa'ida, almost certainly doesn't think about what phase they may be in and what they should be doing as a result. Still, each group does think about what it needs to do based on its current situation and goals. There are, admittedly, problems with analyzing al Qa'ida according to a framework such as this; at the same time, however, there are benefits. The observer has to exercise judgment to understand what the framework can and cannot tell him.

sympathetic civilians to the Internet. Moreover, it is becoming apparent that the network has developed its own intelligence structures and standardized intelligence-gathering procedures.[53]

Krause offers two additional observations that hold potential for counter-terrorist operations, including deception. First, he notes, "The intelligence structure, once established, will be reorganized, grow, or shrink according to the needs and fortunes of the insurgency" (1996, p. 292). By this line of reasoning, states can expect the intelligence structures and activities of groups like al Qa'ida to shift in response to the state's counter-terrorism activities.[54] These shifts will likely be the most pronounced in response to overt activities, such as direct action. Covert measures such as deception will also lead to adaptive shifts, of course, but those shifts may not occur as quickly. Second, Krause suggests, "The new frontiers of information warfare and other technological considerations, and insurgent use of them, will bring both new insurgent intelligence requirements and new techniques to fill them" (p. 307). New terrorist intelligence requirements and techniques, in turn, imply new challenges and opportunities for counter-terrorism—such as new channels with which to deceive.

---

[53] A copy of the al Qa'ida manual describing intelligence gathering activities and procedures, captured during a raid by Manchester (England) Metropolitan Police during a search of an al Qa'ida member's house, is available on the US Department of Justice web site: http://www.usdoj.gov.

[54] One way of viewing these shifts, in keeping with the line of reasoning introduced in the previous section, is between two poles, with targeting at the one end and defense at the other. Terrorist organizations are rarely likely to forego one at the expense of the other, but defense needs may force targeting activities onto a back burner.

Phase	Intelligence Needs	Intelligence Sources	Organization
Organizational	♦ Immediate threats to nascent forces and fragile bases ♦ Info to further political expansion ♦ Strategic-level, politically-oriented intelligence on the state and opposition groups ♦ Information on specific targets	♦ Direct observation and reconnaissance ♦ Rudimentary human intelligence nets ♦ The local population, or popular information networks ♦ Open-source information	♦ Extremely rudimentary ♦ Specific organizations unlikely to exist
Guerrilla Warfare	♦ Basic military intelligence on the government and its forces ♦ Information on an ever-expanding area of interest ♦ Specific information on potential targets of military/terrorist action	♦ Insurgent forces ♦ Specialized reconnaissance units ♦ The populace—simple observation and near-passive collection by civilian supporters ♦ Infiltration and Espionage[55] ♦ Rudimentary SIGINT ♦ POW Interrogation and Defectors ♦ Open Sources ♦ Foreign Support—both state and non-state	♦ Specific intelligence structures are generally formed ♦ May include intelligence structures or elements stationed outside the country, to liaise with friendly governments and collect vital strategic-level intel
Conventional Warfare	♦ Gauge the will and political strength of both the government and its international supporters ♦ Information on other opposition and political groups ♦ General military intelligence requirements	♦ Increased emphasis on and expansion of strategic espionage and SIGINT ♦ Analysis	♦ Formal intel structures at increasingly lower levels ♦ Entire intel structure becomes more hierarchical and standardized

Figure 11. Insurgent Intelligence Needs, Sources, and Organization (Krause, 1996, pp. 292-307)

[55] As Krause notes, "One major position used to infiltrate is that of translator." This is a phenomenon of which I have personal experience. During a tour in Bosnia, one of the factions inserted an agent into our base-camp as a translator. Although the agent was eventually discovered and dismissed, a potential course of action might have been to use the agent as a deception channel to feed misleading information to the concerned faction.

The point of all of this is that terrorist organizations, like their state opponents, gather and process intelligence. Some organizations do so with a greater degree of finesse, but all terrorist organizations do so to one extent or another. Gaining an understanding of how they do so and to what degree of sophistication is a subject of critical importance for the deceiver. A basic framework along the lines of that offered by Krause offers a basic starting point for gaining that understanding. The key to all of this, of course, is intelligence preparation and feedback. If the deceiver's intelligence sources cannot identify how a particular terrorist organization gathers and processes information, then the probability of conducting successful deception is likely to be extremely low.

3. The Future of Terrorism—The Trend Toward Networks

The nature of international terrorism, it seems, is slowly but noticeably changing. In 1997, Edward Mickolus, the eminent chronologer of international terrorism, noted, "the first half of 1993…saw the advent of a new type of terrorist 'non-group.' Composed of small, loosely organized bands of like-minded coreligionists with world-wide contacts," Mickolus notes, "these noncentralized terrorist networks make combating terrorists all the more difficult. They in turn can count on the assistance of fundamentalist extremist colonies throughout the world" (1997, p. xii).[56] In April 2000, the US State Department report Patterns of Global Terrorism: 1999 also noted a major shift taking place in terrorism today. This shift is away from "well-organized, localized groups supported by state sponsors" and toward "loosely organized, international networks of terrorists." These sources and others observe that a wide variety of actors—from transnational terrorists to drug syndicates, and from NGO's to environmental movements—are modifying their organization and concepts of operations to capitalize on the inherent advantages of network designs.[57] Terrorists, it seems,

---

[56] Mickolus has published five exhaustive chronologies of international terrorism over the past two decades. These chronologies are an invaluable source for the serious student of terrorism. For a complete list of Mickolus chronologies, see the Bibliography.

[57] For a full treatment of the subject, see Arquilla and Ronfeldt's Networks and Netwars: The Future of Terror, Crime, and Militancy (2001). Much of the discussion here is derived from this

have grasped the enormous potential of networks and netwar concepts of operation.

John Arquilla and David Ronfeldt coined the term netwar to refer to an emerging mode of conflict short of traditional military warfare, in which the protagonists exploit network forms of organization and related doctrines, strategies, and technologies suitable for the information age.[58] According to Arquilla and Ronfeldt, "these protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command" (2001, p. 6). This form of conflict differs from the more traditional forms, according to Michele Zanini and Sean Edwards, in which the actors employ "conventional" hierarchical organizations and associated doctrines and strategies (2001, p. 30). In theory, netwar allows numerous, dispersed small groups using the latest in communications technologies to act conjointly across great distances. Non-state actors have proven that a netwar concept of operations can be used to great advantage, particularly against more traditional hierarchically organized actors such as states (Arquilla and Ronfeldt, 2001, p. 2). Recent examples of netwar include the Zapatista National Liberation Army's campaign against the Mexican government beginning in 1996, the first and second Chechnyan wars, and the Serb opposition campaign to Slobodan Milosevic in 2000.

a. Networks Explained

Networks are one of the most common forms of social organization, "simultaneously pervasive and intangible, ubiquitous and invisible, everywhere and nowhere" (Williams, 2001, p. 64). Like other organizational forms, networks may vary in size, shape, membership, and purpose. At the very simplest, a

---

book. A complementary perspective is found in Jay Galbraith's Designing Organizations (1995, pp. 11-17, 101-129).

network is a group of nodes connected in one way or another. Nodes, the basic building block of networks, may be individuals, groups or organizations, or even states, so long as they are interconnected in some way (p. 66). The nodes, according to Arquilla and Ronfeldt, "may be large or small, tightly or loosely coupled, and inclusive or exclusive in membership" (2001, p. 8). On the one hand, they may be segmentary—they may look alike and engage in similar activities (p. 8; Gerlach, 2001, pp. 290-293). On the other hand, they may be specialized—that is, "they may undertake a division of labor based on specialization" (Arquilla and Ronfeldt, 2001, p. 8). The boundaries of the individual nodes and the network alike may alternately be well defined or "blurred and porous in relation to the outside environment" (p. 8).

Large networks will generally have both a core and a periphery (Williams, 2001, pp. 72-74). The core of a network typically exhibits strong collective identity, characterized by "dense" connections among a relatively small group of individuals who provide "steering" for the network. The members comprising the core frequently include the network's creators, and they tend to initiate or approve major network activities, arbitrate disputes, and provide direction (p. 72). The relationship between core members is often underpinned by deep interpersonal bonds—such as family, kinship, ethnicity, or shared experiences—that facilitate trust and cohesion (p. 72). The cohesion and strong collective identity of the network's core, while typically a network strength, may also be a weakness. As Williams points out, "cohesion does not necessarily enhance—and can actually reduce—the [core's] capacity to obtain information and 'mobilize resources from the environment'" (p. 73).

Network peripheries, on the other hand, are the eyes, ears, hands, and feet of the network. In effect, the individuals and groups that are the peripheral nodes allow the network to undertake more geographically dispersed,

---

[58] Netwar is not simply cyber terror, as some have confused it to be. Cyber terror, however, is a tool of tremendous potential in the hands of terrorist networks (Zanini and Edwards, 2001, pp. 41-45; Arquilla and Ronfeldt, 2001, p. 331).

more extensive, and more diverse activities than might otherwise be possible in a more conventional organization (Williams, 2001, p. 73). The nodes also give the network a unique capacity to carry out intelligence collection activities (p. 73).[59] The periphery of a network is characterized by less dense patterns of interaction and looser relationships between nodes than the core. As a result, the periphery has a capacity for rapid reconfiguration. Nodes can be added as needed to meet opportunities or challenges more effectively, or severed to respond to external threats.

It is possible to identify three primary types of networks: the chain or line network; the hub, star, or wheel network; and the all-channel or full-matrix network (see Figure 12). The first, the chain network, consists of a line of separated nodes or contacts; communication must pass through all of the intermediate nodes to move from one end to the other. A hub network, in turn, consists of a set of actors tied to a central, although not necessarily hierarchical, node or actor. In the hub network, each of the respective nodes goes through the central node in order to communicate or coordinate with each other. Finally, an all-channel network is one in which each of the nodes is connected to all of the other nodes. This last type, according to Arquilla and Ronfeldt, is the archetypal netwar network (2001, pp. 7-9). One of the three types may prove more appropriate to certain conditions or purposes than the others. There may be hybrids of the three types, "with different tasks being organized around different types of networks" (p. 8). Conversely, there may be hybrids consisting of both networks and hierarchies, with a traditional hierarchy operating inside a particular node in a network, or there may be networks operating inside of networks (p. 8). The number of potential variations is virtually limitless.

---

[59] The late Colombian drug kingpin Pablo Escobar, for example, established a very effective star-type network of cab drivers and vendors in Medellin. Utilizing cellular phones, the network would provide Escobar early warning and real-time information on the activities of the Bloque de Busqueda, the Colombian National Police "Search Bloc," which was tasked with apprehending Escobar (Bowden, 2001).

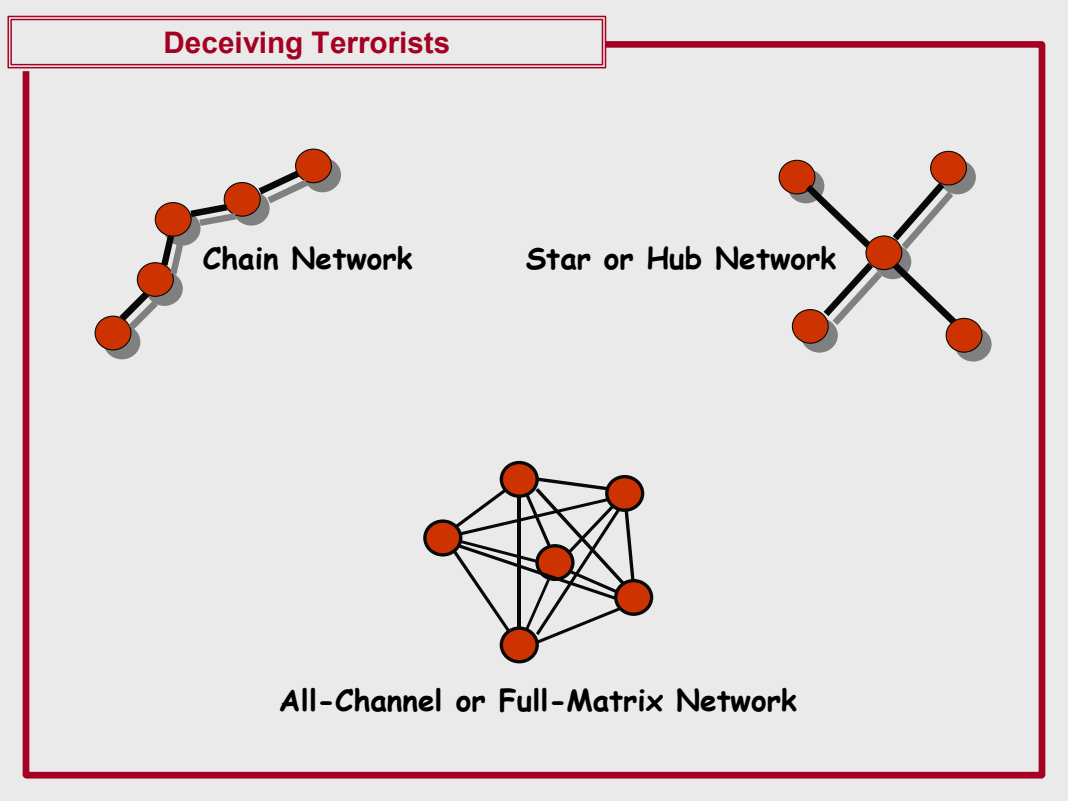


Figure 12. A Summary of Network Types (After Arquilla and Ronfeldt, 2001, p. 8).

The archetypal netwar network—the all-channel network—is the type, according to Arquilla and Ronfeldt, "that gives the network form its new, high potential for collaborative undertakings and that is gaining new strength from the information revolution" (2001, p. 9).[60] Visually, an all-channel network resembles a geodesic "Bucky ball" more than it does a pyramid:

[60] If the available open-source information is correct, Usama bin Laden's al Qa'ida is, in many ways, a good example of the all-channel network, bringing together a "complex network of relatively autonomous groups that are financed from private sources" (Zanini and Edwards, 2001, p. 34; Arquilla and Ronfeldt, 2001, pp. 363-365).

> Ideally, there is no single, central leadership, command, or headquarters—no precise heart or head that can be targeted. The network as a whole (but not necessarily each node) has little to no hierarchy; there may be multiple leaders. Decisionmaking and operations are decentralized, allowing for local initiative and autonomy. Thus, the designs may sometimes appear acephalous (headless), and at other times polycephalous (Hydra-headed) (2001, p. 9).

This all-channel network form has generally proven the most difficult to organize and sustain, primarily because of the "dense" communications that it requires to function optimally. This same type has, however, proven to generally possess the greatest potential, gaining tremendous new capabilities with the advent of the information revolution (Arquilla and Ronfeldt, 2001, p. 9). To realize its full potential, Arquilla and Ronfeldt point out, this type of network "requires a capacity for constant, dense information and communications flows," more so than for other forms of organizations (p. 10). This capacity may take the form of the latest information and communication technologies: cellular or satellite phones, fax machines, email, computer conferencing, or even Internet web site content. Alternately, however, the capacity may take the form of older technologies, such as human couriers, or of mixes of old and new technologies (pp. 10-11).

The use of technology is not the single measure of a network's potential, however. Arquilla and Ronfeldt (2001) suggest that a network's performance depends on what happens across five levels of analysis or practice:

- Organizational—what type of network design is being used; whether and how nodes may act autonomously; where leadership resides or is dispersed; and the mix (if any) of hierarchical dynamics and network dynamics (p. 325).
- Narrative—why the members have assumed and remained in a network form; what stories or narratives, if any, express a common

sense of identity, belonging, cause, purpose, and mission (p. 328).[61]

- Doctrinal—what doctrine exists for gaining the maximum utility from the network form; what doctrine exists to guide members in the case of outside pressures or attacks; what doctrine direct decision-making in the absence of specific guidance (p. 333).
- Technological—what is the pattern of and capacity for information and communications flows within the network; what technologies exist to support those flows; how well the existing technologies "fit" the network's design, doctrine, and story; the security and vulnerabilities of the existing technology (p. 339).
- Social—the nature of and reliance on strong, personal ties at the core, in the periphery, in between the core and periphery, and with the outside; the degree to which the network is or is not a "trust network" (p. 341).

As Arquilla and Ronfeldt point out, "Netwar actors that are strong at all five levels are, and will be, very strong indeed" (2001, p. 343). Organization, narrative, social underpinnings, and doctrine, are just as important as communications to the network's ultimate effectiveness—if not more so. Doctrine, in particular, lends a great degree of resiliency to the network, mitigating weaknesses in the other areas. The network's long-term capacity for optimal performance depends, in all likelihood, on the existence of a common set of principles, interests, goals, or even doctrine or ideology, which is shared by all the members of the network. "Such a set of principles, shaped through mutual consultation and consensus-building," Arquilla and Ronfeldt note, "can enable

[61] The right narrative can help keep people connected in a network whose loose peripheral structure otherwise makes it difficult to prevent defection. Furthermore, the right narrative can help bridge differences between disparate nodes, and can generate the perception that the movement has a winning momentum (Arquilla and Ronfeldt, 2001, pp. 328-329).

members to be 'all of one mind' even though they are dispersed and devoted to different tasks" (p. 9). This common doctrine may facilitate tactical decentralization, setting boundaries and providing "guidelines for decisions and actions so that the members do not have to resort to a hierarchy because 'they know what they have to do'" in the vast majority of situations (p. 9).

b. Network Strengths

The principles of the networked organization—relative flatness, decentralization of operations, delegation of decision-making authority, and loose lateral ties between physically dispersed nodes—lend a number of strengths. Perhaps the most significant is that networks are uniquely suited to benefit from communications and computing advances. Such advances tend to empower the underpinning relationships that make networks so potent an organizational form, according to Zanini and Edwards (2001, p 35). In particular, new communications and information technologies have the potential to aid networked organizations in three ways. First, they tend to greatly reduce transmission time and allow geographically dispersed actors to communicate effectively and coordinate their tasks for maximum effect (p. 35). Second, they tend to significantly reduce communications costs. With these lowered communication and coordination costs, networked organizations are able to further disaggregate through decentralization and autonomy (pp. 35-36). Finally, new technologies tend to substantially increase "the scope and complexity of the information that can be shared, through the integration of computing with communications" (p. 36). Even traditional hierarchical terrorist groups can benefit from advances in communications and computing technologies, of course, but the network benefits the most from these advances.

Another significant strength of networked terrorist organizations lies in their offensive and defensive capabilities. On the offense, Arquilla and Ronfeldt point out, "networks have the capacity to be adaptable, flexible, and versatile vis-à-vis opportunities and challenges," particularly where they can take

advantage of swarming strategies (2001, p. 12).[62] On the defense, "networks tend to be redundant and diverse, making them robust and resilient in the face of attack" (p. 13). Networked groups, particularly those that shun centralized command and control and display a capacity for interoperability, can prove extremely difficult to crack and defeat as a whole. Such groups can much more easily defy targeting of either leadership nodes or other typical Clausewitzian centers of gravity. In this manner, networks tend to be very good at self-protection (Arquilla and Ronfeldt, 2001, p. 13; Williams, 2001, p. 75).

A third strength of networked organizations is their ability to operate clandestinely (Williams, 2001, p. 71). This is critical to many terrorist organizations for whom visibility equates with vulnerability. What can be seen can be identified, and what can be identified can be targeted and killed. The individual nodes of a particular network may occasionally be visible, and thus vulnerable; the overall networks, on the other hand, frequently are not immediately, obviously, or fully visible. In fact, many illicit networks tend to operate under the observable horizon of their enemies, making gathering intelligence on networks a difficult task.

Yet another potential strength of networks is their capacity to transcend typical jurisdictional boundaries and distinctions. The individual nodes of a network may be spread over a number of states, countries, or even continents. As a result, transnational networks in particular have the potential to exploit differences in national laws and regulations, as well as the common distinctions between public and private, war and peace, and civilian and military. This makes it difficult for a government (or group of governments) to adequately implement a single, coherent strategy for dealing with networks (Williams, 2001, p. 71; Arquilla and Ronfeldt, 2001, p. 14,).

---

[62] "Swarming," according to Arquilla and Ronfeldt, "is seemingly amorphous, but it is a deliberately structured, coordinated, strategic way to strike from all directions" at a particular target (2000, p. vii). The overall aim of swarming, they suggest, is sustainable pulsing, wherein

Finally, networks display an ability to leverage relationships, particularly outside the network, to favor the network (Williams, 2001, p. 79). Relationships, particularly between members of the network and individuals outside the network, "can be understood as social capital that can be exploited" to benefit either individual nodes or the network as a whole (p. 78). Williams suggests that criminal and terrorist organizations extend their reach and capabilities by "coopting individuals and organizations in ways that facilitate, enhance, or protect their activities" (pp. 79-80). A well-connected terrorist network thus can theoretically call on the efforts of lawyers, accountants, bankers, financial professionals, businessmen, government officials, and a host of other players who—unlike the terrorist—operate in the licit realm.

c. Network Weaknesses

Although networks clearly enjoy a number of potential strengths, the form is not without its potential weaknesses as well. First, as already discussed in some detail, the archetypal netwar actor requires a dense communications capacity in order to function *optimally* (Arquilla and Ronfeldt, 2001, p. 10). Although cutting-edge communications and information technologies are increasingly resistant to compromise, all communications carry some risk of compromise for terrorist networks.[63] These new technologies, in virtually all cases, have their own weaknesses that the network must cope with. Cellular and satellite telephones, personal computing, email and Internet chat may increase a network's ability to communicate quickly and over great distances, but they also open the door to tracing, hacking, and computer attacks. In many cases, new risks have merely supplanted old risks. Networking and information technology have undoubtedly increased the efficiency of terrorist groups, but have not necessarily mitigated the tremendous risks described by Bell, McCormick and Owen (Zanini and Edwards, 2001, pp. 39-40).

---

network nodes assemble rapidly and stealthily, strike a target from all directions, then break off and disperse again, immediately ready to assemble again for a new pulse (2001, p. 12).

Second, many networks still rely on personal contact (Zanini and Edwards, 2001, p. 39). The need for these contacts, dictated by the nature of the network's social underpinnings, may limit a network's capacity to take maximum advantage of technological advantages. Visually, the need to balance organizational benefits with needs for personal contact and security can be viewed as a juggling act in which one characteristic is always on the rise, one is always on the fall, and one is always in transition (p. 40).

A related potential for weakness lies in the fact that networks, like all groups, have a certain potential for segmentation (Gerlach, 2001, p. 305). Like J. Bowyer Bell, Gerlach suggests that networks are as susceptible to schism as other forms of organization, and may divide over personal power, preexisting cleavages, competition among members, and ideological differences. While this can be a strength when the network faces external threats, it can be a weakness when perceived differences arise between members over ideology, tactics, and objectives.

A fourth weakness common to networks, according to Arquilla and Ronfeldt, is the potential for coordination problems (2001, p. 327). It is clear by this point that coordination is an essential element, if not a raison d'etre, of the network. Coordination is, however, a friction point for all organizational forms. This is particularly the case for organizations—such as the archetypal netwar network—that have and practice diffuse leadership.

Finally, one of the lesser-noted potential weaknesses of networks is that some degree of discipline is required to effectively implement the network form. A network will only function optimally if the nodes communicate and coordinate effectively with each other and/or operate according to the network's doctrine. The failures of a number of nodes to do so threatens not only network effectiveness, but also network survival.

---

[63] Many terrorist and criminal networks have, for example, made effective use of encryption and steganography for some time now, a trend that is likely to increase.

d. Implications For Counter-Terrorism Strategies

In the end, the rise of networked terrorist organizations brings a number of implications for those who would combat them. First, intelligence preparation and feedback are of critical importance in combating networks. Arquilla and Ronfeldt predict that in a war involving networks, the side with superior intelligence wins (Garreau, 2001, p. C01). A state's intelligence preparation should result in an accurate description of a network's dimensions, characteristics, and vulnerabilities on a framework approximating Arquilla and Ronfeldt's levels of network analysis. Specifically, counter-network intelligence should strive to answer the following questions:

- Organization. What kind of network design is being used? Are members allowed to act autonomously? Where does leadership and decision-making reside in the network? Are hierarchical dynamics mixed in with network dynamics and, if so, to what effect? In short, intelligence must be able to answer these questions to be "able to identify and portray the details of a network's structure" just as accurately as when charting a traditional adversary's leadership and organizational structure (Arquilla and Ronfeldt, 2001, p. 325).
- Narrative. Intelligence must also be able to identify a particular network's narrative, since "whose story wins" is often a critical determinant of which side wins overall in a conflict (p. 330). Furthermore, intelligence must be able to answer how the story is told, since conduit is often as important to the narrative as content.
- Doctrinal. What doctrines does the network use and espouse (p. 333)? How does the network's doctrine allow it to respond to external threats? Is the doctrine strongly shared by all members, or does it represent a potential source of schism for the network? Is the network's doctrine a potential source of either commonality or friction with other groups? These are often extremely difficult

questions for intelligence to answer accurately; in many cases, indications of the answers may come as much from action as from edict.

- Technological. What is the pattern of and capacity for information and communications flows within the network? What technologies exist to support those flows? How well do the existing technologies "fit" the network's design, doctrine, and story (p. 339)? What are the strong points and vulnerabilities of the employed technology? These are the critical technological questions that intelligence must be able to answer to effectively combat a network.
- Social. How well and in what ways do the networks members know each other and interact (p. 341)? Are there potential preexisting cleavages within the network? What are the key relationships between the core and the periphery, as well as between the network and the outside? What relationships, both internal and external, are the most fragile under duress? On a related note, how are relationships likely to be affected by threats to the network?

Few of these questions, if any, are easy to answer. Some may, in fact, prove virtually impossible to answer except with the advantage of hindsight. Yet, the answers clearly suggest vulnerabilities that may be targeted as part of a counter-terrorist campaign. Many of the answers, moreover, suggest vulnerabilities to deception. The answers to technological questions, for example, suggest channels that may be targeted either overtly or covertly to perpetrate deception. The answers to the organizational and social questions, in turn, may suggest particular deception tasks, such as targeting relationships between key individuals in order to induce certain responses that will disrupt the

network's effectiveness.[64] As another example, a terrorist network's story may be the focal point of a combined deception and disinformation campaign. The significance of intelligence does not end with intelligence preparation, however. Intelligence feedback is a critical component of counter-network operations, including deception. Given the potential resiliency of networks to attack, it is critical to be able to quickly and accurately measure the impact of such operations in order to exploit success and maintain pressure on the network (Williams, 2001, p. 92).

A second implication of the trend toward netwar lies in the forms of organization and concepts of operation required to effectively fight networks. Arquilla and Ronfeldt observe that hierarchies traditionally have a difficult time fighting networks (2001, p. 15). As a result, they suggest that it takes networks to fight networks, and that whoever masters the network form first and best will gain major advantages, including the strategic initiative (p. 15). Zanini and Edwards draw a similar conclusion, implying that it may be possible for more traditionally organized states and organizations to beat networked terrorists at their own game by learning to draw on the same principles of network forms (2001, p. 54).

The subject of homeland defense is fertile conceptual ground for considering Zanini and Edwards' suggestion. Currently, the new Office of Homeland Security faces the Herculean task of coordinating the activities of more than 120 governmental agencies. Figure 13 suggests the complexity of this task as currently organized, utilizing a traditional hierarchy. A networked organization for the conduct of homeland security, on the other hand, taking advantage of all the communications and computing technologies available to the US government, might prove to be more suited to the task. Figure 14 suggests such an organization, with the Office of Homeland Security serving as a hub of

[64] The Fawaz Yunis case, an example forthcoming in this chapter, displays the use of trust relationships to transmit deception and create opportunities for direct counter-terrorist action.

an all-channel network consisting of each of the major departments of the Executive Branch. Each department, in turn, could either serve as the hub of a network of its own subordinate agencies or continue to utilize its original hierarchical form. Furthermore, direct communication and coordination between agencies of different departments could be established or abolished as necessary to meet changing situations and challenges. This example should not be misconstrued as a critique of existing homeland security policy, but merely as an illustration of the potential utility of a network form of organization in dealing with complex, real-world problems.

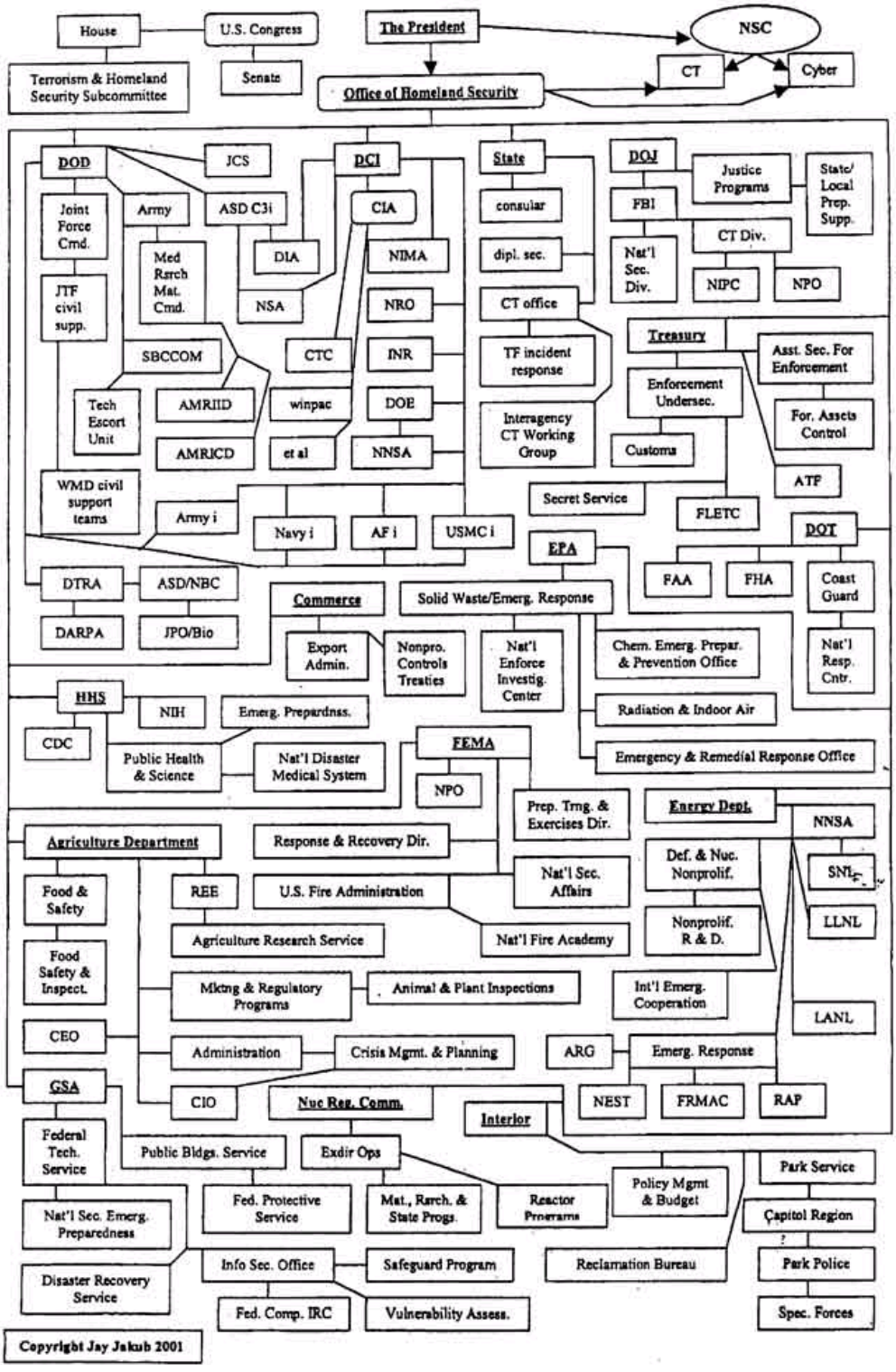


Figure 13. Current Homeland Security Organization. (From Jakub, 2001).

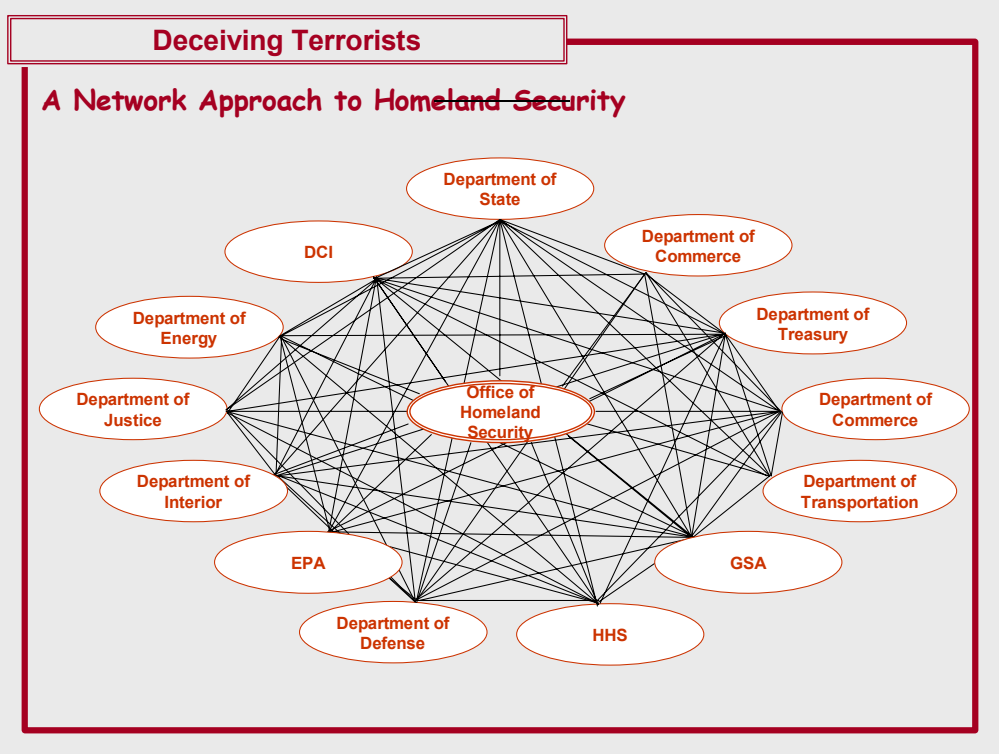


Figure 14. Network Approach To Homeland Security

The requirements for successfully attacking networks—particularly centralized control, detailed coordination, and intelligence—are the same requirements for successful deception (Williams, 2001, pp. 91-93). Thus, just as networks or network principles may be required to combat networks, a network form may be necessary to achieve centralized control and coordination of deception activities directed against terrorist networks. There is, however, a precedent to follow. During World War II, Winston Churchill established the London Controlling Section (LCS) to control and coordinate British strategic deception activities against Nazi Germany (Breuer, 1993, p. 60).[65] Although it had no real authority, the LCS coordinated the efforts of battlefield commanders, heads of states, and innumerable military, civil, and political agencies alike in a manner very similar to a star or hub network. In order to effectively deceive

[65] The LCS had a counterpart American agency in the Joint Security Control, organized under the Joint Chiefs of Staff and consisting of the directors of intelligence for the Army, Navy, and Air Corps (Breuer, 1993, pp. 60-61).

terrorist networks in the future, particularly terrorist networks with a global reach, it may prove beneficial or even necessary to create an LCS-type agency to centrally control and coordinate the activities of a wide variety of agencies and actors.

A third implication of the trend towards networks is that effectively combating networks requires establishing clear, attainable objectives (Williams, 2001, p. 91). Williams suggest that attacks on networks "need to be carefully orchestrated, finely calibrated, and implemented in a comprehensive and systematic fashion" (p. 91). Accordingly, whether the objective of counter-network operations is to destroy the network, degrade the network's capacity to carry out operations, plant misinformation, or to sever the network's external ties, objectives must be carefully calibrated with means and weighed against potential unintended consequences.

While the actual objectives of a counter-network operation will vary according to the network, Arquilla and Ronfeldt, Zanini and Edwards, Williams, and others suggest a number of potential objectives. One potential objective is a network's information flows, since a network's efficiency hinges on smooth communication and coordination (Zanini and Edwards, 2001, p. 53; Garreau, 2001, p. C01). Attacking the network's dense communications, whether by deception or direct action, may force the network to be more inefficient; on the other hand, it may also cause the network to innovate. Another potential objective are the network's external links (Leites and Wolf, 1970, pp. 39-41; Williams, 2001, p. 79). At the very least, cutting external links may starve the network for a time. A third potential objective, particularly for transnational networks, is the boundaries that those networks exploit for operation, movement, and survival (p. 94). Finally, the interpersonal relationships that provide the social basis for the network may be targeted. Although interpersonal relationships and strong social underpinnings may make actual penetration of a network difficult, these same relationships may be particularly susceptible to deception and other information operations (Arquilla and Ronfeldt, 2001, p. 341).

A final implication of the trend towards networks and netwar concerns the unintended consequences of counter-terrorist operations. Unsuccessful targeting of individual nodes may have adverse effects (Williams, 2001, p. 92). If one node is compromised or targeted, for example, it may simply be cut away and other nodes given increased responsibilities to compensate. If intelligence on the larger network is limited, the network may become more elusive once the known nodes are thus eliminated. Another potential unintended consequence is that smaller, more nimble networks may arise as successors to a defeated large network (Arquilla and Ronfeldt, 2001, p. 365).

C. DECEPTION TO CREATE AND EXPLOIT INEFFICIENCIES AND WEAKNESSES

The arguments in this chapter thus far imply that, as a general rule, terrorist organizations have a number of potential vulnerabilities to deception. Thus, one potential use of deception is to create inefficiencies and weaknesses in terrorist organizations. Furthermore, once these are created or identified, deception may also offer a means to exploit existing organizational inefficiencies and weaknesses. McCormick and Owen, Bell, and others have shown that clandestine organizations generally struggle to balance organizational efficiency with operational security. Increased operational efficiency—the ability to commit acts of terror—is purchased at the expense of organizational security. Increased organizational security, on the other hand, is purchased at the expense of operational efficiency (McCormick & Owen, 2000, p. 186; Bell, p, 27). By targeting a terrorist organization's confidence in its operational security, a deceiver should, for a time, be able to affect the terrorists' organizational efficiency. Furthermore, deception may be used to target the trust bonds upon which many terrorist organizations, particularly cellular and networked terrorist organizations, are founded (Bowlin, 1999, p. 89; Garreau, 2001, p. C01).

1. The Prison Sting

The "Prison Sting" is one illustration of deception to create inefficiency in a terrorist organization; although this case was discussed in significant detail in Chapter I, additional insight is offered here (see Figure 15).

a. Review Of The Case

In May 1974, IRA assassins gunned down Constables John Malcolm Ross and Edmund Bell on Finaghy Road in Andersonstown, part of Belfast. Five young men were charged in connection with the killing, but only two—Vincent Heatherington and Miles McGrogan—were ultimately remanded to Crumlin Road Prison. Upon remand, the pair indicated to the IRA officer "commanding" the Republican wing that they were Provisionals from the IRA's 1st Battalion and that they wished to join the Republican population. Even before the men settled into their cells, the IRA began routine, surreptious inquiries into each man's background. The inquiries revealed three key points. First, the reports indicated that Heatherington and McGrogan were not, in fact, regulars from the 1st Battalion, but had merely been members of Fianna Eireann, the youth section of the IRA. The reports also revealed that Heatherington and McGrogan had been tarred and feathered and ejected from the organization for petty larceny. Finally, the reports revealed that Heatherington and McGrogan were in no way responsible for or connected to the murders of the two Constables (Dillon, pp. 75-77).

As a result of the 1st Battalion's reports, the IRA "officer commanding" (OC) questioned the two further regarding their role in the constables' killings. Both indicated that they were innocent, but that they had been coerced into signing confessions. As Mark Dillon points out, "this allayed IRA fears that McGrogan and Heatherington were 'plants'" (1990, p. 77). The OC then quizzed the pair on why they had asked to be admitted to the Republican wing. The pair indicated that they feared for their lives if admitted to either the Loyalist or general population wings on charges of killing policemen. Furthermore, they indicated that their allegiance lay with the Provisional IRA.

The Provo OC accepted the answers, and attributed the pair's omission of their prior tarring and feathering to simple embarrassment. Although the IRA didn't know it yet, a firm foundation of credibility and confirming details was already being laid for the impending deception.

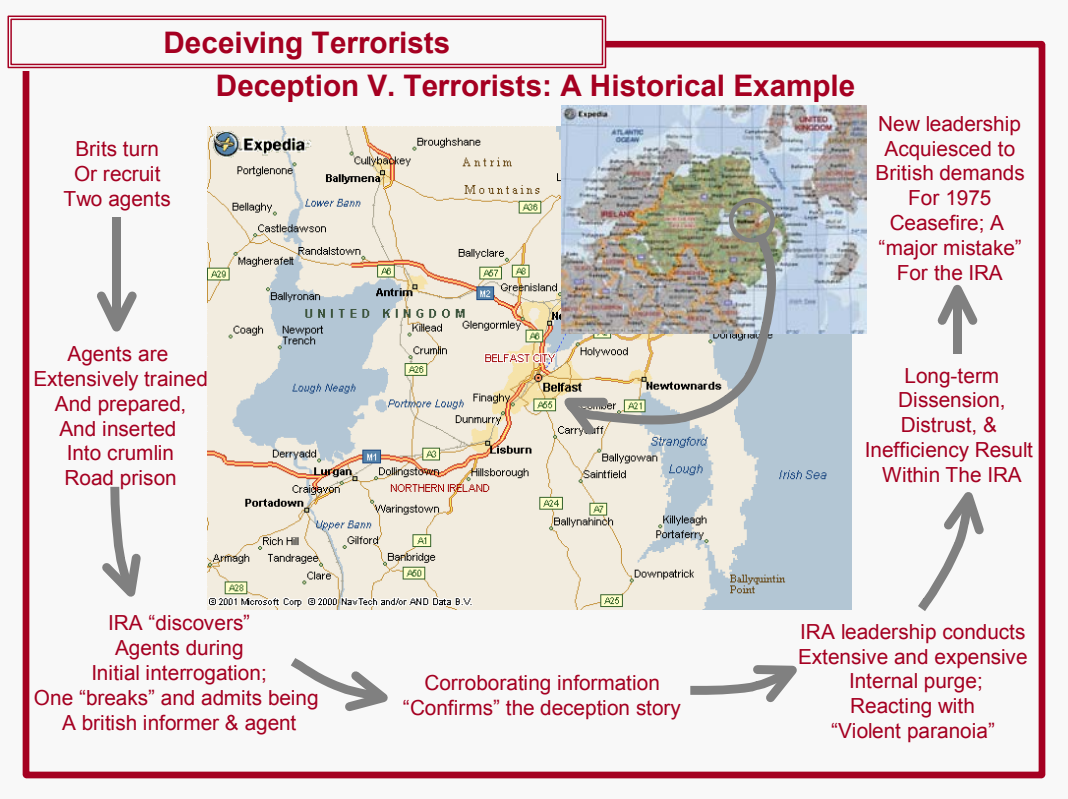


Figure 15. The Prison Sting Revisited

Despite having bought into the pair's stories, the IRA nonetheless continued their debriefings of Heatherington and McGrogan. Under interrogation McGrogan remained calm and collected, revealing nothing of value. Heatherington, on the other hand, became increasingly nervous, evasive, and agitated. As a result, the IRA interrogators began to focus their efforts on Heatherington. Before long, Heatherington "broke" and admitted that he had been a minor British informer, albeit unwillingly, for more than two years. Heatherington seemed relieved to have his secret in the open, and the IRA took his cooperation to indicate that the young man was simply the pawn of more clever and devious people. Heatherington eventually revealed his British

handler's names, and implicated McGrogan as a co-conspirator. As Dillon puts it, "Heatherington was now in full flow, providing a list of names of IRA men, some of whom were in Crumlin Road, others in the Maze [Long Kesh Prison] and several on the outside, whom he claimed were British agents (informers)" (1990, p. 79). Additionally, Heatherington began to reveal details of incidents that the IRA formerly believed were caused by Army forces or Loyalist groups, as well as details of his training and handling by the British.

"All of this," Dillon points out, "was exactly the kind of information that the IRA was eager to hear" (1990, p. 80). The interrogators kept Heatherington and McGrogan apart, and Heatherington's admissions were not revealed to McGrogan. McGrogan's interrogators indicated that he remained calm under interrogation. Then, a note was discovered in Heatherington's cell, ostensibly from McGrogan, warning the former "if he talked he was a dead man" (p. 81). To the IRA interrogators, the note only confirmed their strengthening perception that "in Heatherington they had the right man and McGrogan was confirming his own guilt" (p. 81).

The final confirming evidence appeared to come when the interrogators pressed Heatherington on the real reason for his insertion into Crumlin Road Prison. Under great stress, Heatherington told his interrogators that the charges against him had only been intended to get him into prison. After a time, he confessed, he was to be contacted by a member of the prison staff and supplied with a quantity of poison. He was, he said, to use this poison to kill three senior Provisional officers housed in the Prison. A search of Heatherington's cell was subsequently ordered and poison was, predictably, discovered. Since the plot directly threatened those responsible for assessing Heatherington's story, and since it fit an earlier attempt on an IRA official in Crumlin Road Prison, the IRA bought Heatherington's story hook, line, and sinker (Dillon, 1990, pp. 81-82).

The deception was a stunning success; according to one Provo leader, the IRA leadership was carried away in hysteria. The Provisional IRA responded in a violent, spasmodic rage. Men implicated by Heatherington, both inside and outside of Crumlin Road Prison, were brutally interrogated. An unknown number admitted to crimes that, IRA officials only discovered too late, they could not have committed. Their comrades subsequently executed these loyal men. The leaders of the IRA, both inside and outside Crumlin Road Prison, were deliberately misled. The IRA leadership ordered, and the organization undertook, specific actions that favored the British: specifically, a purge of the organization and the negotiation of a ceasefire that ultimately led to four years of bitter internal feuding and division (Dillon, 1990, p. 83; Bowlin, 1999, p. 91).

b. Assessment Of The Operation

The Prison Sting is a notable example for several reasons. First, it is an excellent showcase for the role of the deception success factors described in Chapter II. In retrospect, the secrecy, organization, & coordination of the "Prison Sting" were all impeccable.[66] The deception was planned at a high-level, and was extremely centralized. Subsequent inquiries on both sides of the affair showed that the Prison Sting had a firm foundation of intelligence preparation, and Heatherington was able to feed the IRA leadership there a mixture of truths, half-truths, and outright lies; all of his stories were either verifiable by the IRA or fit existing preconceptions of the IRA leadership. The channels by which the deception was executed were controlled with extreme efficiency. A relatively high level of secrecy was maintained, protected by plausibility and confirming details. The deception was plausible, and was confirmed repeatedly, particularly when the poison plot was discovered.

Second, the Prison Sting displays the potential in such operations for unintended consequences. Although the IRA was severely damaged by the

[66] As for secrecy, even to this day, the only accounts of the affair come from journalists and the IRA themselves; the British have yet to admit to the affair.

Prison Sting, the organization ultimately reorganized from its traditional battalion formations into a cellular structure, and ultimately proved harder to attack as a result. Having thus survived, the IRA emerged as a "smarter and more determined organization" (Bowlin, 1999, p. 91). It is not clear whether the original deception would have been as successful against the networked cellular organization subsequently adopted by the IRA. A second unintended consequence is that the Provisional IRA ultimately tried Heatherington and McGrogan in absentia and executed the pair. This kind of outcome, however, is always a possibility in such affairs. Mark Urban describes the paradigm of a "Big Boy's Game" played by "Big Boy's Rules": Those who play the game, he suggests, are aware of the potential consequences (Urban, 1992). As one "IRA man" puts it in Dillon's account, "When it comes to the sting, winning matters, not the survival of the double agent" (p. 35).

The final notable feature of the Prison Sting that must be considered is that the deceiver and the deceived shared a number of cultural and language similarities. It is unclear what role these similarities played in the ultimate preparation, execution, and outcome of the deception. Moreover, it is uncertain whether this particular deception would have been as successful against an adversary who didn't share the same general cultural characteristics[67].

2. Deception In The Philippines

Because insurgents—as one form of non-state actor—tend to have far more similarities to terrorists than they have differences, cases of state deception against insurgents have a certain appeal as illustrative examples. There are a number of cases of deception to create and exploit inefficiencies in insurgent groups to be found in the insurgency of the Communist Hukbo ng Bayan Laban Sa Hapon—"Huks," for short—in the Philippines after World War II.

---

[67] The concept of deceiving terrorists who are also one's fellow citizens also raises sticky issues regarding the constitutional and legal rights of those targeted. The British government has suffered immense damage to its reputation for some of their actions during "the troubles."

a. An American In The Philippines

From 1950 to 1954, Edward Geary Lansdale served as an advisor to the Filipino government of Ramon Magsaysay. An enigmatic figure, Lansdale played a key role in the Filipino government's campaign against the Huks. According to his friend and biographer, Cecil B. Currey:

> Lansdale devised tactics, implemented by Magsaysay, that ensured a truly popular election there for the first (and almost the last) time in history. He successfully advocated to Magsaysay policies that helped the government destroy the Huks as a threat to Filipino society. Upon his arrival there, Lansdale found the nation ill and tottering, drained by political leeches, bloodied by an internal insurgent conflict. He left it strong and whole, under the guidance of a magnificent leader (Lansdale, 1991, p. xi).

Lansdale's In the Midst of Wars is a thrilling account of his role in the counter-insurgencies in the Philippines and, later, in Vietnam. In a fascinating series of anecdotes, Lansdale gives a number of examples of the value of deception and other psychological warfare measures against insurgents.

One case Lansdale recounts concerns the deception of the Huk leadership on the eve of the 1951 national elections. The Philippine Military Intelligence Service (MIS) had discovered a Huk agitprop cell operating in the capital of Manila. Lansdale persuaded the MIS to delay arresting members of the clandestine group in favor of exploiting the group to deceive the Huk leadership and undermine their attempts to interfere with the elections. Lansdale crafted "a strongly worded, fake Huk directive asking all Huk adherents to 'Boycott the Election!'" (1991, p. 92). The directive was prepared on a captured Huk typewriter, using captured Huk stationery, and included the appropriate authenticating information. The finished product was inserted via the agitprop cell into the Huk propaganda channels. Within days, the Huk Politburo implemented Lansdale's "Boycott the Election!" slogan, adopting the arguments and slogans that Lansdale had incorporated into the fake directive. The results were disastrous for the Huks. On election day, more than 80% of Filipino

registered voters turned out to vote—a resounding victory for the proponents of democracy and a shattering defeat for the Communist Huk forces. According to Lansdale,

> The government forces, the press, and the citizen volunteers in NAMFREL publicly called to the attention of the Huks and their sympathizers how wrong had been their predictions about the elections…[68] If the Huk leaders could be so wrong this time, then in how many other things could they have been wrong all along? Why should anyone follow them anymore? The Huk rank and file started echoing these sentiments, and Huk morale skidded. Groups of Huks began to come into army camps, voluntarily surrendering and commenting bitterly that they had been misled by their leaders. Well, it was true enough. They had (1991, p. 93).

The Election deception is notable in two decidedly different ways. First, it suggests that deception can be useful to influence terrorist or insurgent to adopt courses of action ultimately harmful to their cause, without actually targeting the interpersonal dynamics of the group. This may prove useful in targeting groups with extremely strong social underpinnings, who otherwise prove difficult to penetrate. Second, it raises an enormous potential risk that is not otherwise discussed in the following chapter on risks and costs. The Filipinos did not have a strong history of unfettered democratic elections prior to 1951. The election deception, had it been exposed, would likely have been accepted as business as usual, particularly since Lansdale's role in the deception was plausibly deniable. For other, similar situations, however, it may prove too costly for the United States—or other nations viewed as champions of free, democratic elections—to be caught interfering in the conduct of another nation's elections.

b. The Filipino Perspective

Colonel Napoleon Valeriano's Counter-Guerrilla Operations: The Philippine Experience, covering the same period, recounts a number of other episodes similar or parallel to those offered by Lansdale. Both Valeriano and

[68] NAMFREL stands for the National Movement for Free Elections (Lansdale, 1991, p. 95).

Lansdale recount how the discovery of a Huk unit in the field was sometimes exploited by a simple "Eye of God" ruse.[69] A light liaison airplane assigned to the BCT would over-fly the Huk unit. The pilot or a passenger—sometimes Valeriano himself—would use a beach master's bullhorn to call out the names of key members of the Huk unit, telling them that they were surrounded (although they typically were not). The deception typically culminated with the observer thanking an anonymous informant within the Huk unit for the information that had allowed the government forces to locate the insurgents, and expressing the hope that the informant had not exposed himself unnecessarily. The Huks' deepest suspicions were invariably aroused, overcoming even the strongest social underpinnings, and Huk kangaroo courts singled out and executed an unknown number of insurgents (Lansdale, 1991, p. 74; Leites and Wolf, 1970, p. 143). According to both Lansdale and Valeriano, this tactic "frequently caused as many casualties to the enemy as a fire fight" (Valeriano, 1962, pp. 49-50). This account suggests that even simple ruses, carefully crafted and skillfully executed, can have a tremendous deceptive impact within a terrorist organization.

Valeriano also recounts the use of deception to cause a village mayor sympathetic to and clandestinely supportive of the Huks to flee his post. Although the government forces in the area had reason to suspect him of collaboration, the mayor had influential contacts in Manila that prevented his removal. After a chance firefight outside the mayor's village, Colonel Valeriano brought some of the Huk dead into the village. Leites and Wolf quote Valeriano's account of what happened next:

---

[69] The "Eye of God" ruse is a simple psychological warfare technique that Lansdale remembered from the siege of Caen in WW II. According to Lansdale, "In the siege of Caen, a German officer would be told by name [using a combat loudspeaker] that he was the next to die because he refused to surrender and moments later an artillery shell would hit his house or headquarters" (1991, p. 73). This is, of course, a technique almost as old as warfare itself, but Lansdale's account suggests the concept's value in operations against terrorists.

> When a large crowd had assembled and the mayor was about to inspect the bodies, Colonel Valeriano stepped up and loudly thanked him "for the information that led to the killing of these two men."…The mayor fled to Manila the next day (1970, p. 143).

In conclusion, Leites and Wolf suggest that deceptions such as this, which compromise members of an insurgent or terrorist group—or members of their support base—by falsely acknowledging their help, can be used to attack both the internal and external relationships upon which the group depends (1970, p. 143).

c. Assessment Of Filipino Deception Operations

In the end, two aspects of the Philippine deceptions require mention. First, the historical record of the counter-insurgency suggests that deception was sufficient in many instances to target strong trust relationships, even tribally based ones.

Second, in most of the cases of government deception in the Philippines, one deception success factor stands out. Lansdale notes that when he arrived in the Philippines, the Huks were the only force using deception or psychological operations to achieve their goals. At Lansdale's urging, however, the Filipino army adopted a concept of operations that made frequent and routine use of deception and PSYOPS. Filipino commanders such as Valeriano aggressively coupled adaptability with this new concept of operations—finding new and innovative ways to apply deception in a wide array of situations to gain an advantage.

3. The Abu Nidal Affair

The Prison Sting and Filipino examples of deception against terrorists and insurgents is compelling, but they indirectly raise another question: what of the use of deception in other cultures and regions, such as the Middle East? Are there any operations that exhibit the potential effectiveness of deception to create or exploit inefficiencies and weakness in Middle Eastern and Arab terrorist organizations, such as al Qa'ida? While there is, unfortunately, a dearth of open-

source examples to draw from, there is one well-documented case of an information campaign that caused a well-known Arab terrorist organization to turn inward on itself. In A Spy For All Seasons, Duane R. "Dewey" Clarridge recounts the results of an informational campaign against the Fatah Revolutionary Council, better known as the Abu Nidal Organization (ANO).[70]

a. The Abu Nidal Organization

At its zenith, the ANO was one of the two highest priorities of the CIA's Counter-Terrorism Center (CTC). The ANO declared itself an enemy of both the US and Israel, as well as of moderate Arab governments such as Jordan, Kuwait, and Egypt. The ANO's activities were largely international in nature, with Americans among the group's favorite targets; by 1986, the CTC estimated that the ANO had been responsible for killing more than 300 people and wounding more than 600.

The ANO was notable for a number of characteristics, including its methods and concepts of operation, its exceptional transnational capabilities, and its strong social cohesion. On the first point, the ANO was an organization that "employed highly sophisticated tradecraft, including rigorous compartmentation and secure electronic communications" (1997, p. 331). ANO operations were planned at a high level and with the utmost of secrecy; even those executing a mission were frequently kept in the dark. Operatives would be trained and sent abroad with no knowledge of their ultimate objective. Upon arrival in the target country, the operatives would link up with a support team, which would provide instructions, weapons, and explosives. Clarridge observes, "If something went wrong, individual terrorists knew nothing, and they could compromise or betray virtually no one else in the organization, even if they wanted to" (pp. 331-332).[71]

---

[70] Clarridge was founding director of the CIA's Counter-Terrorism Center (CTC).

[71] Not surprisingly, Usama bin Laden's al Qa'ida used much the same concept of operations to carry out the 11 September attacks. Although all of the hijackers had indicated a willingness to become martyrs, very few knew that they were going to die on 11 September.

Second, the ANO was truly a transnational enterprise. CIA intelligence-gathering activities and analysis revealed that the ANO had a network of "sleeper" operatives in the US, Mexico, and South America. Additionally, the ANO had an extensive network of commercial interests in Eastern Europe, Greece, Cyprus, Yugoslavia, and to a lesser extent in England, France, and Germany. The head of the ANO commercial enterprise was a Warsaw-based gray-market arms dealer named Samir Hasan Najm al-Din (p. 333). The commercial interests financed the organization's terrorist activities, provided critical cover and support apparatuses, and even gave cover to Eastern European intelligence services.

Finally, ANO recruiting and discipline depended on strong social underpinnings, coupled with an unhealthy dose of intimidation. "Brother would recruit brother and then become responsible for ensuring he didn't screw up" (Clarridge, 1997, p. 332). Betrayal of the organization was answered not only with the execution of the guilty member, but his sponsor and other members of his family as well. This last characteristic made the ANO extremely hard to penetrate (p. 332).

b. Bringing Down The ANO

Although the CIA was able to uncover a tremendous amount of information about the ANO by 1986, the US was relatively impotent when it came to doing anything with the information. Most of the key ANO members and leadership lived in southern Lebanon or Libya; this rendered their extraction impossible. Frustrated, but unwilling to concede, the CTC concluded that the "best way to attack Abu Nidal was to publicly expose his financial empire and his network of collaborators" (Clarridge, 1997, p. 334). The first attempt to do so consisted of State Department demarches to the various governments that either knowingly or unknowingly harbored his activities. This effort ultimately proved fruitless. In almost all the cases, the demarches were watered down to the point that they proved useless.

Frustrated by the failure of the demarches, the CTC pursued a different tack, persuading the State Department to issue a publication titled The Abu Nidal Handbook. According to Clarridge:

> The Abu Nidal Handbook laid out chapter and verse on the ANO, its members and accomplices, and its crimes. It even had an organizational chart. Starting with Sabri al-Banna (Abu Nidal's given name), it set forth in great detail much (but by no means all) of what [the CIA] knew about the organization, including the address of Najm al-Din's headquarters in Warsaw, his home address, the addresses of companies he did business with, and the litany of bombings, hijackings, grenade attacks, and assassinations for which they were responsible. Many ANO addresses were within countries friendly to the United States (1997, p. 335).

The publication of the handbook had an explosive and positive effect from the US perspective. Although many governments squirmed, virtually all—even the Poles and East Germans—divorced themselves from the ANO. For all intents and purposes, the ANO found itself virtually shut down (Clarridge, 1997, p. 335).

To exploit this victory, the CTC stepped up efforts to actively recruit operatives and agents within what remained of the ANO in various countries. Although most of the recruitment pitches failed, they nonetheless had a significant effect within the ANO. Clarridge explains:

> Seeing his financial empire under attack and listening to reports of CIA efforts to recruit his cadres, Abu Nidal was aware for the first time of a concerted offensive against him—we were coming after him and his people. He, like many in his line of work, was paranoid. The CTC fueled his hysteria over plots against him—feeding fear to a paranoid is something we know how to do.[72] Not surprisingly, Abu Nidal panicked. Those who reported having been approached by us were not rewarded for their loyalty, because Abu Nidal never quite believed that anyone in his group had turned us down. Their loyalty was suspect thereafter, and the punishment for disloyalty was torture and death (1997, p. 336).

By 1987, Abu Nidal redirected his external campaign of terror inward on his own organization. A simple allegation of disloyalty usually resulted in torture. Torture, in turn, resulted in a coerced confession. Confession ultimately resulted in summary execution. In southern Lebanon alone, more than 300 hard-core ANO operatives were murdered as part of Abu Nidal's bloody purge. Clarridge points out the brutal toll within the ANO's ranks:

> On a single night in November of 1987, approximately 170 were tied up and blindfolded, machine-gunned, and pushed into a trench prepared for the occasion. Another 160 or so were killed in Libya shortly thereafter. Distrust reached high into the politburo ruling the ANO. Even his closest surviving lieutenants began to believe that Abu Nidal was insane. Abu Nidal's paranoia, fed by our crusade against him, caused him to destroy his organization (1997, p. 336).

Predictably, the ANO collapsed. By 1988, the organization had been rendered virtually ineffective.

c. Assessment Of The Abu Nidal Affair

Although there is no evidence of deception in the Abu Nidal affair, the case nonetheless suggests that a skillfully applied information campaign may prove useful against terrorists whose strong social underpinnings and organizational form otherwise make them difficult to attack. In the case of the ANO affair, the majority of the information, including the underlying narrative,

---

[72] Whether deception or other measures were used to help fuel Abu Nidal's paranoia is not clear

happened to be true. Still, the case suggests that deception—another form of information campaign—has value as a counter-terrorist measure in the cultures of the Middle East.

4. Summary

In the end, there is compelling evidence to support the assertion that deception has value to create and exploit inefficiencies in terrorist and insurgent organizations. In particular, deception operations that suggest the presence of infiltrators, informers, or double agents within a terrorist organization have proven particularly effective. As Leites and Wolf point out, "Once a side becomes aware that infiltration has occurred, the false suspicion and unjust punishments that may be provoked may have a more deleterious effect that the infiltration itself: that is, the second-order impact of the infiltrators may be greater than the first-order impact (1970, p. 144).

Deception to create and exploit inefficiencies and weaknesses in a terrorist organization is not the only application of deception against terrorists, however. Just as deception has played a significant role in conventional tactics and strategy throughout history, so has deception played an important role in facilitating counter-terrorist operations and concealing states' capabilities and intentions toward terrorists. That is the subject of Chapter IV.

---

from the few open-source accounts. Nonetheless, the possibility certainly exists.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DECEIVING TERRORISTS—OPERATIONAL APPLICATIONS

On 13 October 1977, Lufthansa Flight 181, a Boeing 737 en route to Frankfurt, was hijacked less than an hour after takeoff from the resort island of Mallorca. At a refueling stop in Rome, the four terrorists—claiming to represent the Organization of Struggle Against World Imperialism—issued their list of demands. First, they demanded the release of eleven members of the Baader-Meinhof gang imprisoned in West Germany, as well as two Palestinian terrorists jailed in Turkey. Furthermore, the terrorists demanded a $15 million ransom, as well as a payment of DM 100,000 to each of the soon-to-be-released prisoners. Finally, the terrorists demanded that the prisoners be flown to Vietnam, Somalia, or the People's Democratic Republic of Yemen (PDRY) (Mickolus, 1980, pp. 734-735).

Having established their demands, the hijackers took off again, heading first to Larnaca, Cyprus. It was the beginning of a long and bizarre trip. On Cyprus, the hijackers refused the attempts of the local PLO representative to negotiate the release of the women and children on board and, fearing an Entebbe-style commando raid, took off almost immediately for Bahrain. Airports in Beirut, Damascus, Kuwait, and Iraq subsequently refused to allow the terrorists to land as well. Vietnam, Somalia, and the PDRY, all suggested by the hijackers as tentative destinations, indicated a similar reluctance to receive them. Bahrain and Dubai, the next points on the terrorist itinerary, likewise initially refused the aircraft permission to land, although Dubai ultimately assented (Mickolus, 1980, p. 735).

Frustrated by a plan gone awry, the hijackers were forced to let their first deadline slip by and set a new one. The hijackers attempted to increase pressure on the West Germans to acquiesce to their demands by their treatment of the hostages, "establishing an image of being quite willing to kill," and refusing all requests to release sick, young, or female passengers (Mickolus, 1980, p. 736). Before the West Germans could mount a hostage-rescue attempt in Dubai,

the hijackers once more extended their deadline and ordered the plane to take off, this time heading for Yemen. Yemeni officials, in turn, denied the hijackers permission to land in Aden, but the hijackers forced the pilot to land anyway on a rough dirt strip adjacent to the main runway at Aden's airport. At the hijacker's direction, the pilot left the airplane to examine the possible damage that the landing had inflicted on the landing gear. Upon his return to the aircraft, however, he was summarily executed in full view of passengers and crew for "trying to escape" (p. 736). Less than twelve hours later, the terrorists forced the copilot to fly the plane to Mogadishu. Once on the ground in Mogadishu, the terrorists dumped the pilot's body on the runway and doused the passengers and themselves with alcohol in preparation, they said, for burning. The terrorists then issued what they termed their "final ultimatum" (p. 737).

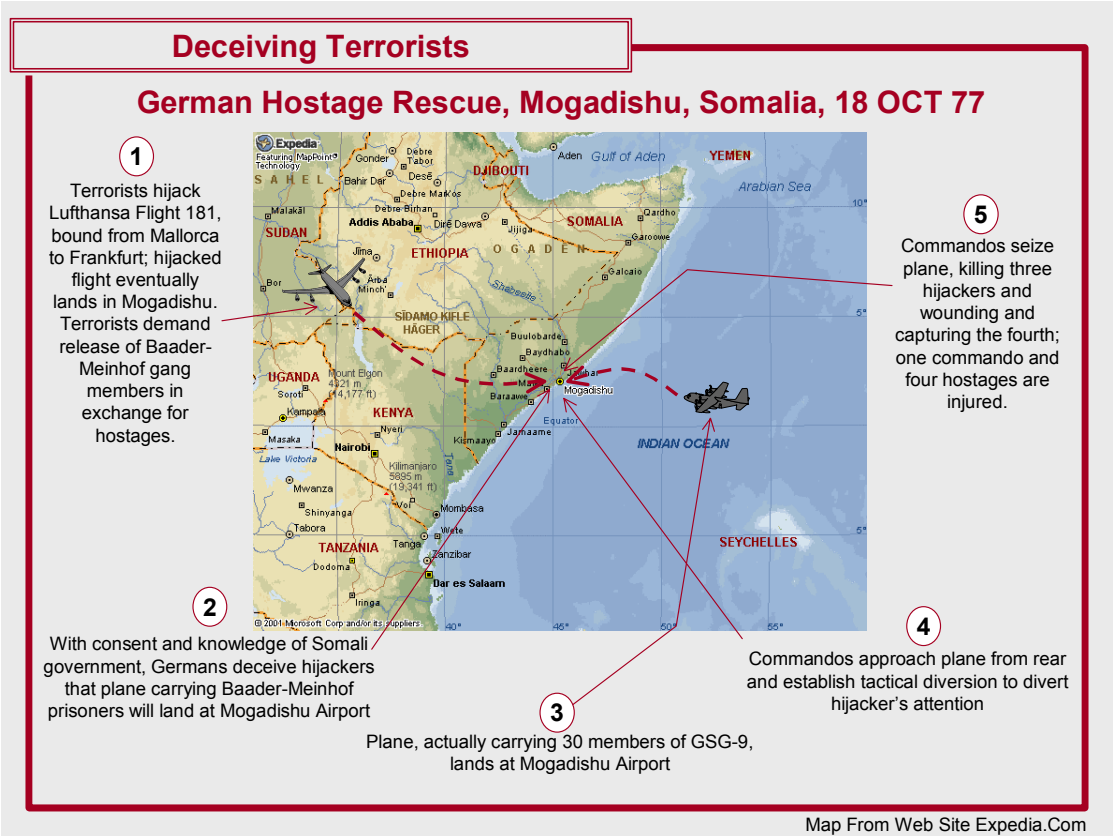


Figure 16. Hostage Rescue At Mogadishu

Early on in the hijacking, the West German government deployed the special anti-terrorist unit Grenzschutzgruppe Neun, better known as GSG-9, to be in position in the event that a decision was made to undertake a hostage-rescue operation. At the same time, though, German negotiators pursued a primary course of action focused on a peaceful resolution of the hijacking. The execution of the airliner's pilot, however, steeled the resolve of the West German government. The Germans decided to attempt a daring hostage rescue (see Figure 16). Once this agonizing decision was made, the Germans were faced with a new problem: how to overwhelm the terrorists and rescue the hostages before the hostages could be killed.

In order to gain the initiative, the Germans resorted to a series of deception measures (Mickolus, 1980, pp. 735-738). First, the Germans announced fairly early on, on 15 October, that GSG-9, which it acknowledged had been standing by for two days in Turkey, had been recalled to West Germany. Then, once the terrorists reached Mogadishu, the Germans informed the terrorists that their demands would be met—that their counterparts would, in fact, be released in exchange for the hostages. Noting the necessity for more time, the West German negotiator requested and was granted a new deadline. Next, with the complete cooperation of the Somali government, a plane landed at Mogadishu's airport carrying 30 GSG-9 commandos and 30 backup medical and communications personnel. The Germans deplaned dressed in "sports outfits," although by midnight they had reverted to black uniforms and face paint.

At 0200 on 18 October, the assault force moved on the hijacked plane. The commandos noiselessly approached the rear of the airliner, placing assault ladders silently beside the airliner's rear doors. Once in position, the Germans resorted to a simple yet effective ruse. According to Bruce Hoffman, "A burning oil drum was…rolled from the rear of the plane toward its nose and down the runway to attract the hijackers' attention" (1985, p. 57). As the hijackers hurried to the cockpit to get a better look at the diversion, the commandos opened the plane's doors simultaneously and rushed the cabin, quickly overpowering the

terrorists. Three of the terrorists were killed immediately; the fourth was wounded and captured. Only one of the assault force members was injured, and all of the hostages were released.[73] Less than six minutes after beginning the assault, all the passengers were safely off the plane, and an ordeal of more than 100 hours was satisfactorily resolved, in no small part due to the contributions of deception.

A. INTRODUCTION—A REVIEW OF SCOPE AND METHOD

Chapter I established that states have routinely used deception in interstate conflict, and suggested that deception also has a role to play in conflict between states and terrorists and other non-state actors. In particular, the chapter suggested that states might use deception to create and exploit inefficiencies and weaknesses in terrorist organizations; to facilitate counter-terrorist operations; and to conceal strategic, operational, and tactical intentions. Chapter II, in turn, established a necessary foundation for thinking about how deception works and what factors contribute to deception success. Chapter III returned to the argument that deception has considerable counter-terrorism potential, exploring the value of deception to create and exploit inefficiencies and weaknesses in terrorist organizations. Cases like the rescue at Mogadishu, however, suggest quite clearly that the potential value of deception versus terrorists is not limited to attempts to create and exploit inefficiencies in terrorist organizations. On a tactical level, there is evidence that deception is extremely useful to facilitate counter-terrorist operations. Moreover, there is ample evidence to suggest that deception is useful to conceal capabilities and intentions. We now address these latter potential uses of deception against terrorists.

This chapter follows the method established in Chapter III. In order to determine whether the potential value of deception to facilitate counter-terrorist operations and conceal capabilities and intentions, the concept or theory

[73] Four of the hostages were injured, but all survived the ordeal (Hoffman, 1985, p. 57).

underlying each use is briefly explored. Next, historical examples are offered to support those theories. Finally, each historical example is examined carefully in order to determine the lessons to be learned or conclusions to be drawn from the examples.

In many ways, this chapter is hindered by the same constraints mentioned at the outset of Chapter III, although they may be more acute. Most modern-counter-terrorist units are less than thirty years old. The United States' 1st Special Forces Operational Detachment—Delta, for example, was not founded until the late 1970's. West Germany's GSG-9 was only created after the terrorist attack at the 1972 Munich Olympics. These forces and their equals in other countries generally remain shrouded in secrecy; some states refuse to even acknowledge their existence. Operations conducted by these units, accordingly, typically remain shrouded in mystery, only occasionally exposed to the light of day.

B. A THEORY OF SPECIAL OPERATIONS

Understanding the role of deception in facilitating modern counter-terrorist operations requires some understanding of the nature of special operations themselves. Bill McRaven's theory of special operations, first proposed in a thesis at the Naval Postgraduate School and later published in the book Spec Ops, is a practical source from which to draw that necessary foundation.

McRaven's theory suggests "special operations forces are able to achieve relative superiority over the enemy if they prepare a simple plan, which is carefully concealed, repeatedly and realistically rehearsed, and executed with surprise, speed, and purpose" (1995, pp. 381-382). The theory places exceptional importance on the concept of relative superiority. According to McRaven, "Relative superiority is a condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well-defended enemy" (p. 4). Relative superiority, once achieved, gives a special operations force the initiative to exploit the enemy's defenses and achieve victory. Gaining

relative superiority doesn't guarantee success, but no special operation succeeds without it (p. 382).

Relative superiority has three basic properties. First, relative superiority is achieved at the decisive point—in terms of time—in an engagement.[74] Typically, this point is also "the point of greatest risk" for the force conducting the mission (McRaven, 1995, p. 5). Second, relative superiority, once gained, must be sustained in order to guarantee victory. The ability to sustain relative superiority depends on Clausewitz's moral factors—courage, intellect, boldness, and perseverance (p. 5). Finally, once lost, relative superiority is difficult to regain. Special operations forces, such as those who typically conduct direct-action counter-terrorist missions, rely on relative superiority rather than overwhelming numbers or firepower to maintain the initiative. Once a special operations force has lost the initiative, the likelihood of regaining relative superiority is increasingly small (p. 6). The key to a successful special operations mission, therefore, "is to gain relative superiority early in the engagement. The longer an engagement continues," McRaven suggests, "the more likely the outcome will be affected by the will of the enemy, chance, and uncertainty, the factors that comprise the frictions of war" (p. 6).

McRaven proposes six principles that allow a special operations force to achieve its objective: simplicity, security, repetition, speed, purpose, and surprise (1995, p. 8). "Gaining relative superiority," McRaven says, "requires proper integration of all six principles" (p. 8). Simplicity is the most crucial of the six, and relies on innovation, a limited number of objectives, and good intelligence preparation (pp. 11-14). Next, security prevents the enemy from gaining an advantage through early detection of the impending attack. Good security is a delicate balance: it "should be as tight as possible, without unduly impeding the preparation or execution of operations" (pp. 14-15). Repetition, in turn, is "the

---

[74] Informally, the decisive point is that point at which—if successful—"we" begin to win and the enemy begins to lose. In other words, it is that critical time, event, or action which signals a critical shift in the course of a battle.

link between the principle of simplicity in the planning phase and the principles of surprise and speed in the execution phase" (p. 10). Repetition is manifested in the training of the force, in detailed mission rehearsals, and in a well-understood doctrine or concept of operations. The fourth concept, speed, is simple. A special operations mission must be accomplished as quickly as possible in order to maintain relative superiority and reduce the force's window of vulnerability. "The enemy's will to resist is a given, and his ability to react a constant," McRaven points out (p. 19). "Consequently, over time the frictions of war work only against the special operations forces and not against the enemy. It is essential, therefore, to move as quickly as possible regardless of the enemy's reaction" (p. 19). Understanding and accomplishing the operation's overall objective regardless of obstacles or distracting opportunities that arise characterizes the fifth principle of special operations—purpose. Purpose is derived from two factors—a clearly defined mission statement and a sense of personal commitment on the part of the special operations forces (pp. 21-22). Surprise, the final principle, generally implies catching the enemy off guard, affording the special operations force the opportunity to seize relative superiority (p. 17). Special operations forces gain surprise, McRaven concludes, by taking advantage of the enemy's vulnerabilities, by precise operational timing, and by employing deception.

At first glance, deception might seem to be incongruent with the principles of special operations. After all, McRaven notes, "The correlation between simplicity, security, and repetition is clear: if a plan is complex it will require extraordinary security, and an overabundance of security hinders effective preparation" (1995, p. 9). Deception, especially on a large scale, is generally a complex undertaking (e.g., the need for centralized control and detailed coordination). The benefits of deception, however, outweigh the potential cost of complexity in the majority of cases, particularly since most special operations are also characterized by strong centralized control and detailed coordination. McRaven observes that "deception, when it works, either directs the enemy's

attention away from the attacking force [misleading], or delays his response long enough [by increasing ambiguity] for surprise to be gained at the critical moment," thus facilitating achieving relative superiority (p. 17). McRaven clearly favors ambiguity-increasing deception over misleading deception for support of special operations. Misleading deceptions, he suggests, are more inherently risky than confusing deceptions, and when the former fail, the result can be disastrous for the special operations force (p. 17).

C. DECEPTION TO FACILITATE COUNTER-TERRORIST OPERATIONS

Deception may facilitate counter-terrorist operations in two ways. First, deception may protect counter-terrorism units and missions by contributing to the achievement of relative superiority. Second, deception may be used by special operations and/or counter-terrorist units to create operational & tactical opportunities where none otherwise exist (Hoffman, 1985, p. 22).

1. Deception to Protect Counter-Terrorist Units and Missions

The modern special mission units that conduct direct action missions are generally valuable assets with extremely limited recuperability. The organizational capabilities and individual experience possessed by the members of a special mission unit, if lost, may take years to replace. By contributing to the achievement of relative superiority, deception gives counter-terrorist units a greater chance of operational success and the survivability that goes with it (Hoffman, 1985, p. 22).

a. The Israeli Raid at Entebbe

The case of the 1976 Israeli hostage-rescue at Entebbe illustrates the value of deception to achieve relative superiority, and thus to protect counter-terrorist units and missions. On Sunday, 27 June 1976, Air France Flight 139 had just taken off from Athens, its intermediate destination on a journey from Israel's Lod Airport to Paris, when terrorists hijacked it. The hijackers ordered the crew of the A300 airbus to fly first to Benghazi, Libya, and subsequently to Entebbe, Uganda. In Entebbe, the four original hijackers—two German

members of the Baader-Meinhof gang and two Palestinian members of the PFLP—were joined by three additional Palestinians.[75] The hijackers demanded the release of 53 prisoners: Arab, Israeli, and Japanese terrorists held in prisons in West Germany, France, Switzerland, Kenya, and Israel. If their demands were not met, they claimed they would begin executing passengers at 1400, Israeli time, on 1 July (McRaven, 1995, p. 334).[76]

Almost immediately, the Israeli Defense Force (IDF) began planning and preparing for a number of potential hostage-rescue scenarios. Ultimately, the plan called for a force of Israeli commandos, paratroopers, and Golani Infantry to fly directly to Entebbe in four C-130's and conduct a nighttime assault landing at Entebbe airport (see Figure 17). This concept, according to the commander of the C-130 squadron, "was based on the fact that no one would think we were crazy enough to fly there, so it would be a total surprise" (McRaven, 1995, p. 336). Once on the ground, the commandos—members of the Sayeret Matkal Counterterrorist Unit, typically referred to as the Unit—would storm the airport's old terminal, where the terrorists held the hostages. Subsequently, the paratroopers and Golani infantry would seize the airport's new terminal and control tower and serve as reinforcements and escorts for the hostages (pp. 336-338).

In order to gain relative superiority, the assault force planned to approach the old terminal in a Mercedes and two Land Rovers. The Mercedes was modified to resemble an official Ugandan vehicle, complete with Ugandan flags. This simple ruse, if successful, would allow the assault force to reach the terminal and begin their assault without alerting either the terrorists or Ugandan security forces (McRaven, 1995, pp. 339-340).

---

[75] McRaven suggests that there is reason to believe that three additional terrorists joined the group in Entebbe, raising the total to ten terrorists. At the time of the assault, however, only seven terrorists were present at the Entebbe airport (McRaven, 1995, p. 334).

[76] The deadline was eventually extended until Sunday, 4 July, as a result of the Israeli acceptance of the exchange proposal (McRaven 1995, p. 337).

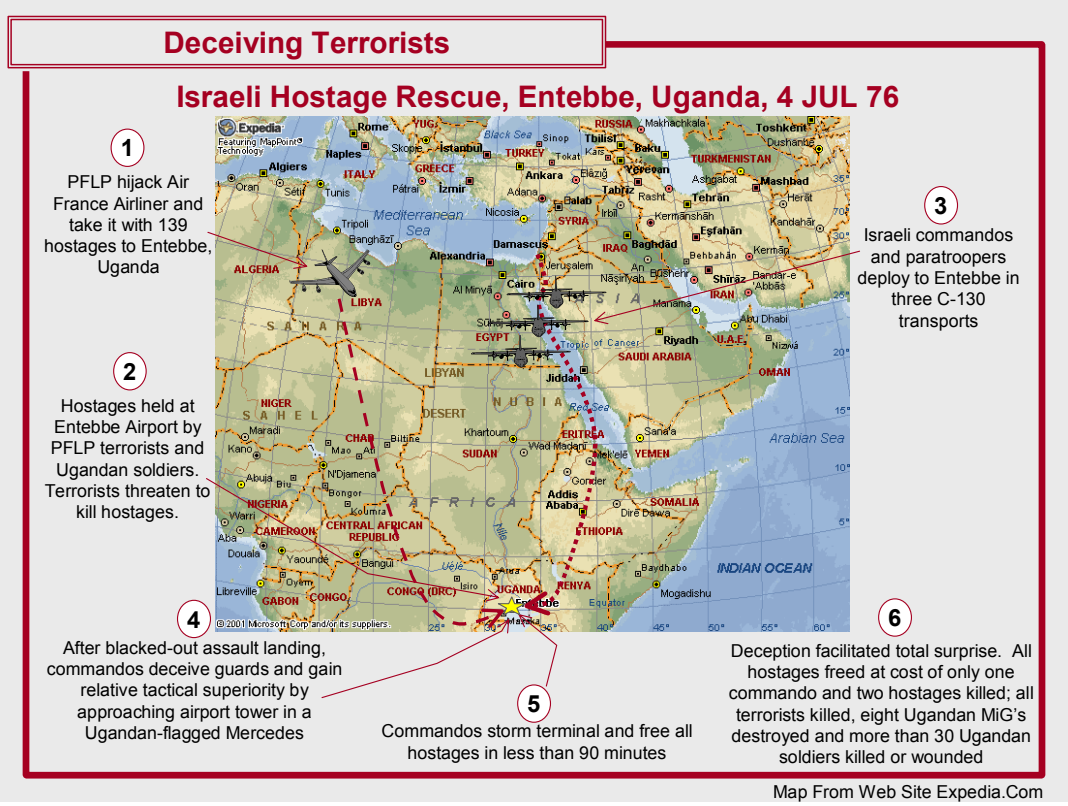


Figure 17. The Entebbe Raid

Following an intense series of briefings and rehearsals, the entire assault force departed from a staging base at Sharm-a-Sheikh in the Sinai on the afternoon of 3 July, less than 24 hours before the terrorist's extended deadline. Seven and a half hours later, the lead C-130 touched down on the runway at Entebbe. As the plane taxied, soldiers jumped from the slow-moving aircraft and began to place runway lights to guide the trailing aircraft. On order, the aircraft's ramp was lowered and the Mercedes and the two Land Rovers exited and began moving toward the old terminal (McRaven, 1995, pp. 356-358).

On the ground, tactical deception measures proved as critical to mission accomplishment as planners had anticipated. First, the vehicle ruse permitted the assault force to close to within extremely short range of the Ugandan sentries, allowing the commandos to engage the sentries before they could be engaged. Second, the deception initially misled the terrorists to believe

that their Ugandan hosts had revoked their hospitality and attacked the terrorists.[77] This second order effect of the deception was unintended, but fortuitous nonetheless. Before the terrorists could correctly ascertain what was going on and begin killing the hostages, the commandos had entered the terminal and begun clearing the building. The terrorists and their Ugandan counterparts never regained the initiative (McRaven, 1995, pp. 358-360). In the end, McRaven concludes, deception was a key success factor in achieving success at Entebbe: "surprise was not absolute, but, coupled with deception, it was sufficient to confuse the Ugandans and terrorists long enough to allow the commandos to penetrate the old terminal and rescue the hostages" (p. 375).

b. Other Israeli Special Operations

The Israeli raid at Entebbe is neither the first nor the last case of Israeli use of tactical deception to facilitate counter-terrorist operations (see Figure 18). Four years earlier, on 8 May 1972, "eighteen commandos disguised as mechanics, Red Cross officials, and released Palestinian prisoners" stormed a hijacked Sabena aircraft being held by four Black September terrorists at the Lod Airport (Hoffman, 1985, p. 37).[78] In a raid that lasted less than 90 seconds, the commandos killed two of the hijackers, wounded another, and captured the fourth unharmed. Moreover, they freed all 97 hostages on board the aircraft without a single commando or hostage being killed (p. 37).[79]

Although this case demonstrates the value of deception to protect counter-terrorism units and missions, it also raises the issue of the legality of certain ruses. Special operations forces, like their conventional counterparts, are subject to the laws governing land warfare. While deception is an accepted and

---

[77] One of the terrorists who was outside the old terminal at the outset of the attack purportedly ran back into the terminal shouting, "The Ugandans have gone nuts—They're shooting at us!" (McRaven, 1995, p. 359).

[78] The proven ability of the Unit to "resolve" hijackings culminating at Lod Airport likely figured in the 1976 hijackers decision to fly to Uganda rather than return to Israel to negotiate their demands.

[79] Three members of the assault team and five passengers were injured, a remarkably low number given the nature of close-quarters combat in a cramped airliner (Hoffman, 1985, p. 37).

legally permissible component of warfare, perfidy—the betrayal of trust—is not. Specifically, Articles 37 and 38 of Protocol I of the Geneva Conventions prohibit "the feigning of protected status" and the "improper use of the distinctive emblems of the red cross, red crescent or red lion and sun" to mislead potential adversaries (Protocol I, Art. 37-38, 1977).[80] Israeli commandos disguised as mechanics or even Palestinians "fit" under the laws of land warfare; commandos disguised as Red Cross officials, on the other hand, violate those same laws.

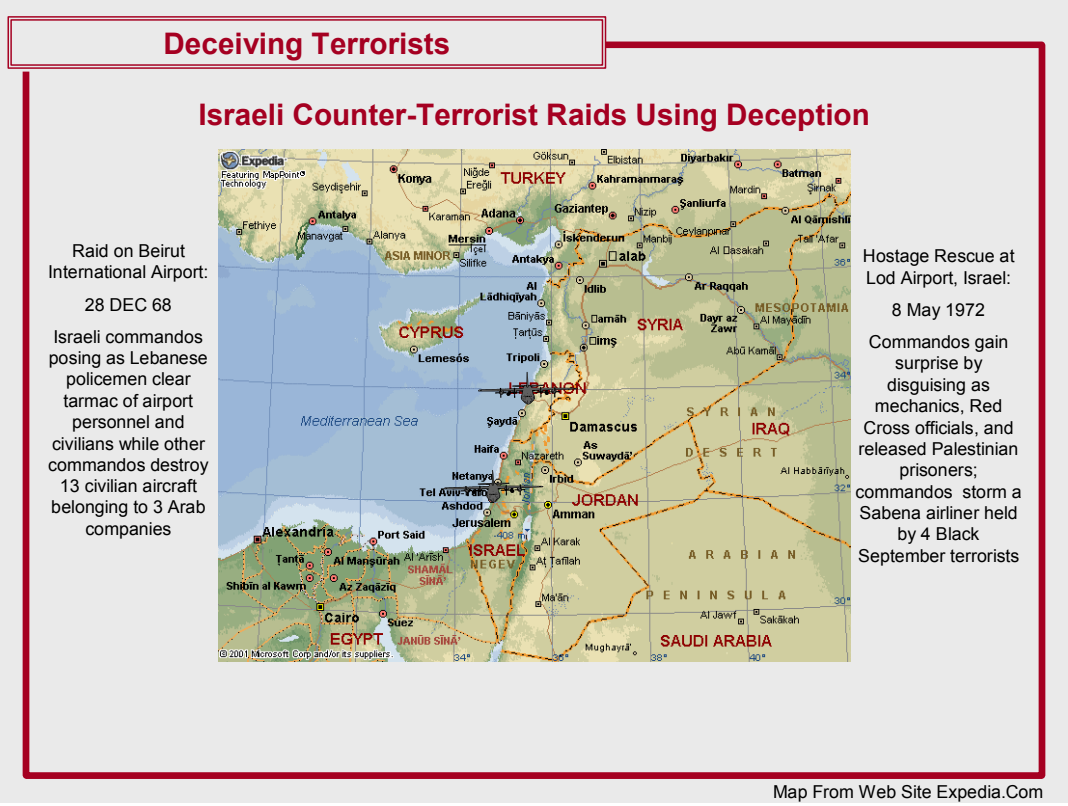


Figure 18. Israeli Use Of Deception In Direct Action Counter-Terrorist Operations

In another case, on 28 December 1968, Israeli commandos conducted a daring cross-border raid to Beirut Airport in retaliation for the hijacking of an Israeli airliner two days earlier. Commandos posing as Lebanese

[80] For a complete text of the Geneva Conventions and subsequent Protocols, as well as an excellent commentary, refer to the Society of Professional Journalists Web Site: http://www.the-spa.com/genevaconventions/Protocol1.html.

policemen cleared the tarmac of airport personnel and civilians while other commandos placed explosive charges on parked aircraft. In only 45 minutes, the commandos destroyed 13 civilian aircraft belong to three Arab countries, causing more than $40 million in damages (Hoffman, 1985, p. 34). While this last case does not involve terrorists, the case is nonetheless valuable for its illustration of the use of deception to carry out a successful special operation. The greatest threat to the Israeli commandos and the success of the mission consisted of the airport personnel and civilians—non-state actors with the capacity to interfere. Rather than liquidating these non-state actors, the Israelis used simple deception to mitigate the risk that they posed.

c. Rhodesian Use Of Tactical Deception

In Commando Raids, Bruce Hoffman of RAND analyzes 100 commando raids conducted between the end of WW II and 1983. As part of his study, Hoffman includes 15 counter-terrorist and counter-guerrilla raids conducted by the Rhodesian Army between 1974 and 1979; six of the fifteen accounts are notable for the mention of the role deception played in achieving success. One example took place on 13 May 1976. In Operation Detachment, twenty Selous Scouts, disguised in FRELIMO uniforms and driving vehicles modified to resemble Mozambican Army transports, conducted a raid on a ZANLA compound more than 180 kilometers inside Mozambique.[8182] The simple deception allowed the raiders to penetrate safely, conduct the assigned mission, and withdraw without incident (Hoffman, 1985, p. 50).

In another instance, the Rhodesians undertook Operation Long John, an attack against a ZANLA base 80 kilometers inside Mozambique on 25

---

[81] The Selous Scouts are discussed in greater detail later in this chapter.

[82] FRELIMO is the Frente da Liberataco de Mocambique, the Marxist guerrilla organization that fought against the colony's Portuguese rulers until Mozambique achieved independence in 1974. After 1974, FRELIMO "normalized" and became the Mozambican Army (Hoffman, 1985, p. 30). ZANLA is the Zimbabwe African National Liberation Army, the military wing of the Zimbabwe African National Union (ZANU), led by Robert Mugabe (p. 49). ZIPRA, in turn, stands for the Zimbabwe People's Revolutionary Army, the military wing of the Zimbabwe African People's Union (ZAPU) (Hoffman, 1985, p. 48).

June 1976. As in Operation Detachment, a force of Selous Scouts used trucks and scout cars disguised as FRELIMO military vehicles not only to penetrate Mozambique, but also to convince sentries to allow the force into a terrorist base at Mapai. Once inside, the Scouts killed or wounded nearly fifty terrorists, confiscated the camp's armory, and destroyed thirteen Mercedes buses used by the terrorists for transport to staging bases on the Rhodesian border (Hoffman, 1985, pp. 50-51).

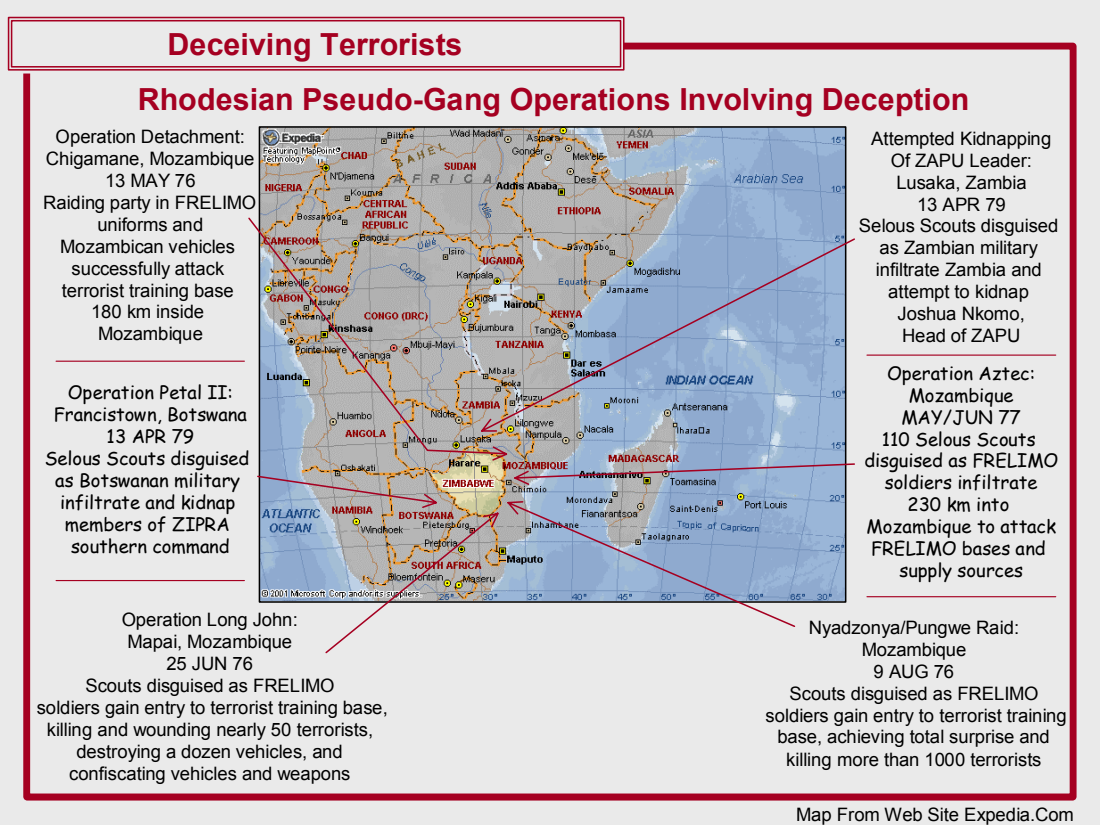


Figure 19. Rhodesian Tactical Use of Deception

On 9 August 1976, the Scouts conducted their largest cross-border operation to date. A Scout column of 10 trucks and four armored cars, again painted to resemble FRELIMO vehicles, penetrated more than 100 kilometers into Mozambique. At Nyadzonya, the Scouts—dressed in FRELIMO uniforms—gained easy access to a terrorist training camp. Much to their own amazement, the Scouts were able to drive right in and line up on the edge of the camp's

parade ground, where a force estimated at more than 1000 terrorists was assembled for morning formations. At the sight of the vehicles, the terrorists, believing them to be a new shipment of military vehicles and weapons, broke ranks and rushed toward the Scouts. The Scouts opened fire just before the mob reached the trucks, killing nearly a thousand and capturing 14 key ZANLA leaders. Not a single Scout was killed, and only five received minor injuries (Hoffman, 1985, p. 51; Thompson, 1988). As in previous operations, the Scouts overcame overwhelming odds and maintained relative superiority throughout the mission as a result of a very simple ruse.

In May and June 1977, a force of 110 Scouts conducted Operation Aztec, an extended series of raids on ZANLA bases deep inside Mozambique. Disguised as FRELIMO soldiers and using disguised vehicles, the Scouts raided terrorist camps at Jorge do Limpopo, Mapai (site of a previous successful operation), and Madulo Pan. Tactical deception, coupled with a high level of proficiency and tradecraft, enabled the Scouts to destroy a key railway line that served as the chief supply source for the terrorist bases, seriously interdicting ZANLA operations.

Rhodesian use of tactical deception in support of counter-terrorist and counter-guerrilla operations was not restricted to missions against the ZIPRA and ZANLA in Mozambique. On 13 April 1979, the Scouts resorted to very basic deception to facilitate the attempted kidnapping of a key terrorist leader, ZAPU head Joshua Nkomo, from his home in Lusaka, Zambia. In this mission, an unknown number of Scouts disguised as Zambian soldiers and traveling in Land Rovers disguised as Zambian Army vehicles crossed the border without incident. The raiders were able to drive directly to Nkomo's residence at ZAPU's well-guarded headquarters and initiate their raid. In a lightning operation, the Scouts killed 10 ZAPU soldiers, wounded 12, and destroyed two of the buildings on the compound. Despite quickly gaining and maintaining relative superiority, however, the mission was ultimately a failure, albeit not as a result of the deception. Intelligence failed to indicate that Nkomo was not in Lusaka at the

time of the attack. The Scouts were forced to withdraw from Zambia without their target (Hoffman, 1985, p. 53).

At nearly the same time, in what turned out to be one of the last Selous Scout missions, deception again played a significant role. A captured ZIPRA intelligence operative revealed that the entire ZIPRA southern command operated out of a single house in Francistown, Botswana. On 13 April, a Scout column of two armored cars and some light trucks were able to drive across the border deep into Botswana. Dressed in Botswanan military uniforms, the Scouts were able to seize all of the occupants of the house in question and spirit them back across the border into Rhodesia before ZIPRA forces knew what had happened (Hoffman, 1985, pp. 54-55).

d. Assessment

The German, Israeli and Rhodesian examples mentioned thus far all share one common characteristic: the creative use of deception to facilitate counter-terrorist direct-action missions, particularly at the tactical level. Furthermore, the Rhodesian examples suggest that, despite the differences between special and conventional operations, one fact remains constant. Creative and skillful use of deception has immense value on the field of conflict.

2. Deception To Create Counter-Terrorist Opportunities

Deception to protect counter-terrorist operations and achieve relative superiority is only effective when the conditions for counter-terrorism missions already exist. Deception can also contribute to counter-terrorist efforts by creating opportunities where none exist.

a. The Fawaz Yunis Case

The Fawaz Yunis affair is one case that illustrates the value of deception to create opportunities for other counter-terrorism operations. In 1985, Fawaz Yunis—a Lebanese Shiite used-car salesman from Beirut—gained notoriety as an international terrorist. On June 11 of that year, Yunis and several compatriots hijacked a Royal Jordanian Airlines plane from Beirut. Refused

permission to land in Tunis, the terrorists blew the plane up on the tarmac in Beirut at the end of a two-day ordeal. Two days later, Yunis emerged into the spotlight again, this time as a co-conspirator in the hijacking of TWA Flight 847. Along with Imad Mugniyeh, head of the Islamic Jihad, Yunis was one of the reinforcements who boarded the TWA plane in Beirut after the murder of American hostage Robert Stethem (Clarridge, 1997, pp. 349-350). Although Yunis' crimes were committed on Lebanese soil, the fact that Americans were on board each aircraft allowed the FBI to pursue Yunis under the provisions of the Omnibus Crime Act. The FBI was hindered, however, by two constraints. First, the FBI could only apprehend Yunis in international waters or airspace. Second, for legal considerations, no CIA agents could be physically present at the time of his apprehension.

The operation to apprehend Fawaz Yunis was eventually code-named Goldenrod. The plan, according to Dewey Clarridge, then head of the CIA's CTC and the man overall responsible for the deception, called for the CIA to "dangle the bait, set the trap, and be sure that the target was delivered into the FBI's hands in international waters" (1997, p. 351). The CIA recruited a long-time Yunis acquaintance named Jamal Hamdan to lure the terrorist to Cyprus, ostensibly to negotiate a major drug deal. According to Clarridge, "Hamdan had been friendly with Fawaz Yunis since 1981 and had even served as a sort of mentor to him in the shadowy world of Middle Eastern black-market commerce" (p. 350). Hamdan convinced Yunis to come to Larnaca, Cyprus, where he had supposedly arranged a meeting with an international drug kingpin named "Joseph" aboard a yacht in the Mediterranean (p. 352). If all went as Hamdan suggested it would, both men stood to profit immensely from the meeting.

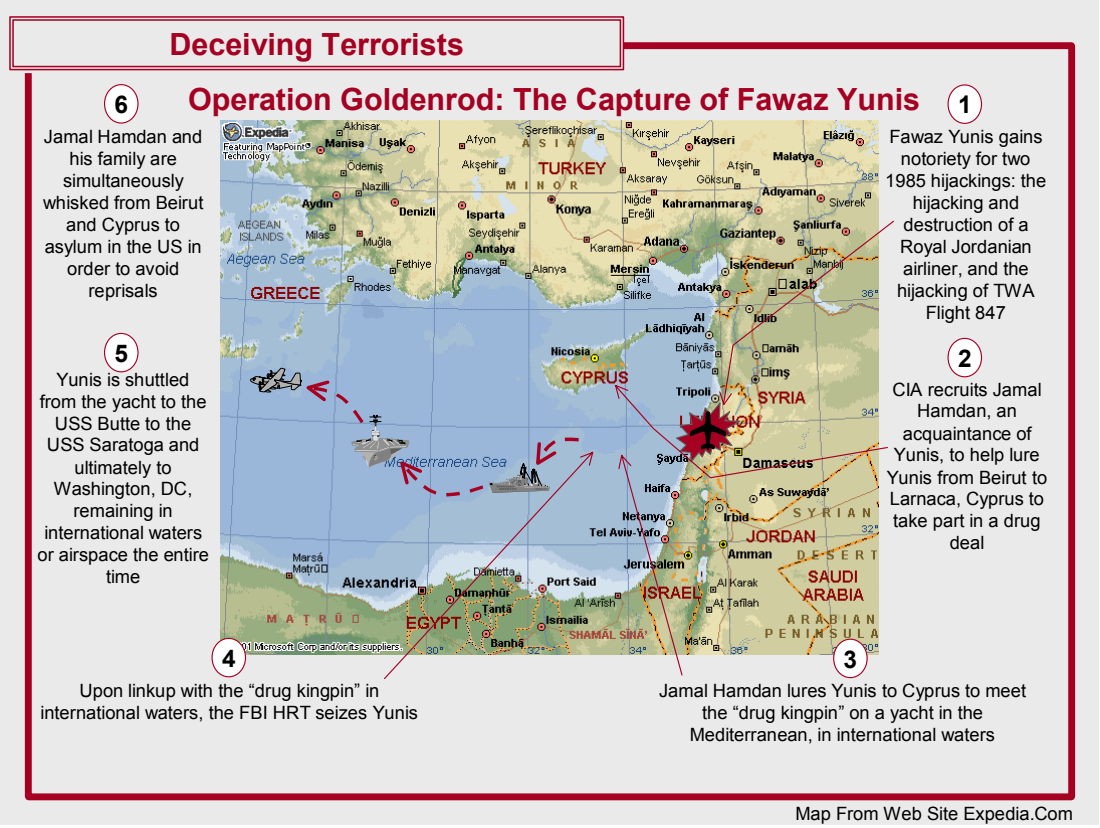


Figure 20. The Capture of Fawaz Yunis

The actual operation included an almost comical series of minor crises. Even before the operation got underway, the FBI Hostage Rescue Team (HRT) assigned to apprehend Yunis resisted the plan to have bikini-clad women on board the alleged kingpin's yacht, even though they were necessary to the drug kingpin cover. After a tense dispute with Clarridge, the HRT finally consented to the presence of three female FBI agents to portray the correct deception picture. Second, the local authorities had Yunis on a watch list of suspected terrorists, and began searching for him in local hotels upon discovering he had entered Cyprus. The CIA narrowly averted this crisis by having Hamdan check himself and Yunis into the same hotel from which Operation Goldenrod was being run. Third, upon leaving the harbor, Hamdan and his brother Ahmad, as well as the CIA agents designated to guide them at a distance to the yacht link-up, had trouble finding the yacht, which was out of

position. Finally, to compound the navigational problems, the elaborate communications system set up to support the operation began to malfunction as the operation commenced. Eventually, however, all of the crises were successfully resolved (Clarridge, 1997, pp. 354-358). In the end, communications were restored and Hamdan and Yunis successfully linked up with the yacht. As Clarridge had suspected, Yunis attention was immediately drawn to the "party girls." He failed to suspect that "Joseph" and his bodyguards were actually members of the HRT until he lay face down on the yacht's deck.

Within hours, the HRT transferred a straitjacketed and drugged Yunis from the yacht to a Navy ammunition ship, the *USS Butte*. Four days later, the *Butte* rendezvoused with the aircraft carrier *USS Saratoga*, where the HRT put Yunis on an S-3 Viking for the circuitous flight to Washington, DC. After the longest S-3 flight in Navy history, including two midair refuelings, Yunis and his captors landed at Andrews AFB, Maryland, without ever having entered the sovereign airspace or waters of another country (Clarridge, 1997, p. 358-359).

In retrospect, Clarridge's account of the Fawaz Yunis affair bears indications of all of the deception success factors. As the head of the operation and architect of the deception, Clarridge exercised solid, centralized control. His ability to coordinate with the HRT to resolve potential problems played a key role in achieving success. The intelligence preparation for the mission was sound. Since the target had no significant preconceptions applicable to the situation, the CIA appealed to a bias nearly as strong: greed. The fact that all involved in the operation were experienced professionals contributed to adaptability, particularly in dealing with potential crises. Finally, the deception story was extremely plausible, and was enhanced by appreciable confirming details such as the female FBI agents.

The Fawaz Yunis affair suggests one potential downside to deception to create counter-terrorist opportunities, however. As was the case in this affair, future deceptions involving third party foreign-nationals may require

employing potentially unsavory characters. Jamal Hamdan was, even within the context of the ongoing situation in Lebanon, a murderer and a black-marketer, hardly the kind of person with whom the American government prefers to affiliate. Yet, a Jamal Hamdan was absolutely necessary in order to gain the confidence of a Fawaz Yunis. While the employment of insalubrious informers and agents has been prohibited or discouraged in recent years, however, in the wake of the 11 September attacks this may no longer be a potential sticking point. The considerations that once made dealing with individuals unacceptable appear to gradually be disregarded in favor of more pragmatic approaches.

b. Sindikat I And II

In the early years of its existence, the Soviet Union conducted a number of deception operations to create opportunities for action against non-state actors viewed as threats to the fledgling nation. Operations Sindikat I and II, running from 1921 to 1927, are typical of these undertakings. Both operations targeted Boris Savinkov, a former Socialist Revolutionary Party terrorist and strong anti-Bolshevik leader who fled had fled to the West. In Operation Sindikat I, a Cheka agent named Eduard Opperput contacted Savinkov, portraying himself as a defector and presenting a suitcase full of forged documents. The documents told the story of a significant opposition movement, allegedly headed by Opperput himself, operating in Byelorussia. Ultimately, Opperput persuaded Savinkov to trust him, the forged materials, and the deception that they depicted. Savinkov accepted Opperput as a collaborator and fellow traveler. As a result, Opperput gained access to lists of genuine anti-Bolsheviks operating in Soviet territories, as well as lists of potential contacts. The Soviet intelligence and security apparatus netted virtually all those on the list; the overwhelming majority were summarily executed (Tugwell, 1990, p. 17).[83]

[83] Whereas many case presented thus far indicate tactical use of deception the Sindikat cases tend to blur the distinction between tactical and strategic.

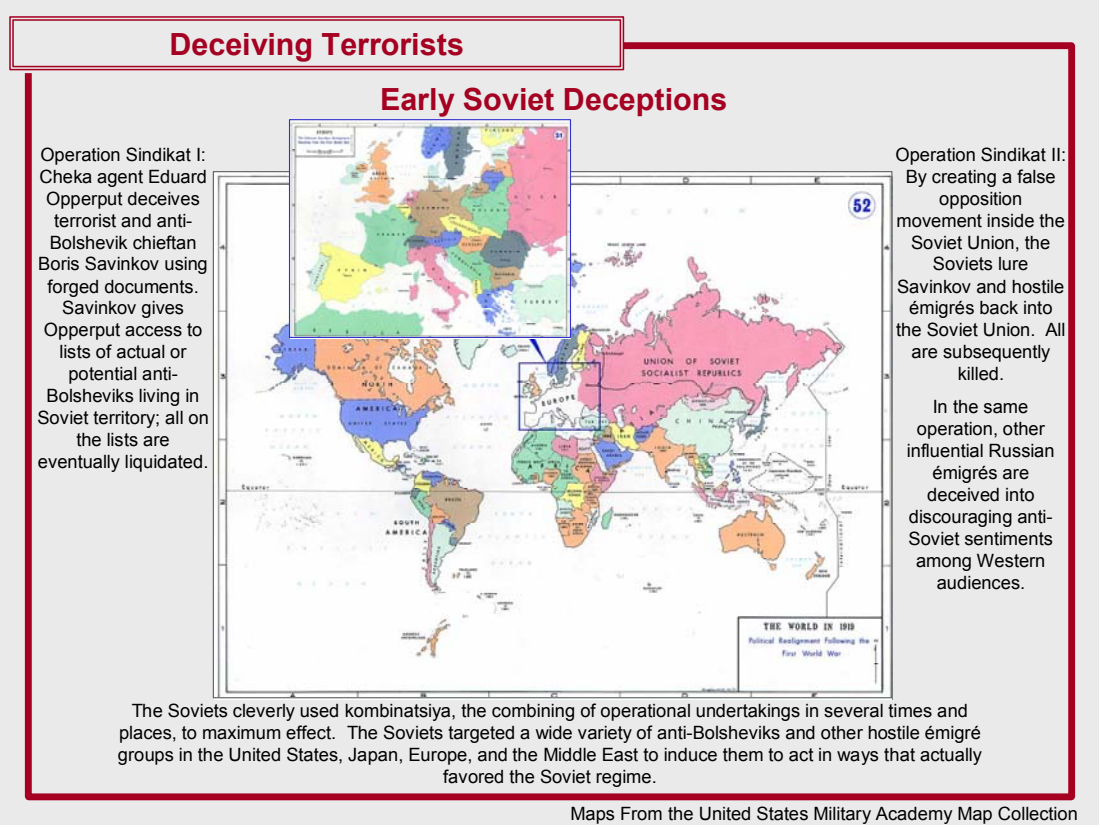


Figure 21. Soviet Capability And Intention Deceptions

Operation Sindikat II, in turn, built on the success of Sindikat I. According to Tugwell,

> The legend underpinning Sindikat II lured Savinkov into Russia where he was later killed, although it is unclear whether he had already struck a deal with the regime before returning. What seems reasonably certain is that this second legend was the famous 'Trust' (Tugwell, 1990, p. 17).

The Trust was a fabrication of Soviet state security, and it took the form of a notional opposition within the Soviet Union, supposedly named the Monarchist Association of Central Russia. The fictional Moscow Municipal Credit Association, also an invention of Soviet state security, served as the Association's cover title. Soviet state security used the Trust legend to project a false picture of reality toward not only anti-Soviet émigré's in the West, but also toward opponents within the Soviet Union and Western intelligence services and

their governments. The Trust deception was not only successful in luring Savinkov back to the Soviet Union; it also lured Sidney Reilly, the freelance agent connected with British intelligence, back into Russia as well.

c. Pseudo-Gangs

One of the most successful uses of deception against terrorists, particularly in the latter half of the twentieth century, has been the use of pseudo-gangs. The purpose of a pseudo-gang, according to Lettieri (2001), is to "perpetrate or pretend to be someone or something you are not, to sham or fake out an opponent in thinking you are one of their own in order to attain a decisive tactical advantage or surprise over the opponent you are impersonating."[84] Pseudo-gangs are typically counter-terrorist or counter-insurgent forces that pose as terrorists by adopting terrorist dress, equipment, speech, behavior, and operational methods in order to contact and intermingle with terrorists, gather intelligence, and facilitate or even conduct direct-action counter-terrorist operations. The use of pseudo-gangs has repeatedly proven to hold great potential against terrorists and insurgents. When successful, pseudo-gangs create opportunities for direct-action counter-terrorist operations, force terrorists to sacrifice efficiency in order to regain security, and assist in identifying crucial external links that the terrorist or insurgent groups rely on for support.[85]

The best-known and best-chronicled use of pseudo-gangs is that of the Rhodesian Selous Scouts, already mentioned in Chapter III. Officially formed in 1973, the Scouts were organized in response to a "drastic" increase in terrorist operations on the part of the ZIPRA and ZANLA (Dozer, 2000; Bruton, 1978, p. 17). Officially, the Selous Scout mission was tracking terrorist patrols infiltrating from safe-havens in Mozambique and Zambia. While Scouts actually performed this mission to some extent, the mission was actually a cover for their real raison

---

[84] Lettieri and other authors use the terms pseudo-gangs, pseudo-insurgents, and pseudo-terrorists interchangeably.

[85] Lettieri, Dozer, Thompson, and other authors who have written extensively on the use of pseudo-gangs in Kenya and Rhodesia use the terms insurgent and terrorist interchangeably.

d'etre: pseudo-gang operations. After detailed intelligence preparation, a Scout team would enter an area in which terrorists were known or suspected to be operating. The Scouts would establish contact with the local population in general, and specifically with terrorist "agents" within the local villages. Ultimately, the Scouts would meet and mingle with the terrorists; these meetings were either used to gather intelligence to allow other units to conduct direct-action missions against the terrorists, or were exploited by the pseudo-gangs as opportunities for immediate ambushes (Lettieri, 2000). The targets of pseudo-gang deception were two-fold. On one hand, the population of the villages was deceived to disrupt support for the terrorists. On the other hand, the terrorists themselves were deceived in order to facilitate direct action missions against them.

Rhodesian pseudo-gangs adopted a number of creative techniques to target terrorists. On more than one occasion, Scout pseudo-gangs would denounce a known terrorist contact as a traitor to the terrorist cause and subsequently execute him in front of his entire village. Since his fellow citizens invariably knew the terrorist contact to be a loyal and staunch terrorist supporter, the execution would cause incredible disillusionment and an erosion of popular support for the terrorists. At other times, pseudo-gangs posing as either ZIPRA or ZANLA terrorists would attack forces of the other group. This tactic virtually ensured that there would be a repeat clash the next time ZIPRA and ZANLA forces met. In a somewhat more dubious tactic, the Scouts would sometimes call in an air strike or direct attack on a terrorist force as the force left a kraal (village). According to Lettieri, "after two or three such occurrences the [terrorists] invariably suspected the kraal members of informing [Rhodesian] Security Forces of their presence. In revenge, and to forestall any repetition, innocent kraal members were executed" (2000). Almost without exception, this would put an end to any voluntary support that the terrorists could expect from the kraal.

While these pseudo-terrorist techniques proved effective in identifying and targeting terrorist groups and activities, they eventually incurred a substantial cost for the Rhodesian authorities. As Lettieri concludes:

> In such operations the population inevitably became the battleground. If adequate protection from the insurgents is not provided, pseudo operations cause the local population to be yet further alienated from the Security Forces. In fact, the widespread use of such operations in Rhodesia trapped the local population between the two opposing sides: the insurgents on the one hand and the Security Forces posing as insurgents on the other (2001).

In the end, the effect of these operations on the collective opinion of the population, coupled with the lack of a coherent counter-terrorism strategy, resulted in the negotiation of a political settlement to the insurgency that ultimately favored the terrorists.

The Rhodesians, however, did not pioneer the use of pseudo-gangs. Rather, the concept was copied from British operations in Kenya during the Mau Mau uprising of the early 1950's. In the later stages of the Kenyan counter-insurgency campaign, the British Special Branch used pseudo-gangs to infiltrate and then kill or capture roving bands of terrorists. British pseudo-gangs were typically led by white officers and consisted of loyal Kikuyu tribesmen, sometimes drawn from the tribal police or regular constables, and even turned Mau Mau.[86] Moreover, pseudo-gangs often included women as members, since real Mau Mau gangs typically included female terrorists. Like the real terrorists, the pseudo-gangs would call on villages at night for food, gathering information in the process. According to Thompson (1988), this not only made it easier to pass as real Mau Mau, but was also the time that the real terrorists came calling. In some cases, pseudo-gangs would use the confidence thus gained in order to arrest or ambush the terrorists. The preferred course of action of Kenyan

---

[86] The British officers, Thompson recounts, used potassium permanganate solution to color their skin, wore wigs made from the hair of dead terrorists, and learned the Mau Mau ways of

pseudo-gangs, however, was to pass the intelligence gathered through this simple deception method to tracker-combat teams for direct-action missions.

The British and Rhodesian use of pseudo-gangs is not the only case to be found. Edward Lansdale describes the use of pseudo-gangs against the Huks in the Philippines in the 1950's. According to Lansdale, the Filipino's trained and organized a company of Colonel Valeriano's 7th BCT to pose as a Huk squadron. The pseudo-Huks "lived in a jungle camp, barefoot, eating with their fingers out of community bowls, letting hair and beards grow, dressing as Huks, learning the pat phrases of dialectical materialism, and singing the enemy's songs (Lansdale, 1991, p. 88). Once employed in the field, the pseudo-Huks were able to mingle with real Huk squadrons and get close enough to surprise the insurgents in close-quarters or hand-to-hand combat.

Lansdale's account of the pseudo-Huks reveals two potential risks of such operations. First, a neighboring Filipino BCT, unaware that the pseudo-Huks were operating in their area of operations, mistook the pseudo-Huks for real Huks and engaged them. The lesson from this episode is that pseudo-gang deception operations require exceptionally close but covert coordination in order to prevent fratricide. Second, the Huks adopted the pseudo-Huk concept as their own, disguising a real Huk squadron as a Filipino BCT company. This experiment proved to be short-lived. Lansdale recounts, "On its first operation, [the real Huks] ran afoul of 7th BCT troops whose suspicions were aroused when these men in 7th BCT uniforms didn't know passwords or countersigns" (1991, p. 88). After a brief and intense firefight, the disguised Huks withdrew. Unfortunately for the Huks, however, after retreating several kilometers, they met the real pseudo-Huks returning to their own camp. After exchanging greetings and pleasantries, the two units realized the other's true identities, and the Huks found themselves engaged again in a fierce fight. After this encounter, both

---

squatting, eating, taking snuff, and other day to day activities. In addition, each white officer in a pseudo-gang had a cover man or bodyguard assigned to draw attention away from him (1988).

sides gradually dropped pseudo-gang deception operations. Lansdale concludes that tighter safeguards on both sides made the operations increasingly difficult and decreasingly productive (p. 88).[87]

The use of pseudo-gangs brings several potential risks or costs. First, according to Dozer, terrorists are likely to place greater emphasis on security. While this is a desirable effect on the one hand, since terrorist efficiency and security tend to be inversely related, it may ultimately make pseudo-terrorist and other counter-terrorist operations much more difficult (Dozer, 2001). Furthermore, there is the ever-present risk of fratricide against pseudo-terrorists. Pseudo-operations, like any other deception, thus require considerable coordination or centralized control in order to avoid compromise or "friendly-fire." This second risk must be regarded as a constant risk of pseudo-operations, but is conceivably acceptable when the benefits of the pseudo-operations outweigh the potential cost. Finally, there is, according to Dozer, the constant danger that pseudo-operations may be used as license of cover for transgression of the law. If pseudo-terrorists fail to exercise extraordinary self-discipline, terrorists or insurgents may ultimately gain considerable propaganda effects from exposing or exploiting pseudo-operations (Dozer, 2001). The use of pseudo-gangs is a new application of one of the oldest stratagems, and has been attempted in many conflicts both before and after the accounts mentioned here. In Northern Ireland, for example, the British attempted to form a pseudo-IRA effort; the attempt, however, was relatively unsuccessful and short-lived.

In the end, the close relationships between the government forces and elements of the local population were clearly a factor in the ultimate success of the pseudo-gangs. In Rhodesia, initial pseudo-gang members were loyal members of the Rhodesian army or police forces. In Kenya, Kikuyu tribesmen

---

[87] Before their use was halted, the pseudo-Huks were also used to gather information by "capturing" some in sham battles. The captured pseudo-Huks were imprisoned with real Huks; when they were released from prison, the men invariably had gathered a great deal of information on Huk operations (Leites and Wolf, 1970, p. 144).

with long-standing loyalty to the British colonial government formed the backbone of the pseudo-gangs. In neither case is there a mention of pseudo-gang members betraying their comrades. Filipino pseudo-gangs, in turn, were created from some of the best units of the Philippine Army, and had a similar reputation for loyalty. It is unlikely, however, that future pseudo-gang operations would be as successful in operations against groups where barriers to social acceptance and local support for terrorists are high.

D. DECEPTION TO CONCEAL CAPABILITIES AND INTENTIONS

States have used deception throughout history to conceal their strategic, operational, & tactical capabilities and intentions. In theory, deception can certainly be used in the same way against terrorists (Jones, 1979; Handel, 1982, p. 148). Yet, of the three categories of deception against terrorists, deception to conceal capabilities and deceptions is the most difficult to comprehend. Why should a state try to deceive terrorists about its intentions? After all, the state's ultimate goal is almost invariably to defeat terrorist opponents using any and all means available. The ultimate goal of state deception of terrorists regarding capabilities and intentions is not, however, a case of attempting to conceal the state's ultimate goal, but rather the state's specific plan for combating the terrorists. In particular, a state attempts to deceive terrorists regarding its strengths and weaknesses, specific means, and timetable for counter-terrorism operations.

Michael Handel offers one way of looking at deceptions to cover strengths and weaknesses and specific means. According to Michael Handel, these deceptions fall into two categories. "The first is intended to create an exaggerated evaluation of capabilities in terms of both quantity and quality, the second attempts to conceal existing capabilities" (1982, p. 129). The former type of bluff, Handel contends, is normally practiced by a relatively weak state that is trying to accomplish one of three ends: deter a more powerful adversary; translate an imaginative superiority in military capabilities into political gains; or

trying to gain enough time to close a dangerous capability gap (p. 129). The second type of capability deception tries to hide a state's real capabilities in order to create the impression that the state is incapable of executing certain offensive plans. In many ways, such a deception is also an attempt to conceal intentions. This latter type of deception, Handel suggests, is more frequently attempted "by military leaders and military organizations whose standard operating procedures require secrecy and deception" (Handel, 1982, p. 132). Handel concludes, "Both types of capability-oriented deceptions need not (particularly in wartime) be contradictory or mutually exclusive. A state may wish simultaneously to conceal certain capabilities and inflate others" (1982, p. 129).[88]

Maurice Tugwell, on the other hand, describes the concept behind deception to conceal a state's timetable for counter-terrorist operations: "Under such circumstances [when a state of war or conflict already exists and the intention to attack in one place or another is taken for granted]," he writes, "deception becomes much more important because it has to give the adversary the wrong expectation concerning one's inevitable and known intention to take action" (Handel, 1982, p. 128).

1. Capability And Intention Deception At Entebbe

Michael Handel suggests that the Israelis used deception to conceal their capabilities and intentions to undertake the raid at Entebbe. According to Handel:

[88] The US, for example, may want to conceal certain capabilities and intentions while greatly exaggerating others in order to force terrorists to either "go to ground" or go deeper underground.

> It is perhaps little known that the preparations for the Israeli raid on Entebbe in July 1976 also included a deception plan intended to misdirect primarily the Americans, who were apparently watching by satellite. The deception plan indicated (mainly through spreading rumors to the press) that the Israelis planned to launch a large-scale attack on PLO targets in the Lebanon in order to capture hostages who could be traded for the hijacked passengers in Entebbe. As far as is known, this deception plan successfully directed attention away from the possibility of a direct raid on Entebbe itself. The attack was a total surprise for everyone (Handel, 1982, p. 128).

Handel's allegation is certainly interesting. Unfortunately, it is neither substantiated nor supported. Moreover, the kind of deception Handel suggests was virtually unnecessary. As McRaven points out, the Entebbe mission was only possible at the strategic level because the idea of rescuing hostages from a sovereign country so geographically removed was so improbable (1995, p. 376). McRaven notes, "The boldness of the plan created an environment in which surprise was possible. As Shani said later, the raid was a total surprise, because 'nobody [thought] we were crazy enough to fly there'" (p. 376).

Those facts notwithstanding, it certainly seems plausible that the Israelis could have used deception in the manner Handel suggests. In the end, however, if true it is a case of one state deceiving another, and not of a state deceiving terrorists. A much better example of such deception is the German announcement prior to the Mogadishu hostage rescue that GSG-9 had returned to West Germany.

2. Soviet Capability And Intention Deceptions

Superior but more obscure examples of the deliberate use of deception to conceal capabilities and intentions are found in Tugwell's accounts of early Soviet deceptions such as Sindikat I and II. Tugwell suggests that a common component of the Soviet deceptions of the period was concealment of Soviet capabilities and intentions:

> Collectively, they can be viewed as survival exercises—operations to pre-empt possible threats to the young Bolshevik state. The main targets were the émigré White Russians in West Europe, the United States, and Japan, who were still actively plotting to overthrow the regime; the governments and intelligence agencies in the host countries, some of which might assist émigré operations; and, at a more abstract level, the very notion that resistance to Communism could ever succeed (1990, p. 16).

Sindikat II, for example, did not merely lure opposition leaders and agents back to their deaths. In one instance, an opposition leader was unwittingly recruited to work for the Soviet Union. Prominent émigré leader V V Shulkin was duped into making an "underground tour" of Russian opposition forces. Shulkin's visit was covertly facilitated by Soviet security, and resulted in a glowing report that was approved by the "Trust" (in actuality, Soviet security) and subsequently published in Berlin. Shulkin's report declared that Communism was on the way out in Russia and that the Soviet leaders were actually misunderstood nationalist-monarchs. This coincided with Dzerzhinskiy's New Economic Policy, which portrayed a return to a form of free market economy within the Soviet Union. By the time Operation Sindikat II concluded in 1927, the Soviets had achieved all of their original goals and then some: "internal and external opposition had been eliminated or mortally wounded, Western intelligence agencies had been humiliated, and any lingering hopes among Western governments that the Soviet regime might be overthrown were shattered" (Tugwell, 1990, p. 18).

For the Soviets, deception was just one of the elements of kombinatsiya—"the combining of operational undertakings in several times and places for maximum impact" (Tugwell, 1990, p. 18). In addition to deception, kombinatsiya made use of provocation, penetration, diversion, fabrication, and influence. Kombinatsiya, in turn, concealed or misrepresented Soviet capabilities and intentions, presenting the direction and long-term implications of real or supposed changes within the Soviet Union in such a way that the deceptions' target(s) ultimately acted to the advantage of the regime (p. 17). The effects of

the deceptions were not limited to the terrorists themselves. Western luminaries, including George Bernard Shaw, Bertolt Brecht, and Harold Laski were deceived by these kombinatsiya; in turn, they deceived their audiences with idealistic opinions and stories that were ultimately unfounded.

3. Summary

While there is, thus, evidence to suggest that deception to intentionally conceal capabilities and intentions from terrorists is a plausible application, the evidence is far less compelling—and ultimately more troubling, especially for a democratic society—than for the other uses of deception against non-state actors. An analysis of the cases presented here suggests that deception to conceal capabilities and intentions is more often a by-product of other deception operations than it is a deliberate goal (see Table 7).

Case	Primary Deception Objective	Capability & Intention Deception Intentional	Capability & Intention Deception a By-Product
Prison Sting (Strategic)	Create fissures in the IRA	No	No
Huk Rebellion (Strategic)	Create fissures in Huk forces; separate Huks from their popular base	No	No
Abu Nidal Affair (Strategic)	NA	No	Yes
German Hostage Rescue at Mogadishu (Strategic/Tactical)	Divert attention and gain relative superiority	Yes	Yes
Israeli Hostage Rescue at Entebbe (Tactical)	Confuse guards and terrorists and gain relative superiority	Uncertain	Yes
Israeli CT Operations (Strategic)	Prevent interference with operations	Yes	Yes
Rhodesian Tactical Operations (Strategic/Tactical)	Facilitate infiltrations and gain relative superiority	Yes	No
Fawaz Yunis Capture (Tactical)	Create opportunity for direct action	No	No
Sindikat I and II (Strategic/Tactical)	Identify terrorist structure; create opportunities to target threats to state	Yes	Yes
Pseudo-gang Operations (Strategic)	Overcome weaknesses in intelligence gathering and facilitate direct-action missions	Uncertain	Uncertain

Table 6. Assessment Of Deception To Conceal Capabilities And Intentions

E. CONCLUSION

Deception to create and exploit organizational weaknesses and inefficiencies holds enormous potential. Deception to facilitate counter-terrorist

operations seems to occur routinely. Finally, although the evidence is hardly substantial enough to be conclusive, deception to conceal a state's capabilities and intentions seems to occur most frequently as a by-product of other operations.

States have clearly used deception throughout history to gain a competitive advantage against terrorist opponents. It is just as clear, however, that deception has not proven to be a "silver bullet," guaranteed to work all of the time, to achieve the desired result, etc. Quite to the contrary, it is evident that the use of deception against terrorists holds a number of potential costs and risks. Chapter V turns to the subject of the costs and risks of deceiving terrorists.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE COSTS AND RISKS OF DECEPTION

On 18 February 1978, two gunmen entered the Hilton Hotel in Nicosia, Cyprus, and assassinated Yusuf el Sabai, editor of the Egyptian newspaper *Al Ahram* and secretary general of the Afro-Asian People's Solidarity Organization. One of the terrorists pinned el Sabai to the floor of the hotel lobby with his knee and shot him three times in the head—killing him instantly. Then, the terrorists took 30 hostages in the hotel's restaurant, threatening to blow them up with grenades unless the Cypriot government flew them out of the country. Among the hostages were the Moroccan, Sudanese, Syrian, Somali, Yemeni, PLO, and Lebanese Communist Party delegates to the AAPSO meeting (Mickolus, 1985, pp. 774-776).

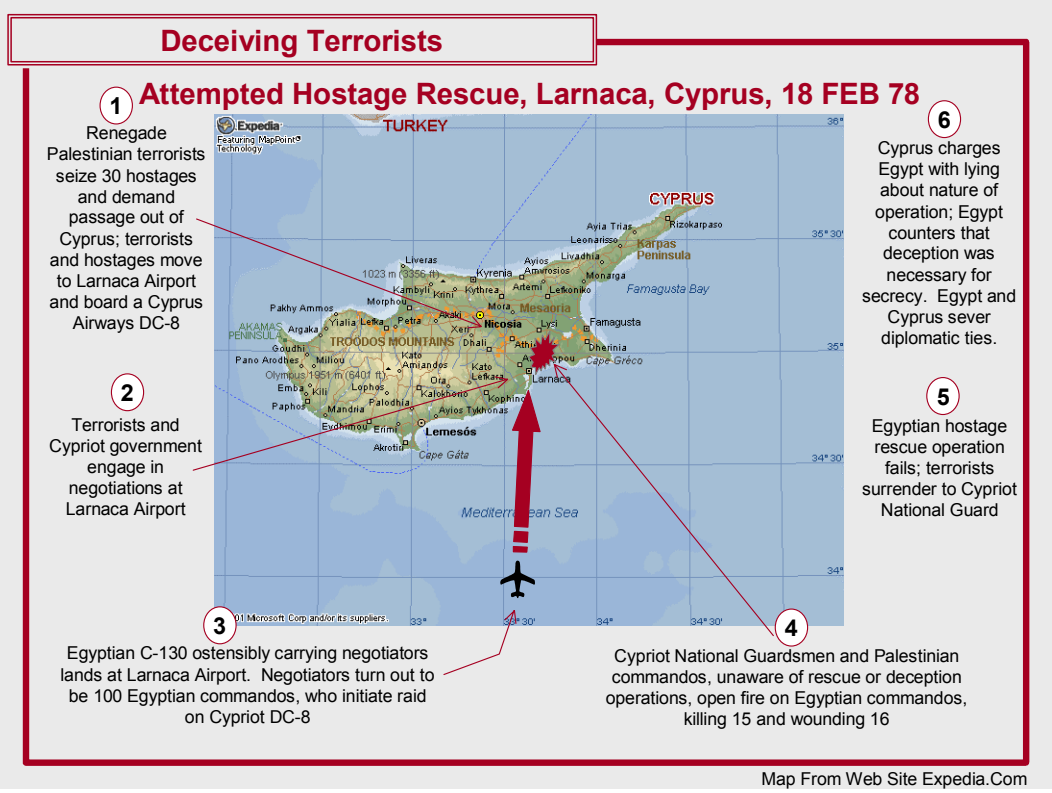


Figure 22. Egyptian Hostage Rescue Attempt at Larnaca

At 1400 that day, the terrorists agreed to release 12 hostages in return for safe transport to Larnaca airport. Once at the airport, the terrorists released an

additional seven of the remaining hostages in exchange for a Cyprus Airways DC-8. At 2030 that evening, the terrorists and their hostages, along with a four-man volunteer crew, took off in to the Mediterranean night. Once in the air, the terrorists were denied entry first by Libya, then by Kuwait, Somalia, and Ethiopia in rapid succession. Yemen likewise refused the plane permission to land. Finally, Djibouti allowed the plane to land, but only to refuel and leave the country. By 1730 the following afternoon, with Algeria having refused entry to the terrorists as well, the terrorists and their hostages were back in Larnaca, where the flight had begun.

Once in Larnaca, talks between the terrorists and the Cypriot government resumed. Bruce Hoffman describes what happened next:

> In the midst of negotiations between the Cypriot government and the two terrorists, an Egyptian C-130 landed at the airport, supposedly containing Egyptian government officials who would assist in the negotiations. Instead, the plane contained 100 commandos, who burst out of the aircraft and proceeded to attack the Cypriot DC-8. Cypriot National Guardsmen and a team of Palestinian commandos sent by PLO leader Yasir Arafat to assist the Cypriots opened fire on the Egyptian commandos, killing 15 and wounding 16 (1985, p. 57).

Despite what was—up until the moment of assault—a successful deception, the hostage-rescue mission proved a complete failure for the Egyptians. The Egyptian commandos were thoroughly routed. The terrorists immediately surrendered to the Cypriot National Guardsmen. Cyprus angrily claimed that the Egyptians had deceived them about the fact that the C-130 carried commandos instead of the expected negotiators. Egypt immediately countered that they had, in fact, informed the Cypriots of the rescue attempt, only to recant the next day and admit that they failed to notify the Cypriots because they feared a leak. Cyprus responded that a tentative surrender had already been negotiated. Cyprus rejected Egypt's extradition request, and the nations suspended diplomatic relations two days later.

Many of those who study about and write on deception suggest that deception is cheap. Michael Handel, for example, observes that deception "is neither labor- nor capital-intensive. It is among the least expensive types of modern intelligence work yet yields a high return for a relatively small investment" (1982, p. 143). As a result, he recommends that deception should be included in virtually all operations: "Rationality dictates that a move which involves little cost and little risk of failure should always be included in one's repertoire (p. 144). The case of the failed hostage rescue at Larnaca, however, suggests that deception is not without certain risks and costs. In fact, one of the least explored aspects of deception concerns those characteristics and the impact they have on those who endeavor to deceive.

This chapter considers the costs and risks of deception, beginning with a general discussion of those costs and risks. Once the discussion of risks and costs is concluded, this chapter turns to a closely related subject: the legal cases for deception. The second section of this chapter outlines the legal considerations concerning the use of deception in general, and its application against terrorists in particular. Then, the section turns to the subject of the ethics of deception. A general framework for analyzing the ethics of deception operations is offered; this framework is subsequently applied to some of the cases already discussed in this thesis.

A. COSTS AND RISKS OF DECEPTION

Although costs and risks might appear at first to be one and the same, there is in fact a distinction between the two. A deception cost, on the one hand, is an expenditure that may be incurred as a result of undertaking deception. A deception risk, on the other hand, is a chance of injury, damage, or loss as a result of undertaking deception. Costs are almost certain to arise, although they are by no means guaranteed; risks are less certain to arise, consisting more of potentially adverse outcomes. There are six general categories of deception

costs, as well as four general categories of deception risks. The next sections explore these risks and costs.

1. Deception Costs

The costs that states may incur through the use of deception fall into six general categories: time, resources, flexibility, intelligence, coordination, and reputation. The first category, time, is generally overlooked as a potential cost of deception, despite the fact that the decision to resort to deception generally incurs some time cost for the deceiver. As noted in Chapter II, decision-makers must approve a deception, planners must design it, and the "transmitters" must send the appropriate signals to the enemy. On the target's side, receivers must observe the signals; analysts must determine what those signals mean (putting the deception story together); gatekeepers must screen the information and pass it on to decision-makers. Once the deception reaches enemy decision-makers, a decision must be made and specific actions ordered. It takes some amount of time, in turn, for those actions to occur, and more time still for the deceiver to gather feedback on whether the deception is working.

For a tactical deception, these steps may take a very short time—no more than a few days. For a strategic deception, on the other hand, the deception may take months or even years to develop and to produce results. Generally speaking, the deceiver has more time at the strategic level. However, if the deceiver's situation compels him to take action immediately—to forestall a particular enemy course of action, for example, or to facilitate a planned operation—the time costs of an elaborate deception may make deception too expensive a course of action.

The second category of deception costs concerns resources. Despite the assertion of Handel and others that deception is a relatively cheap course of action insofar as resources are concerned, the decision to employ deception nonetheless imposes some resource costs on those who undertake it. Chapter II suggested that competition for finite resources is a dilemma that every

commander faces at one point or another. Even for a resource-rich nation such as the United States, there are rarely enough resources for a decision-maker or commander to do all that he needs or would like to do. As John Van Vleet points out, “Competition for resources…is such that the requirements [to carry out deception] will have to be filled using the existing force structure. Any proposal for how to do that will have significant drawbacks and will produce many reasons that it cannot be done” (Van Vleet, p. 229). Deception operations invariably draw resources away from other missions and operations. Deception thus generally incurs some resource cost on those who undertake it.

The third category of deception costs concerns flexibility costs. At an operational or tactical level, commitment to a deception operation generally commits leaders and decision-makers to a particular course of action. This is not merely because the deception supports one particular course of action, but because the allocation of resources to the deception operation may preclude other operational courses of action. At a strategic or grand strategic level, on the other hand, commitment to a deception operation may reduce the political and diplomatic options available to decision-makers, force them to take certain actions to support the deception, and preclude the pursuit of other activities which might expose the deception or reveal the dissimulated course of action.

The fourth and fifth categories of deception costs, respectively, are intelligence and coordination costs. These costs, and their impact on the success of deception, were also covered in significant detail in Chapter II. Intelligence, for example, must perform five critical roles in the planning and conduct of deception. First, intelligence must identify adversary decision-makers and assess their vulnerability to deception. Second, intelligence must determine the adversary’s preconceptions of friendly capabilities and possible courses of action. Third, intelligence must produce estimates of adversary actions under various friendly actual and deception scenarios. Fourth, intelligence must identify adversary information gathering capabilities and communication systems to determine the best conduits for a particular deception. Finally, intelligence must

assist in the establishment and monitoring of feedback channels to evaluate the effectiveness of the deception operation by observation of the adversary's reaction. Because these basic intelligence tasks must be undertaken in order for deception to succeed, intelligence is, therefore, a necessary cost of deception (JP 3-58, 1996, p. II-2-3; Sherwin, 1982, pp. 79-80).

Coordination is also a necessity for successful deception—and may be costly. As Chapter II made clear, detailed coordination—along with centralized control—contributes to successful deception by facilitating mutual support between deceptions and actual operations (Fowler and Nesbit, 1995, p. 44). This mutual support subsequently contributes to the likelihood of success by insuring against compromise of the deception, by facilitating protection of limited resources, and by facilitating positive control (Godson and Wirtz, 2000, p. 426; Van Vleet, 1985, p. 19). Undertaking deception, therefore, incurs a coordination cost on the state that chooses to use it.

The final category of deception costs, however, is one not yet mentioned anywhere else in this thesis; it concerns the reputation of the deceiver. Damage to the deceiver's reputation is always a potential cost of deception. It is, however, less certain to be incurred than the other costs of deception. Nowhere is this potential cost felt more acutely for the deceiver than on the domestic front. As the noted ethicist Sissela Bok observes in her commentary on lying to enemies, "all too often, the lie directed at adversaries is a lie to friends as well; and when it is discovered, as some always are, the costs are high" (1999, p. 141). Maurice Tugwell echoes and elaborates on Bok's simple observation. On the domestic front, Tugwell suggests,

> [The] dichotomy between ethics and practice can have serious consequences when deception fails, or [even] when it is discovered. This is particularly so when, as these cases reveal, the domestic audience becomes one of the primary targets of a deception. While the immediate embarrassment of the perpetrator may be short-lived, the long-term consequences may be much more serious: the erosion of public confidence and trust in elected officials which is essential to a healthy democracy (Tugwell, 1990, p. 265).

Costs to the deceiver's reputation are potentially substantial on the international front as well. "Trust," Tugwell suggests, "is the first casualty of deception on the international front" (1990, p. 405). Failed or discovered deception, according to Tugwell, invariably erodes whatever trust exists between nations. "Without trust," he asks, "how can relations between blocs, states, or individuals be anything other than a state of undeclared war (Tugwell, 1990, p. 405)?

While there is a certain common sense to Tugwell's statement, it must be placed in context, however. States are rarely completely forthcoming in their interactions with each other. Some minimum threshold level of espionage, deception, and gamesmanship is an inherent part of the relationship between nations. The case of the failed Egyptian rescue attempt at Larnaca, however, illustrates that some deceptions, as well as the operations that they cover, may cross that threshold and incur a high cost for the nation that is discovered.

2. Deception Risks

While costs are almost certain to arise from the use of deception, risks are less certain. Risks more accurately correspond with potential adverse outcomes of deception. There are four basic categories of deception risks: deception failure; exposure or blowback; unintended consequences; and third party actions (see Table 8).

Deception Failure
The message is lost in transmission and never reaches the target
A competing signal or noise overwhelms the message in transmission
The "clue" is modified or garbled in the channel; the target receives a different signal
The transmission is received but competing signal(s) overwhelm it in interpretation and replace it
Target receives the transmission but analysts garble the interpretation
Analysts receive and interpret signal correctly but dismiss the message as trivial or irrelevant
The transmission is received and interpreted correctly but a gatekeeper prevents it from reaching the decision-maker
Exposure or Blowback
Media may discover and expose deception operation prior to execution
Media or other parties may expose deception after the fact
Unintended Consequences
Target receives and interprets signal correctly but the decision-maker ignores it
Target decision-maker receives and interprets the signal as intended but takes an altogether unintended action
Unintended targets on the deceiver's side may receive deception message and take action as a result
Third-Party Risks
Third parties receive deception signal and take unintended action
Third parties interfere with target taking desired action

Table 7. Summary of Potential Deception Risks[89]

As with any operation, failure is always a risk attendant to deception. Even with the perfectly executed deception, there is no guarantee of success, even though all of the success factors are present. Deceptions fail for any number of reasons. One common source of deception failure, as Robert Jervis points out, is improper crafting of the deception message: "Deception that is too

[89] Like the list of potential deception outcomes, this list is not exhaustive; rather, it merely illustrates the range of potential deception risks.

sophisticated and elegant may be intellectually satisfying to those who create it, but may not be picked up by the intended victim" (Handel, 1982, p. 134). Handel expands on Jervis's observation:

> There is an obvious danger that the message developed by the deception planners is understood by them in the context of the endless meetings in which alternatives were weighed and details worked out. They are so familiar with their own thinking that they risk overlooking the degree to which the message is clear only to them only because they know what to look for (Handel, 1982, pp. 134-135).

Yet deceptions fail for other reasons as well, as the preceding figure illustrates. Sometimes, the target either simply fails to pick up the signals that comprise the intended message or sees through them. At other times, the cacophony of competing noise prevents the target from paying proper attention to the message. Furthermore, the deception message may be received and may be believable, but it may be ignored nonetheless at some level of the target's hierarchy.

The second deception risk is exposure or blowback. Simply put, the discovery of deception may cause a backlash against the deceiver. This may or may not cause the deception to fail, but virtually always results in unwanted attention or pressure.[90] One example of deception blowback is the American attempt to destabilize the Libyan regime of Moammar Gadhafi and end Libyan sponsorship of terrorism in 1986. When the American media discovered that not only was there a plot, but that they had been used to unknowingly perpetrate the deception, the resulting blowback was immense (Walcott, 1986, p. A1; Tugwell, 1990, pp. 403-404).[91] Tugwell suggests that exposure or blowback is more likely to occur in and to open, democratic nations than in closed ones (Tugwell, 1990, pp. 403-404).

---

[90] This is closely related to the potential deception cost of reputation.

Unintended consequences are another potential deception risk. Unintended consequences, in turn, can be classified into two categories—friendly and enemy. Chapter II suggested two potential enemy unintended consequences. On the one hand, the target may receive and interpret the deception correctly, only to have the decision-maker ignore the message for one reason or another. Alternately, the target may receive and interpret the deception correctly, but the message may prompt the decision-maker to take unintended actions (Herbig and Daniel, 1981, pp. 28-32). Moreover, the target may redouble its own efforts as a result of the deception and end up in a position of strength relative to the deceiver (Handel, 1982, p. 132).[92] In short, even if the target "buys" the deception message, he may do something entirely different than what the deceiver wants and intends, something ultimately detrimental to the deceiver. Furthermore, even if the target understands and does what the deceiver intends for him to do, he may take some long-term action that works in his favor and against the deceiver. The IRA reorganization following the Prison Sting is one such example of a long-term unintended consequence.

Unintended consequences on the part of the target are not the only risk to the deceiver. Unintended consequences also occur when the deceiver is seduced by his own deception. The risk of falling for one's own deceptions is not a simple matter of believing in one's own capabilities even though one should know better. In some cases, it is a matter of one hand not knowing what the other is doing, as Tugwell points out:

---

[91] The paradox of blowback is that the risk is generally strategic, even if the deception itself is not. The blowback from the Egyptian operational deception at Larnaca certainly occurred on a strategic, even though the deception was a simple, tactical one.

[92] The British development of a strong defensive air force as a result of German strategic deception in the 1930's is a classic example of this unintended consequence (Mihalka, 1980). When war ultimately broke out, the British won the Battle of Britain as a long-term result of the German deception.

> Moreover, these [propaganda & deception] activities may have complicated the intelligence analysis process; on more than one occasion OSS-planted disinformation rumours [sic] were picked up by Allied intelligence, which was unaware of the original source of the information. This kind of blow-back is a risk inherent in deception operations where co-ordination [sic] is poor, as was sometimes the case during [WW II] (Tugwell, 1990, p. 270).

The final category of deception risks is third party actions (Jervis, 1968, p. 476). As pointed out in Chapter II, even if all goes well in the exchange between deceiver and target, third parties may take actions that cause a deception to fail or to be altered. On the one hand, third parties may interject their own messages that interrupt, overwhelm, modify, or contradict the deceiver's signals. Moreover, third parties may see through and unmask the deception either intentionally or unintentionally. Finally, third parties may be deceived themselves and take unintended actions as a result (Reese, 1982, pp. 99-102; Moose, 1982, pp. 137-138). The actions of the Cypriot National Guard during the attempted hostage rescue at Larnaca illustrate the potential for third party actions to either undo the deception or render it useless.

B. THE RIGHT AND WRONG OF DECEPTION

Serious consideration of the topic of deception should, at a minimum, address the basic legal and ethical questions to which deception gives rise. Is deception legal? Is deception ethical? What ethical argument exists to justify deception? This section offers a brief examination of these questions.

1. The Legal Status of Deception

In general, the use of deception by states as a tool of armed conflict is legally permissible under the provisions of the Geneva Conventions, albeit within

certain guidelines.[93] Specifically, Protocol I of the Conventions, relating to the "Protection of Victims of International Armed Conflicts," allows:

> Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation (Protocol 1, Art. 37).

What is not legally permissible, according to Protocol I, are perfidious acts. The Protocol defines perfidy as "acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence…" (Protocol I, Art. 37). Conspicuously perfidious acts include feigning intent to negotiate under a flag of truce or surrender, feigning incapacitation by wounds or sickness, feigning civilian or other non-combatant status, or feigning protected status through the use of signs, emblems, or uniforms of "neutral" organizations such as the United Nations or the International Committee for the Red Cross (Protocol I, Arts. 37-39). Moreover, under the 1977 Protocol, the use of "the flags or military emblems, insignia or uniforms of adverse parties while engaging in attacks or in order to shield, favour, protect, or impede military operations" is also prohibited (Protocol I, Art. 39).

---

[93] There is not simply one Geneva Convention. In fact, the first Geneva Convention was signed in 1864 to cover the subject of sick and wounded in war. Two conventions were signed in 1899, concerning asphyxiating gases and expanding bullets. Thirteen treaties covering a variety of subjects were signed in 1907. The Geneva Gas Protocol was added in 1925, covering the use of poison gas and bacteriological warfare. Two more conventions were adopted in 1929 to deal with treatment of wounded and prisoners of war. In 1949, four new conventions were added to extend protections to civilians and to those shipwrecked at sea. Since that time, two additional conventions and two protocols have been included. In most contexts, the common term Geneva Convention thus includes the vast body of international law and treaties on the conduct of armed conflict (see Society of Professional Journalists Web site: http://www.the-spa.com/genevaconventions/history.html).

The Department of Defense's Operational Law Handbook elaborates on the distinction between lawful deception and perfidy, offering several useful examples in the process:

> Protocol I, Art. 37 prohibits belligerents from killing, injuring, or capturing an adversary by perfidy. The essence of this offense lies in acts designed to gain advantage by falsely convincing the adversary that applicable rules of international law prevent engaging the target when in fact they do not. The use of enemy codes and signals is a time-honored means of tactical deception. However, misuse of distress signals or of signals exclusively reserved for the use of medical aircraft would be perfidious. The use of deception measures to thwart precision guided munitions would be allowed, while falsely convincing the enemy not to attack a military target by evidence that it was a hospital would be perfidious (Meyer and Bill, 2001, p. 358).

These distinctions can be used as a basic test to analyze some of the cases presented to this point. Under international conventions, the actions of Israeli commandos posing as Red Cross officials in order to facilitate hostage-rescue operations are not, in isolation, perfidious. On the other hand, Israeli commandos posing as Red Cross officials and actually taking part as "shooters" in the hostage-rescue and killing or wounding the hijackers appears to be perfidious. In a similar manner, Selous Scouts acting as pseudo-terrorists in order to gather information later used to take direct-action against terrorists is not a case of perfidy (Meyer and Bill, 2001, p. 20). On the other hand, Selous Scouts posing as FRELIMO soldiers in order to gain access to a terrorist training camp and subsequently raiding that training camp while still dressed as FRELIMO soldiers is a fairly clear case of perfidy (Meyer and Bill, 2001, p. 20; Protocol I, Art. 37).

While these simple distinctions are fairly clear, the waters become muddied in the case of conflict between a state and a terrorist group. According to the Operational Law Handbook, "terrorists, by definition, do not meet the four requirements necessary for combatant status" (Meyer and Bill, 2001, p. 314).

Since terrorists are not legal combatants, the international conventions that govern armed conflict theoretically no longer bind the state that is compelled to respond to terrorism with force. Generally speaking, terrorists do not wear uniforms or other distinctive insignia; neither do they carry arms openly. Moreover, terrorists are not presumed to be under the command of a person legally responsible for group actions. Finally, terrorists generally do not conduct their operations in accordance with the international laws of armed conflict. Still, US policy is to "apply the 'principles and spirit' of the Law of War" to the conduct of its own soldiers, regardless of the nature of the enemy or the applicability of the Law of War (Meyer and Bill, 2001, p. 10). As an example, soldiers taking part in peacekeeping operations do not, technically, have to follow the laws of armed conflict; nonetheless, the US generally requires its soldiers to follow those laws.

From these seemingly conflicting viewpoints, two conclusions can be drawn. First, state deception against terrorists, like state deception against other states, is generally legal (Personal communication with Colonel Jim Coyne, Staff Judge Advocate, V Corps, USAREUR, 23 October 2001). Second, while perfidious acts against terrorists are not technically illegal, for Americans at least, the same body of law that governs armed interstate conflict generally guides the practice of deception against terrorists.

2. The Ethical Status of Deception

Because something is legal, however, doesn't make it ethical. Certainly, segregation of African-Americans in the United States was legal in many states in the years prior to the 1960's. Just as certainly, however, those laws were unethical. That this paradox exists between legality and ethics compels us to look more closely at whether deception is, in fact, ethical.

Maurice Tugwell is one of the few serious researchers of deception who addresses its ethical status in any way. According to Tugwell:

> On the one hand, there are strong ethical strictures against deception, rooted in the West's religious teachings and moral philosophy. The Ninth Commandment, for example, states clearly, 'Thou shalt not bear false witness…' Yet it is equally clear that deception has a long history in the West, dating from classical times. The writings of Francis Bacon, Edmund Burke, Alexis de Tocqueville, and Lewis Carroll attest—in their criticism of deception—to its longevity and persistent presence in political life. In this century, its use has spread from party politics to business and advertising and to war and diplomacy. Western democracies have resorted to deception readily in time of war, and with only slightly less enthusiasm in the 'Cold War'. In short, insofar as Western experience is concerned, ideals are one thing, practical affairs are somewhat different (Tugwell, 1990, p. 265).

Tugwell's insight is a starting point for thinking about the ethical status of deception, although more is needed. Deception must be held up to the magnifying glass of ethical decision-making in some way. Thus, let us take for a moment the viewpoint of one well-known ethicist. Rushworth M. Kidder, the author of How Good People Make Tough Choices, suggests "an orderly sequence for dealing with the admittedly disorderly and sometimes downright confusing domains of ethical issues" (1995, p. 183). Kidder's nine-step framework holds promise as a tool for analyzing the ethical status of deception.

The first set in making an ethical decision, according to Kidder, is to recognize that there is a moral issue (1995, p. 183). This step requires a decision-maker to identify the issues needing attention, rather than brushing past them without consideration. Moreover, it requires the decision-maker to sift genuine ethical questions from those that merely involve social conventions. The second step, in turn, is to determine the actor—that person or entity responsible for making the decision on the issue at hand (p. 183). The third step, then, is to gather the relevant facts. As Kidder points out, "ethics does not happen in a theoretical vacuum but in the push and pull of real experience, where details determine motives and character is reflected in context" (pp. 183-184).

The next step in the ethical decision-making framework, according to Kidder, is to test for right-versus-wrong issues (1995, p. 184). The first test of right-versus-wrong is legal; that is, is the law clear on the question at hand? If the choice is, indeed, one between right and wrong, legal and illegal, then there is no ethical dilemma.[94] If the law is not clear on the question at hand, however, Kidder suggests three tests to help determine the proper course of action. The first is rule-based reasoning, or what Kidder refers to as the "stench test." Kidder advises that if an action "just smells wrong," in a visceral sense, it probably is the wrong ethical decision. The second test is ends-based reasoning, which looks to consequences as a decision factor. Kidder refers to this test as the "front-page test." This test asks the decision-maker to judge the "right" course of action according to how he would feel if the decision were to become public, front-page material. The final test is care-based reasoning, something Kidder describes as the "Mom test." The focus, according to Kidder, is what choice the decision-maker thinks his mother or some similar moral exemplar who cares deeply about the decision-maker would choose (pp. 184-185). If an issue fails these tests, Kidder offers, "there's no point going on to the following steps. Since you're dealing with a right-versus-wrong issue, any further elaboration of the process will probably amount to little more than an effort to justify an unconscionable act" (p. 185).

If the issue facing the decision-maker passes the right-versus-wrong tests, the next step is to test for right-versus-right paradigms. Based on a broad survey of various schools of ethical thought, Kidder suggests four ethical dilemma paradigms: truth-versus-loyalty; self-versus-community, short-term-versus-long-term; and justice-versus-mercy. The reason for identifying the applicable paradigm is not merely an academic exercise; rather, the decision should bring

---

[94] Even if an ethical question passes the initial legal test, the decision-maker should at least consider the following steps. After all, as the segregation example points out, just because something is legal doesn't make it "right."

the dilemma into a decidedly sharper focus, particularly if it pits two deeply held values against each other (Kidder, 1995, p. 185).

Once the dilemma has been brought into focus, the next step is to apply the resolution principles of classical ethical thought: the ends-based or utilitarian principle; the rule-based or Kantian principle; and the care-based or Golden Rule principle (Kidder, 1995, p. 185). The goal in this step is to determine which of the three seems most relevant and persuasive to the question at hand.

After that, the next step is to investigate the "trilemma" option. Specifically, this step, which may actually be called into play anywhere in the nine-step process, asks if there is a third way through the dilemma. The third way out, if present, may either be the result of a compromise between the principles at play or the result of a creative course of action that comes to light during consideration of the issue (Kidder, 1995, pp. 185-186).

Once these steps are complete, the subsequent step is to make the decision. This step is the critical link between analysis and action, and between the theoretical and the practical (Kidder, 1995, p. 186). Finally, Kidder suggest that the decision-maker return to the question once the issue has settled somewhat, reviewing the question and seeking the lessons that will build expertise, adjust the moral compass, and provide new examples for moral discourse and discussion (p. 186).

When applied to the subject of deception of terrorists in general, Kidder's framework reveals little. In a general sense, we have already seen that deception is legal. However, too many key details necessary to frame the questions and apply the right-versus-right paradigm and resolution principles are missing to grant blanket ethical approval to deception against terrorists.[95]

The framework is valuable on a case-by-case basis, however, for determining whether a particular deception operation is ethical. The Egyptian

deception operation in support of the attempted hostage-rescue at Larnaca, for example, fails at the right-versus-wrong step of Kidder's framework for two reasons. First, the failure of the Egyptians to "read in" the Cypriots on the plan, while understandable, violated the sovereignty of the state of Cyprus. In contrast, the German notification of the Somali government, admittedly a calculated risk, respected the sovereignty of the Somalis.[96] Second, the portrayal of commandos as negotiators, although not expressly forbidden by international law, tends to violate the good faith principle that underlies that body of law. In contrast, the Fawaz Yunis affair passes the ethical test. Not only was the operation legal, but the real ethical question—whether to employ Jamal Hamdan to deceive Yunis—was justifiable under the right-versus-right paradigms and the utilitarian resolution principles. The framework thus offers one tool for resolving ethical questions regarding the use of deception in specific cases against terrorists.

C. SUMMARY

The observations of Whaley, et al, suggest that deception generally is a low-cost, low-risk undertaking. This, however, is not always the case, as this chapter shows. The potential costs and risks of deception operations are substantial. In many ways, deception, even if successful, may result in a high price for the state that chooses to use it. Still, though, conflict itself is an expensive business. There are risks and costs attendant to virtually every action that a state takes in armed conflict, even in armed conflict with terrorists. For this reason, those who choose to employ deception as a tool against either state or non-state actors should strive to gain an appreciation of the risks and costs that a

---

[95] This does not imply that deception versus terrorists, while legal, is unethical in most cases; it merely suggests that more information is usually necessary to make a valid ethical decision.
[96] One common cognitive bias is the false analogy. In keeping with that bias, it is tempting to use the example cited here to question the Israeli operation at Entebbe. After all, the Israelis did not have Ugandan permission to conduct the operation. In fact, however, the complicity of the Ugandans in the terrorist operation changes the facts of the case entirely, negating the legal consideration of sovereignty.

particular deception course of action will incur relative to the benefits that deception is likely to provide.

Moreover, careful consideration should be given to whether a particular deception is, in fact, legal, and whether it is ethical. The framework offered here is only one means of making that decision regarding the legality and ethics of a given deception operation.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

"…A peaceful, gain-loving nation is not far-sighted, and far-sightedness is needed for adequate military preparation, especially in these days."

Alfred Thayer Mahan, 1894

A. SYNOPSIS

This thesis addresses one means available to states for dealing with terrorists. The study began by exploring the body of theoretical literature in order to establish the foundation necessary for a discussion of deception. Deception was defined as those actions taken during periods of conflict or intense international competition to deliberately confuse or mislead enemy decision-makers, with the ultimate goal of gaining a decisive advantage by provoking a specific action (or the lack thereof) on the adversary's part. Furthermore, deception was distinguished from related activities such as PSYOPS, propaganda, OPSEC, and camouflage.

Next, the thesis examined the six reasons that states use deception in interstate conflict. In particular, the study found that states employ deception during periods of armed conflict in order to gain or maintain surprise, to create conditions favorable to victory, and to reduce risks and costs. It also demonstrated that states use deception in situations short of armed conflict in order to mobilize groups and to protect legitimacy. Finally, it noted that there is considerable evidence that states use deception in periods of both war and peace to conceal capabilities and intentions. From this list, three potential uses of deception against terrorist were suggested. Specifically, the thesis proposed that states use deception to create and exploit organizational inefficiencies and weaknesses in terrorist organizations, facilitate counter-terrorist operations, and conceal counter-terrorist capabilities and intentions. Subsequently, the cases presented in this thesis illustrated that deception has enormous potential as one tool to deal with terrorists. In particular, they revealed that states have in fact successfully used deception in the past to create and exploit organizational

inefficiencies and weaknesses in terrorist organizations, facilitate counter-terrorist operations, and conceal counter-terrorist capabilities and intentions.

The examination of deception against terrorists was prefaced with a look at the rise of terrorist networks, a trend that holds unusual significance for counter-terrorism. From this brief appraisal, a number of implications, both for counter-terrorism in general and for deception against terrorists in particular, were offered.

Finally, this thesis also explored two areas that normally receive little attention in typical anecdotal studies of deception. First, it explored the analytical works of deception observers from a number of different academic backgrounds. The resulting multidisciplinary approach afforded a unique glimpse into how deception works and suggested a number of factors necessary for successful deception. Second, this thesis addressed the often-overlooked subject of risks and costs, demonstrating that the use of deception is almost never without expense. Even when deception succeeds, its use inevitably incurs costs and opens the door to certain risks. Moreover, the study showed that deception—while both legal and ethical in the larger sense—might be illegal or unethical in certain applications.

B. CONCLUSIONS

This thesis shows that deception is, indeed, a valuable tool against terrorists. It is necessary, however, to emphasize four additional conclusions in this closing chapter.

First, the likelihood of achieving successful deception depends on four success factors: centralized control, coordination, and integration; intelligence; adaptability and feedback; and plausibility and confirmation. These success factors can be viewed in much the same way as McRaven's six principles of special operations. All are present to some extent in successful deceptions; however, the importance of each varies in relation to the situation. Although

there is no magic formula that can be applied to deception, the success factors can be viewed as four pillars on which every deception should be founded.

Second, the "right" application of deception depends on the situation. The cases presented here seemed to suggest that each potential use of deception against terrorists may be more beneficial at certain levels of application than others. Judging solely on the basis of these cases, the organizational application—deception to create and exploit organizational inefficiencies and weaknesses in terrorist organizations—seems to have the greatest potential utility at the operational level and above.[97] The operational applications of deception, on the other hand—particularly deception to facilitate counter-terrorist operations—seem to have the greatest utility at the operational level and below. Furthermore, the cases suggest that the third application—deception to conceal capabilities and intentions—occurs most frequently in subordination to and support of the other applications.[98] These observations do not imply that each application of deception only works at certain levels, but rather that their effects seem to be best applied at certain levels.

Third, there is a great danger in seeing each opportunity for a counter-terrorist operation as a nail, and deception as a hammer. As Chapter V demonstrated, costs and risks may occasionally outweigh the benefits of deception. While deception creates opportunities where none previously existed, it invariably closes the doors to other options at the same time. The decision-makers who appoint and approve the use of deception, particularly deception against terrorists, should understand and weigh the potential costs and risks in relation to the benefits that deception promises.[99] That cost-benefit calculus

---

[97] The Filipino examples, however, demonstrate that the utility of this application in the hands of skilled deception practitioners is not limited to the strategic and operational levels.

[98] For example, the United States government should want its terrorist enemies to know that they will be hunted down and brought to justice for their actions. It should, however, conceal its plans for doing so, in order to achieve maximum effect with its counter-terrorist measures, be they deception, direct action, diplomatic initiatives, asset seizure, or any other host of options.

[99] The cost and risk analysis itself should address at least four questions. First, what is the risk and result of discovery? Second, what will the deception make the enemy do, and what happens

should invariably include consideration of the ethical and legal status of deception within the context of the situation.

Finally, deception has the potential to be very complex. Skillful deception thus requires knowledgeable execution. Some researchers have suggested that deception should be institutionalized, either by creating formal organizations to conduct it, or by designating a professional cadre whose expertise is deception. While recognizing both the logic behind and the potential value of these recommendations, the author of this thesis stops short of endorsing either. On the first point, professional institutions have a tendency over time to move away from a collective mindset that favors innovation toward a mindset that avoids risk. Yet, innovation is a key component of successful deception. Over time, a deception organization—like any organization—would have the tendency to succumb to the organizational propensity toward bureaucracy; consequently, the organization's effectiveness would have the potential to decline to the point that it would outlive its usefulness. As to the second point, an individual whose focus is solely deception will rarely have the access to decision-makers that he needs to be of real value. Often, he will only be summoned when those above him see no other way. What is needed, in contrast to these two courses of action, is a fundamental change in the way we think about deception. Those whose area of responsibility includes the potential for deception—political, diplomatic, and military decision-makers in particular—should adopt a mindset in which deception is always considered as one of many tools potentially available.

C. WHAT MIGHT FUTURE DECEPTION AGAINST TERRORISTS LOOK LIKE?

This study has paid considerable attention thus far to what cases of deception versus terrorists have looked like in the past. Little mention has been made, however, of what deception against terrorists might look like in the future.

---

if he doesn't do it? Third, what's going to be different with and without the deception? Finally, are you better off in the long run with or without deception?

In order to remedy this shortcoming, this section departs from the tone of the rest of the thesis and offers a number of very simple deception scenarios. For the sake of unity, each is portrayed as an operation against the same terrorist alleged to be behind the instance of terrorism that opened this thesis—Usama bin Laden (UBL). For the sake of convenience, all of the events described here are referred to in the present tense. While the tone of the paper clearly shifts to prosaic and speculative at this point, the underlying implications are serious and solid: deception is a counter-terrorist tool with tremendous potential.

1. Scenario #1—Create Inefficiency In The Organization

One way to reduce the efficiency of a clandestine organization is to target the group's operational security, or at least the group's confidence in its security. With this in mind, the US government undertakes the task of deceiving UBL about our having penetrated his communications networks, if not his inner circle itself (see Figure 23). That we have not in fact done so is a moot point. A carefully crafted series of messages is "slipped" to bin Laden's backers through previously trusted channels. This effort is augmented with press releases by various overt agencies and statements by high government officials. As a result, the deception successfully plants the doubt necessary to cause UBL to begin to believe that his organization has been compromised from within. Subsequently, one of UBL's lieutenants receives large unexplained deposits in his bank accounts; this fact too is "slipped" to UBL's backers, ultimately reaching UBL through channels he trusts. Unable to be certain whether it is a setup or not, bin Laden is forced to upgrade his operational security at considerable expense to his operational capacity by eliminating a previously trusted lieutenant. The net effect on those portions of the al Qa'ida network directly influenced by bin Laden is chaos and inefficiency; operations in progress are delayed by months, if not years, and the organization as a whole feels the adverse impact.

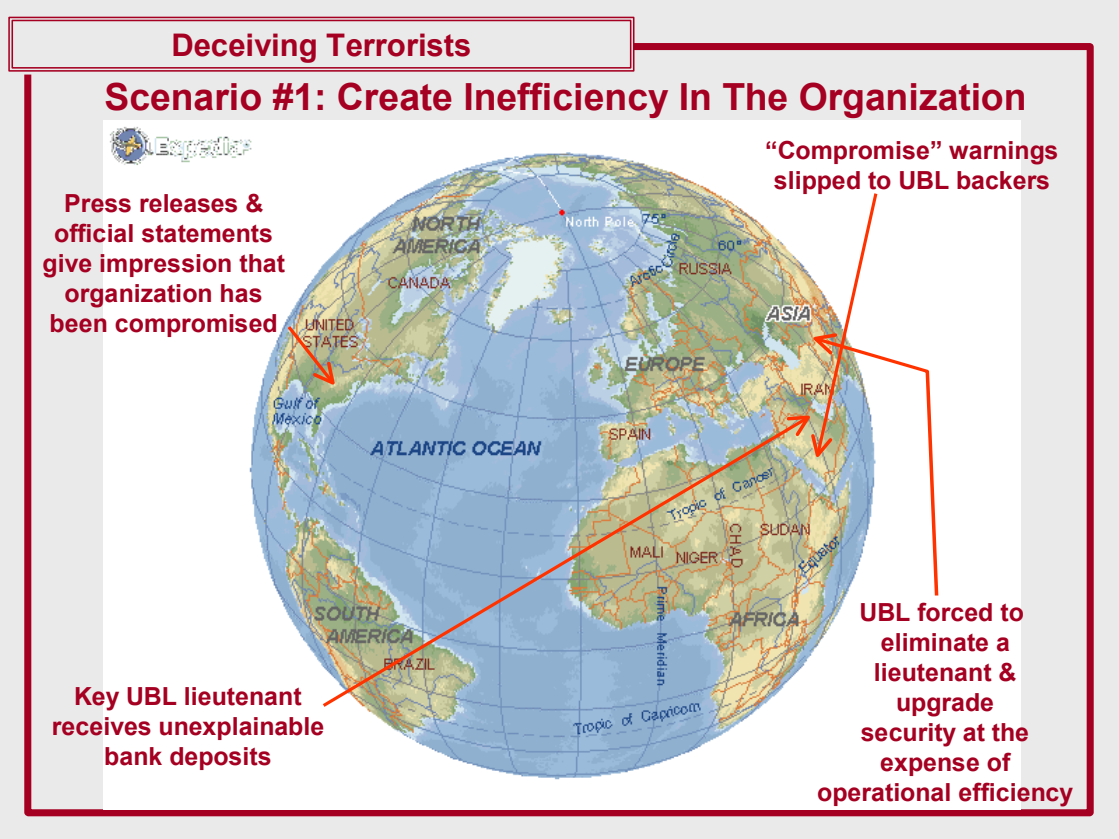


Figure 23. Organizational Approach Scenario

A concept like the one presented here may prove successful on more than point. First, it may cause an organization that practices good communications procedures to forego those procedures, even for a time, in the interest of increasing security. Second, it may prove useful for breaking the ties of a trust network. However, the risk of unintended consequences is always a possibility, even with successful deception. That danger is a significant possibility in this first scenario. Such a deception might cause a group like the one targeted here to respond not with chaos, but rather with innovation, ultimately making the organization much more difficult to target.

2. Scenario #2—Exploit Security Shortcomings

At about the same time, a US government agency discovers a number of the "channels" used by UBL's organization to pass encrypted information over the Internet. The US government implements a deception to convince UBL that

we have not penetrated this medium. In fact, a number of sources are used to convince UBL that we are focusing on the wrong media entirely—primarily satellite phones and wireless communications, in this case—in efforts to intercept his communications. The net effect is the purchase of time to exploit the resulting security flaws. For more than eight months, we are able to intercept a significant amount of UBL's message traffic to cells operating in Europe and the US.

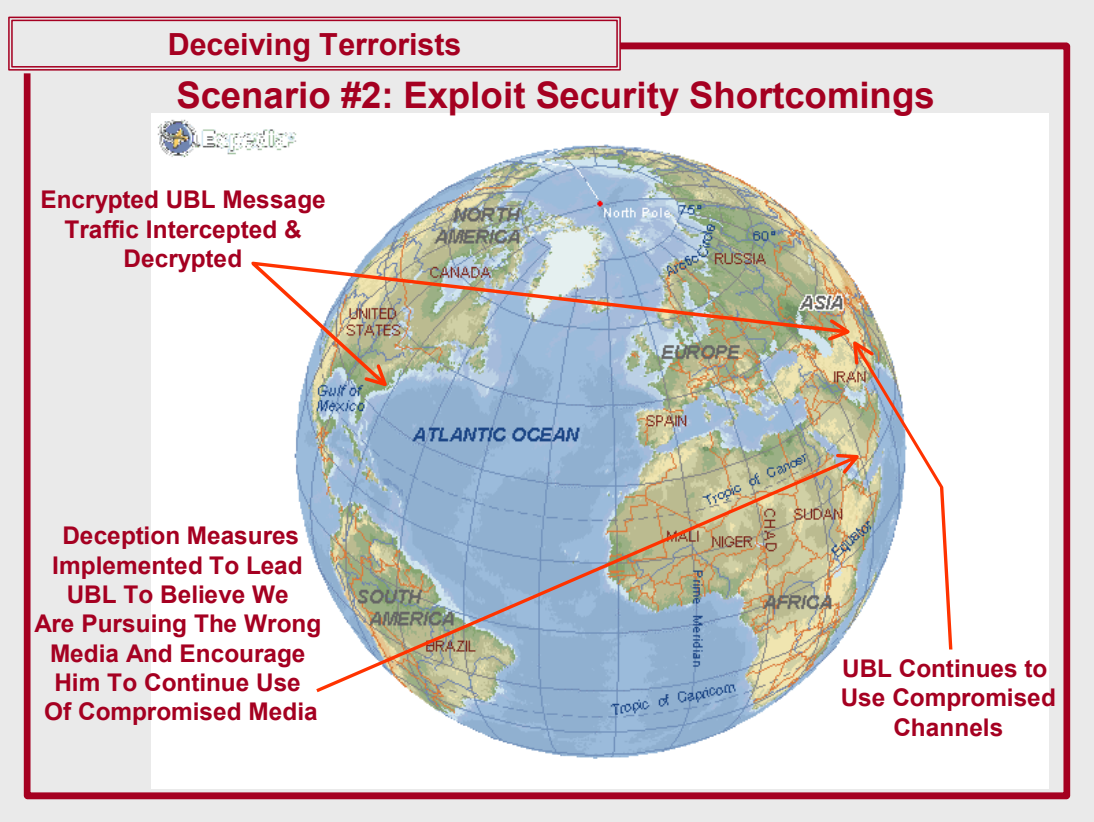


Figure 24. Exploitation Scenario

There is a long history of the use of deception to cover the exploitation of compromised communications channels and other security shortcomings. This was certainly the case with some of the deceptions carried out by the British Committee for Special Means during WW II, in which deception was one means used to concealing the fact that ULTRA allowed the Allies to "read" the Germans

"mail." A deception such as the one suggested here follows in much the same vein.

3. Scenario #3—The Lightning Rod

Through the source in Scenario #2, we learn that UBL wants to attack a US government facility in Asia. UBL's targeting of such a facility reflects the realities of an increasingly restrictive security environment in the US, Europe, the Middle East, and Africa. By various means, information is slowly but surely leaked to UBL that indicates that a specific facility in Indonesia meets his targeting needs. The net effect is a baited ambush. Within a few weeks, Indonesian government forces apprehend a group of UBL's "soldiers" as they prepare to carry out their mission. The fact that American agents and special mission units support the bust is well concealed; in the following days and weeks, all indications and reports to and through the media are painted to look as if the bust was a lucky break for the Indonesian government.

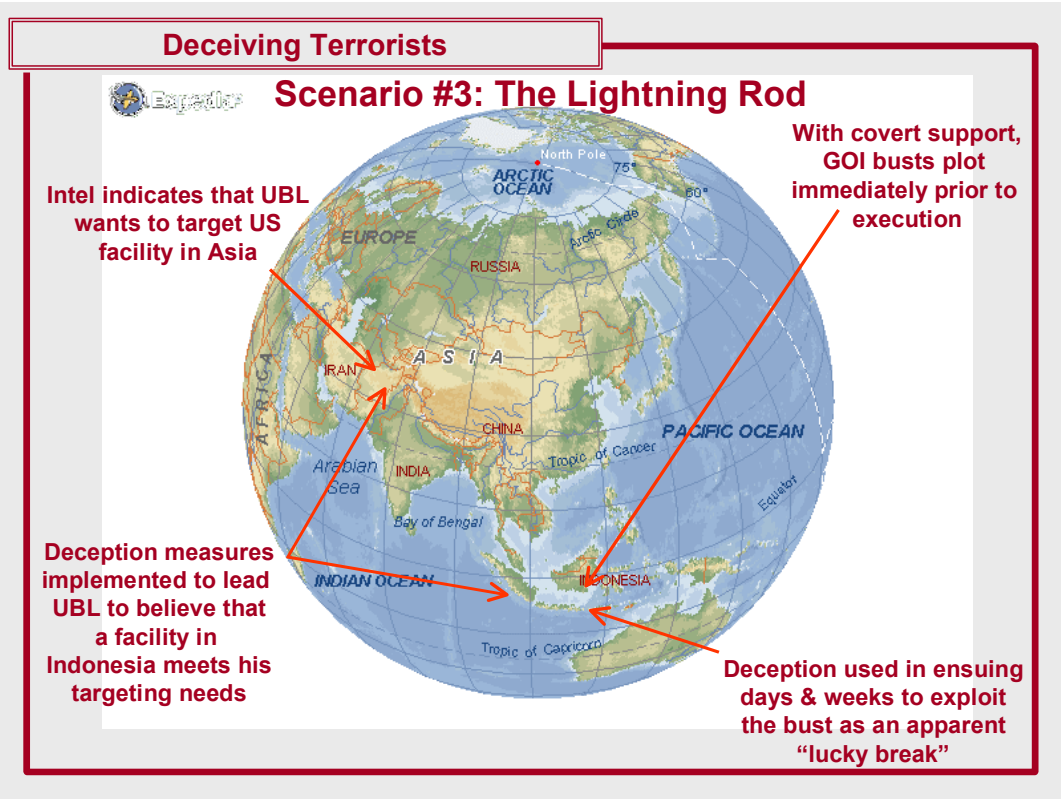


Figure 25. Lightning Rod Scenario

Deceptions such as the one suggested by scenario 3 tend to be risky undertakings. Inviting attack when it can also be discouraged is a dangerous game in which the deceiver assumes the ability to outmaneuver the target of the deception. The concept of unintended consequences, however, suggests that such a deception might not only inspire the target to undertake the desired operation, but may cause him to do so in ways that the deceiver had unanticipated. The opportunity of a critical interception of a terrorist organization "in the act" must, in this case, be weighed against the probability and consequences not of failing at the deception, but of failing at the operation the deception was intended to facilitate.

4. Scenario #4—Deception As A Stand-Alone

US intelligence sources discover that UBL is planning to take delivery of nuclear materials from "entrepreneurs" in a breakaway state of the former Soviet Union (see Figure 26). Sensitive political concerns—not to mention the risk of exposing key intelligence methods and sources—make a direct preemptive strike extremely risky, although UBL and his business associates do not know it. To the contrary, the US government makes it clear through multiple channels that an American special operations task force is prepared to interdict the transaction. Sympathizers in the intelligence service of a neighboring state send urgent messages to UBL through his backers that a robust force is indeed on the ground, and ready to undertake long-range interdiction operations. Although he does not entirely believe that the Americans could reach out to interdict the transaction, UBL is nonetheless impelled to cancel the buy.

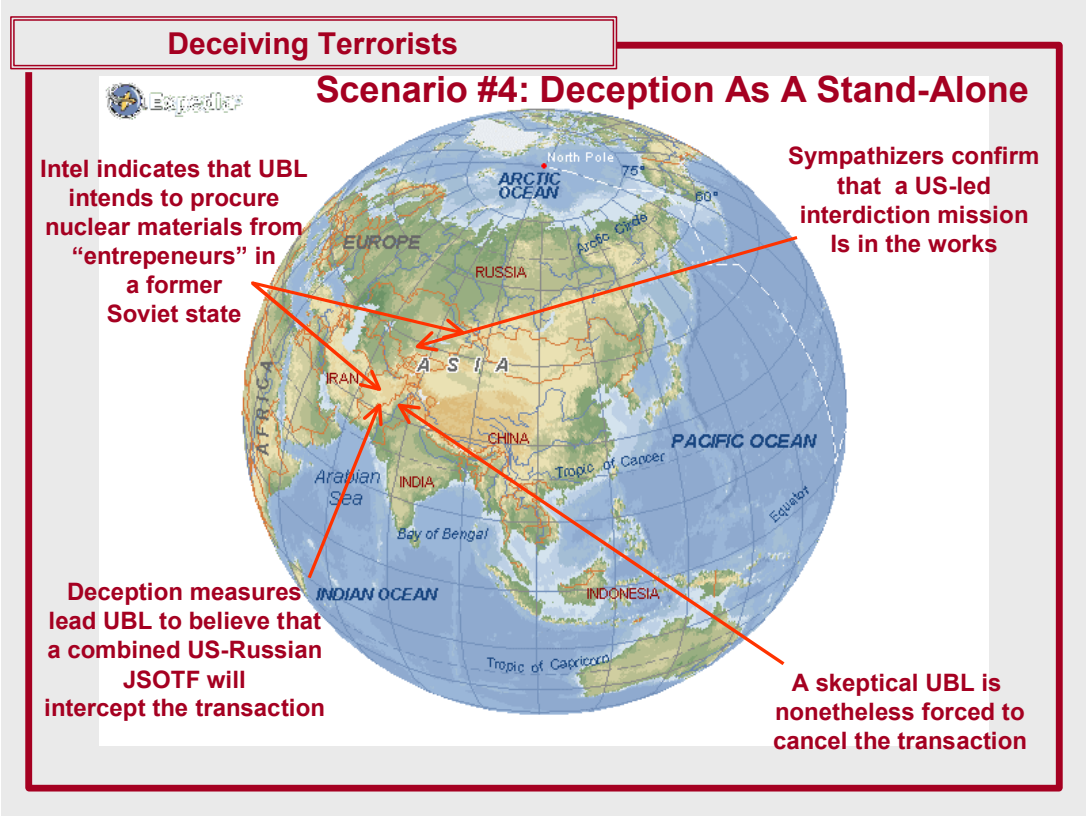


Figure 26. Stand-Alone Scenario

Given bin Laden's propensity and stated willingness to use weapons of mass destruction against his perceived enemies, there are few—if, indeed, any—political concerns that would prevent the United States and its allies from actually targeting a transaction like the one proposed here. That is not the point of the scenario, however. What is relevant is that on occasion, deception has the ability—if carefully crafted and skillfully execute—to serve as a stand-alone course of action. The opportunities for such deceptions are rare, but they do exist.

5. Scenario #5—Going Hunting

Finally, the US and its allies spun a new deception story—that we are about to seize UBL in Afghanistan. Again, does not know that the Commander in Chief of US Central Command has no desire to conduct an operation to root bin Laden from a cave complex, but the point is a minor one. At a minimum, we

expect to cause inefficiency as UBL is again forced to sacrifice operational capacity to guarantee his security; at a maximum, however, we expect to convince him to give up his current security environment, flushing him into the open where he can be hit. In fact, the latter occurs. On Christmas Day, a Ranger company intentionally conducts a full-blown deception raid on a "dry hole" used very recently by UBL. Convinced that the US is only a step behind, UBL is convinced to flee the country. As he flees, a waiting special operations task force intercepts him in the open rather than in one of his well-prepared and heavily defended cave complexes. The fight is short and intense, but bin Laden is killed in the end.

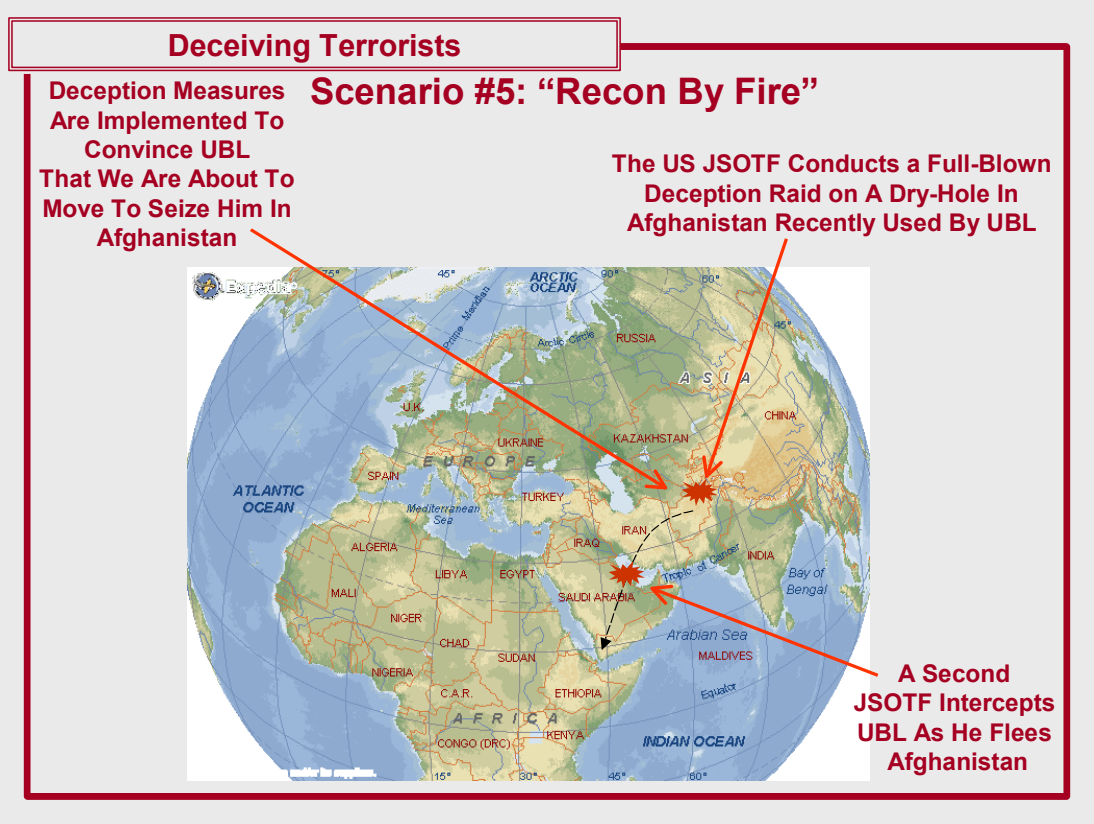


Figure 27. Final Scenario

On a practical note, such a deception seems implausible. After all, the series of events that culminated with the events of 11 September justify going after terrorists like bin Laden at almost any cost. What those actions do not

justify, however, is recklessness—employing special operations troops in situations where relative superiority cannot be either gained or sustained. A special mission unit like Delta is expected to take risks and assume casualties; a few men lost in an extremely important mission, however tragic their loss may be, can ultimately be replaced. An entire Delta squadron, on the other hand, cannot be easily replaced. Deception is a proven means of helping such units gain relative superiority, thus ensuring the accomplishment of missions and objectives so critical to the nation's interests.

Although somewhat whimsical, these scenarios suggest the value of deception against terrorists; in this context, it is easy to see the potential of deception as a counter-terrorist tool.

D. AREAS FOR FURTHER RESEARCH

As one of the first forays into the field of deceiving terrorists, this thesis merely opens the door to the subject. In so doing, however, it exposes a number of related subjects that require further study.

1. Terrorist Use Of Deception

Most notably, the research for this thesis turned up a very large number of examples of terrorist deception against states. Deception, necessitated by the desire to survive, is a key component of terrorist tradecraft. As the United States' war on terrorism continues, this is a subject that demands serious, immediate attention.

2. Analysis Of Classified Cases Of Deception Against Terrorists

Furthermore, the cases used as illustrative examples in this thesis are all open-source cases. Presumably, other cases exist, hidden behind the veil of secrecy mentioned first in Chapter III. One area for further research is thus a detailed study of the classified cases of deception against terrorists and other non-state actors. Such a study is necessary, ultimately, to cast the conclusions of this report in their proper perspective.

3. Empirical Analysis Of Deception Versus Terrorists

Next, two of the most useful references in preparing this work were Barton Whaley's Stratagem and John Van Vleet's Tactical Military Deception. Each work is notable for the detailed, empirical analytic approach to the subject of military deception, as well as the conclusions that can be drawn from such an approach. As the body of literature on deception versus terrorists expands, this same analysis is necessary for this "new" area of deception.

4. Legal and Ethical Status Of Deception Against Terrorists

Additionally, while this study broached the subject of the costs and risks of deception, much more detailed analysis of these closely related areas is necessary. Currently, deception against terrorists is "undiscovered country." The decision-makers and leaders who will lead the expedition into this undiscovered country need and deserve sound guidelines on which to base their decision and actions. A detailed comparison of the costs and risks of deceiving terrorists on both a strategic and tactical level is thus necessary in order to determine whether certain deceptions carry higher costs and risks than others. Also, more research is needed into the legal and ethical status of efforts to deceive terrorists, in order to produce better guidelines for decision-makers.

5. Psychological Approach

Finally, in order to guide those who will conduct deception against terrorists, more research is needed to suggest the role that psychology plays in deception. Since there is no universal psychological profile for terrorists, some other means of predicting the vulnerabilities and reactions of terrorists to deception is necessary. One possible starting place for that research is in the area of influence psychology—the study of how we all are affected by what amount to universal influence principles, such as reciprocity, commitment and consistency, liking, and others. Terrorists are, after all, human, and are—within reason—predictably subject to the same psychological principles as everybody else.

E. PAST, PRESENT, AND FUTURE

If there is anything that the historical record suggests to us, it is that terrorism is and will be a long-enduring phenomenon. The Zealots Sicarii, for example, raged first against the Greek population of Judea and then their Roman governors for more than a quarter of a century (Rappoport, 1984, pp. 658-669). The original Thugs terrorized India for more than six centuries; their modern counterparts, in turn, for more than three.[100] The Assassins terrorized the Muslim world for more than two hundred years, bent on purifying the Islamic faith.[101] In our own century, Abu Nidal gained and held the world's attention for more than a decade (Seale, 1992). Most recently, Usama bin Laden and al Qa'ida have commanded a position on the world stage for a time.

History shows us that bin Laden, like his predecessors, will someday fade away—another name in a history book. Yet, there will be others. Even now, a young man living on the West Bank, or in Chechnya, Afghanistan, or Indonesia is walking the long path that will someday lead him from troubled youth to terrorist superstar. Like those who came before him, he will need to be dealt with.

This thesis opened with the premise that an innovative tool was required for the new war that America finds itself in. At the end of 2001, even with the Taliban regime broken and the future of Usama bin Laden's al Qa'ida network uncertain, that requirement still exists. Deception, history suggests, may be that tool.

---

[100] The best single-source document summarizing the history of the Assassins, the Thugs, and the Zealots-Sicarii is David Rappoport's Terrorism in Three Religious Traditions (1984, pp. 658-677).

[101] The Assassins were also known as the Ismailis-Nizari (Rappoport, 1984, p. 664).

LIST OF REFERENCES

Arquilla, J. (1993). Louder Than Words: Tacit Communications In International Crises (Reprinted from Political Communication, 9, 155-172). Santa Monica, CA: RAND.

Arquilla, J. & Ronfeldt, D. (2000). Swarming & The Future Of Conflict. Santa Monica, CA: RAND.

Arquilla, J. & Ronfeldt, D. (Eds.) (2001). Networks And Netwars: The Future Of Terror, Crime, And Militancy. Santa Monica, CA: RAND.

Axelrod, R. (1979). The Rational Timing of Surprise. World Politics, 31, 228-246.

Bacon, D.J. (1998). Second World War Deception: Lessons Learned For Today's Joint Planner. Maxwell AFB, AL: Air Command & Staff College.

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. Portland, OR: Frank Cass Publishers.

Bell, J.B. (1999). Dragonwars: Armed Struggle And The Conventions Of Modern War. New Brunswick, NJ: Transaction Publishers.

Bok, S. (1999). Lying: Moral Choice In Public And Private Life. New York: Vintage Books.

Bowden, M. (2001). Killing Pablo: The Hunt For The World's Greatest Outlaw. New York: Atlantic Monthly Press.

Bowlin, M. (1999). British Intelligence And The IRA: The Secret War In Northern Ireland, 1969-1988. Monterey, CA: Naval Postgraduate School.

Breuer, W.B. (1993). Hoodwinking Hitler: The Normandy Deception. Westport, CT: Praeger Press.

Bruton, J.K., Jr. (1978). Counterinsurgency In Rhodesia (Report Posted on the Selous Scouts Web Site]. Retrieved 18 October 2001 from the World Wide Web: http://members.tripod.com/selousscouts/counterinsurgency_in_rhodesia.htm.

Carr, C. (Ed.). (2000). The Book of War. New York: Random House.

Clarridge, D.R. (1997). A Spy For All Seasons: My Life In The CIA. New York: Scribner.

CNN. (2001, December 2). Terror Attacks Kill At Least 28 In Israel (Article On The Web Site CNN.com). Retrieved December 2, 2001 from the World Wide Web: http://www.cnn.com/2001/WORLD/meast/12/02/mideast/index.html.

Daniel, D.C., & Herbig, K.L. (Eds.). (1982). Strategic Military Deception. Elmsford, NY: Pergamon Press.

Deutsch, H.C. (Ed.). (1989). Covert Warfare: Basic Deception And The Normandy Invasion. New York: Garland Publishing.

Dillon, M. (1990). The Dirty War. London: Arrow.

Dozer, T.A.L. (2001). Selous Scouts Web Site. Retrieved 18 October 2001 from the World Wide Web: http://members.tripod.com/selousscouts.

Dunigan, J. F., & Nofi, A.A. (1995). Victory And Deceit: Dirty Tricks At War. New York: William Morrow And Company, Inc.

Epstein, E.J. (1989). Deception: The Invisible War Between The KGB And The CIA. New York: Simon & Schuster.

Field Manual 90-2: Battlefield Deception. (1988). Washington, DC: US Army.

Galbraith, J. (1995). Designing Organizations: An Executive Briefing On Strategy, Structure, And Process. San Francisco, CA: Jossey-Bass, Inc.

Garreau, J. (2001, September 17). Disconnect The Dots: Maybe We Can't Cut Off Terror's Head, But We Can Take Out Its Nodes. Washington Post, p. C01. Retrieved September 18, 2001 from the World Wide Web: http://www.washingtonpost.com/wp-dyn/articles/A41015-2001Sep16.html.

Gerlach, L.P. (2001). The Structure Of Social Movements: Environmental Activism And Its Opponents. In J. Arquilla & D. Ronfeldt (Eds.) Networks And Netwars: The Future Of Terror, Crime, And Militancy (pp. 289-310), Santa Monica, CA: RAND.

Godson, R., & Wirtz, J.J. (2000). Strategic Denial And Deception. International Journal of Intelligence and Counterintelligence, 13, 424-437.

Handel, M. (1982). Intelligence and Deception. In A. Perlmutter & J. Gooch (Eds.), Military Deception And Strategic Surprise (pp. 122-154), London: Frank Cass & Co. Ltd.

Hatton, J.L. (1998). We Deceive Ourselves: The Role Of Preconception In Operational Deception [Article Posted On The Website Of The National Defense University Institute For National Strategic Studies]. Retrieved January 11, 2001 from the World Wide Web: http://www.ndu.edu/inss/books/essaysch2.html.

Herbig, K.L., & Daniel, D.C. (1981). Battle Of Wits: Synthesizing And Extrapolating From NPS Research On Strategic Military Deception. Monterey, CA: Naval Postgraduate School.

Herbig, K.L., & Daniel, D.C. (1980). Multidisciplinary Perspectives On Military Deception. Monterey, CA: Naval Postgraduate School.

Hesketh, R. F. (1949). Excerpt From Fortitude: A History Of Strategic Deception In North Western Europe, April 1943 To May 1945. In D. Daniel & K. Herbig (Eds.), Strategic Military Deception (pp. 233-242). Elmsford, NY: Pergamon Press.

Heuer, R. J., Jr. (1982). Cognitive Factors In Deception And Counterdeception. In D. Daniel & K. Herbig (Eds.), Strategic Military Deception (pp. 31-69). Elmsford, NY: Pergamon Press.

Hoffman, B. (1985). Commando Raids: 1946-1983. Santa Monica, CA: RAND.

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

Jervis, R. (1976). Hypotheses On Misperception. World Politics, 20, 454-479.

Joint Publication 3-58: Joint Doctrine For Military Deception. (1996). Washington, DC: Government Printing Office.

Kidder, R.M. (1996). How Good People Make Tough Choices: Resolving The Dilemmas Of Ethical Living. New York: Fireside.

Krause, L.B. (1996). Insurgent Intelligence: The Guerrilla Grapevine. International Journal Of Intelligence And Counterintelligence, 9, 291-311.

Lansdale, E.G. (1991). In The Midst Of Wars (2nd Ed.). New York: Fordham University Press.

Leites, N., & Wolf, C., Jr. (1970). Rebellion And Authority: An Analytic Essay On Insurgent Conflicts. Santa Monica, CA: RAND.

Lesser, I. (2000). Countering The New Terrorism. Santa Monica, CA: RAND.

Lettieri, T.A. (2000). Pseudo-Terrorist Operations [From the Selous Scouts Web Site]. Retrieved 18 October 2001 from the World Wide Web: http://members.tripod.com/selousscouts/pseudo_main.htm.

Mahan, A.T. (1987). The Influence Of Sea Power Upon History, 1660-1783 ("An Unabridged, Slightly Altered Republication Of The Fifth Edition [1894] Of The Work Originally Published By Little, Brown, And Company, Boston, In 1890"). Mineola, NY: Dover Publications, Inc.

McCormick, G.H. & Owen, G. (2000). Security And Coordination In A Clandestine Organization. Mathematical and Computer Modeling, 31, 175-192.

McKnight, G. (1974). The Terrorist Mind. New York: Bobbs-Merrill Company, Inc.

McRaven, W.H. (1995). Spec Ops: Case Studies In Special Operations Warfare Theory And Practice. Novato, CA: Presidio Press

Meyer, J.M. & Bill, B.J. (Eds.) (2001). Operational Law Handbook, 2002. Charlottesville, VA: The Judge Advocate General's School.

Mickolus, E.F. (1980). Transnational Terrorism: A Chronology Of Events, 1968-1979. London: Aldwych Press Limited.

Mickolus, E.F. & Simmons, E.F. (1997). Terrorism, 1992-1995: A Chronology Of Events And A Selectively Annotated Bibliography. Westport, CT: Greenwood Press.

Montagu, E. (1996). The Man Who Never Was. Oxford: Oxford University Press.

Moose, P.H. (1982). A Systems View Of Deception. In D. Daniel & K. Herbig (Eds.), Strategic Military Deception (pp. 136-150). Elmsford, NY: Pergamon Press.

Patterns Of Global Terrorism: 1999. (2000, April). From the Department of State, Office of the Secretary of State, Office of the Coordinator for Counterterrorism. Retrieved November 29, 2001 from the World Wide Web: http://www.state.gov/www/global/terrorism/1999report/intro.html.

Perlmutter, A. & Gooch, J. (Eds.). (1982). Military Deception And Strategic Surprise. London: Frank Cass & Co. Ltd.

Protocol I, Additional To The Geneva Conventions Of 12 August 1949, Relating To The Protection Of Victims Of International Armed Conflicts (1977, June 8). Posted on the Society of Professional Journalists' Web Site. Retrieved 13 December 2001 from the World Wide Web: http://www.the-spa.com/genevaconventions/protocol1.html.

Rappoport, D. (1984, September). Fear And Trembling: Terrorism In Three Religious Traditions. The American Political Science Review, 78, 658-677.

Reese, W. (1982). Deception Within A Communications Theory Framework. In D. Daniel & K. Herbig (Eds.), Strategic Military Deception (pp. 99-114). Elmsford, NY: Pergamon Press.

Ronfeldt, D. & Arquilla, J. (2001). What Next For Networks And Netwars? In J. Arquilla & D. Ronfeldt (Eds.) Networks And Netwars: The Future Of Terror, Crime, And Militancy (pp. 311-361), Santa Monica, CA: RAND.

Saxe, J.G. (1963). The Blind Men and the Elephant: John Godfrey Saxe's Version of the Famous Indian Legend, [Excerpt from the Web Site Noogenesis.Com]. New York: Whittlesey House. Retrieved October 29, 2001, from the World Wide Web: http://www.noogenesis.com/pineapple/blind_men_elephant.html.

Schultz, R.H. (1999). The Secret War Against Hanoi: Kennedy's And Johnson's Use Of Spies, Saboteurs, And Covert Warriors. New York: Harper Collins.

Seale, P. (1992). Abu Nidal: A Gun For Hire. New York: Random House.

Sheldon, R.M. (1997). The Ancient Imperative: Clandestine Operations and Covert Action. International Journal of Intelligence and Counterintelligence, 10, 299-315.

Sherwin, R.G. (1982). The Organizational Approach To Strategic Deception: Implications For Theory And Policy. In D. Daniel & K. Herbig (Eds.), Strategic Military Deception (pp. 70-98). Elmsford, NY: Pergamon Press.

Sherwin, R.G., & Whaley, B. (1982). Understanding Strategic Deception: An Analysis Of 93 Cases. In D. Daniel & K. Herbig (Eds.), Strategic Military Deception (pp. 177-194). Elmsford, NY: Pergamon Press.

Stanley, Z. (1985). An Annotated Bibliography Of The Open Literature On Deception. Santa Monica, CA: RAND Corporation.

Thompson, L. (1988). Dirty Wars: Elite Forces Vs. The Guerrillas [Excerpts posted on the Selous Scouts Web Site]. Retrieved 18 October 2001 from the World Wide Web: http://members.tripod.com/selousscouts/unconventional.htm.

Tugwell, M. (Ed.)(1990). Deception Operations: Studies In The East-West Context. London: Brasseys (UK).

Tugwell, M. (1990). Eastern Approaches. In M. Tugwell (Ed.), Deception Operations: Studies In The East-West Context (pp. 11-24), London: Brasseys (UK).

Valenta, J. (1982). Soviet Use Of Surprise & Deception. Survival, 54-55.

Valeriano, N.D. & Bohannan, C.T.R. (1962). Counter-Guerrilla Operations: The Philippine Experience. Westport, CT: Praeger.

Van Creveld, M. (1985). Command in War. Cambridge, MA: Harvard University Press.

Van Vleet, J.A. (1985). Tactical Military Deception. Monterey, CA: Naval Postgraduate School.

Whaley, B. (1982). Toward A General Theory Of Deception. In A. Perlmutter & J. Gooch (Eds.), Military Deception And Strategic Surprise (pp. 178-192), London: Frank Cass & Co. Ltd.

Whaley, B. (1969). Stratagem: Deception And Surprise In War. Cambridge, MA: MIT Center For International Studies.

Williams, P. (2001). Transnational Criminal Networks. In J. Arquilla & D. Ronfeldt (Eds.) Networks And Netwars: The Future Of Terror, Crime, And Militancy (pp. 61-97), Santa Monica, CA: RAND.

Zanini, M. & Edwards. S.J.A. (2001). The Networking Of Terror In The Information Age. In J. Arquilla & D. Ronfeldt (Eds.) Networks And Netwars: The Future Of Terror, Crime, And Militancy (pp. 29-60), Santa Monica, CA: RAND.

Zernike, K. & Van Natta, D. (2001, November 4). Hijacker's Meticulous Strategy Of Brains, Muscle And Practice. New York Times. [Article Posted On The Web Site New York Times.Com]. Retrieved 2 December 2001 from the World Wide Web.

BIBLIOGRAPHY

Adams, J. (1998). The Next World War. New York: Simon & Schuster.

Black, I. & Morris, B. (1991). Israel's Secret Wars: A History Of Israel's Intelligence Services. New York: Grove Weidenfeld.

Broad, W.J. (1992). Teller's War: The Top-Secret Story Behind The Star Wars Deception. New York: Simon & Schuster.

CALL Newsletter No. 3-88: Deception. (1988). Fort Leavenworth, KS: Center For Army Lessons Learned.

Cialdini, R. B. (1993). Influence: The Psychology Of Persuasion. New York: William Morrow And Company.

Cialdini, R.B., Wosinska, W., Barrett, D.W., Butner, J., & Gornik-Durose, M. (1999, October). Compliance With A Request In Two Cultures: The Differential Influence Of Social Proof And Commitment/Consistency On Collectivists And Individualists. Personality And Social Psychology Bulletin, 25, 1242-1253.

Clayton, A. (1976). Counter-Insurgency In Kenya. Nairobi, Kenya: Transafrica Publishers.

Coogan, T.P. (1996). The Troubles: Ireland's Ordeal 1966-1996 And The Search For Peace. Boulder, CO: Roberts Rinehart Publishers.

Crenshaw, M. (1981, July). The Causes of Terrorism. Comparative Politics, 379-399.

Crenshaw, M. (1985) Theories Of Terrorism: Instrumental And Organizational Approaches. In D.C. Rappoport (Ed.), Inside Terrorist Organizations (pp. 13-31). London: Frank Cass & Co. Ltd.

Crenshaw, M. (2000). The Psychology Of Terrorism: An Agenda For The Twenty-First Century. Political Psychology, 21, 405-420.

Cullather, N. (1999). Secret History: The CIA's Classified Account Of Its Operations In Guatemala, 1952-1954. Stanford, CA: Stanford University Press.

Della Porta, D. (1992). Introduction: On Individual Motivations In Underground Political Organizations. International Social Movement Research, 4, 3-28.

Foot, M.R.D. (1984). SOE: An Outline History Of The Special Operations Executive, 1940-46. London: British Broadcasting Corporation.

Gray, C.H. (1997). Postmodern War: The New Politics Of Conflict. New York: The Guilford Press.

Hart, B.H.L. (1968). Strategy (2nd Revised Edition). New York: Frederick A. Praeger, Publishers.

Hoffman, B., Taw, J.M., & Arnold, D. (1981). Lessons For Contemporary Insurgencies: The Rhodesian Experience. Santa Monica, CA: RAND Arroyo Center.

Hosmer, S.T. (1996). Psychological Effects Of US Air Operations In Four Wars: 1941-1991. Santa Monica, CA: RAND.

Howard, M. (1990). British Intelligence In The Second World War, Volume 5: Strategic Deception. New York: Cambridge University Press.

Hulnick, A.S. (1997). Intelligence And Law Enforcement: The "Spies Are Not Cops" Problem. International Journal of Intelligence and Counterintelligence, 10, 269-286.

Ionov, (1971). On Methods Of Influencing An Opponent's Decision (Translated From The Russian). Moscow.

Jervis, R. (1976). Perception And Misperception In International Politics. Princeton, NJ: Princeton University Press.

Kahneman, D., Slovic, P. & Tversky, A. (Eds.) (1982). Judgment Under Uncertainty. New York: Cambridge University Press.

Kitson, F. (1971). Low Intensity Operations: Subversion, Insurgency, Peace-Keeping. Harrisburg, PA: Stackpole Books.

Kronman, M. (1978). Interim Note Number T-11: The Deceptive Practices Of The 23rd Headquarters, Special Troops During World War II. Aberdeen Proving Grounds, MD: Tactical Operations Analysis Office.

Lambeth, B.S. & Lewis, K.N. (1988). The Strategic Defense Initiative In Soviet Planning And Policy. Santa Monica, CA: RAND.

Lloyd, M. (1997). The Art Of Military Deception. London: Leo Cooper.

Masterman, J.C. (2000). The Double-Cross System. New York: The Lyons Press.

Mattox, J.M. (2000). The Moral Status Of Military Deception [A paper for the 2000 Joint Services Conference on Professional Ethics]. Retrieved February 27, 2001 from the World Wide Web: http://www.usafa.af.mil/jscope/JSCOPE00/mattox00.html

Metz, S. (1995, February 28). Counterinsurgency: Strategy And The Phoenix Of American Capability. Carlisle Barracks, PA: US Army War College.

Mickolus, E.F., Sandler, T., & Murdock, J.M. (1989). International Terrorism In The 1980's: A Chronology Of Events, Volume I: 1980-1983. Ames, IA: Iowa State University Press.

Mickolus, E.F., Sandler, T., & Murdock, J.M. (1989). International Terrorism In The 1980's: A Chronology Of Events, Volume II: 1984-1987. Ames, IA: Iowa State University Press.

Mickolus, E.F. (1993). Terrorism, 1988-1991: A Chronology Of Events And A Selectively Annotated Bibliography. Westport, CT: Greenwood Press.

Mihalka, M. (1980). German Strategic Deception in the 1930's. Santa Monica, CA: RAND

Nacos, B.L. (1994). Terrorism And The Media. New York: Columbia University Press.

Neustadt, R.E. & May, Ernest, R. (1986). Thinking In Time. New York: The Free Press.

Pustay, J.S. (1965). Counterinsurgency Warfare. New York: The Free Press.

Radvanyi, J. (Ed.). (1990). Psychological Operations And Political Warfare In Long-Term Strategic Planning. New York: Praeger Publishers.

Reich, W. (1998). Origins Of Terrorism: Psychologies, Ideologies, Theologies, States Of Mind. Washington, DC: Woodrow Wilson Center Press.

Rhoads, K. (2000). An Introduction To Social Influence [Article posted on the Web site Influence At Work]. Retrieved May 22, 2001 from the World Wide Web: http://www.influenceatwork.com.

Romerstein, H. (1990). Soviet Active Measures and Propaganda: "New Thinking" and Influence Activities In The Gorbachev Era. In J. Radvanyi

(Ed.), Psychological Operations And Political Warfare In Long-Term Strategic Planning (pp. 36-68). New York: Praeger Publishers.

Schelling, T.C. (1960). The Strategy Of Conflict. London: Oxford University Press.

Schultz, R.H. & Godson, R. (1984). Dezinformatsia: Active Measures In Soviet Strategy. Elmsford, NY: Pergamon Press, Inc.

Star Wars: Delusions and Dangers. (1985). Moscow, USSR: Military Publishing House.

Stata, R. (1994). Basic Definitions [Article posted on the Web site vix.com]. Retrieved June 11, 2001 from the World Wide Web: http://www.vix.com/objectivism/Writing/RaymieStata/indism/subsection3_1_1.html.

Steefel, L. (1962). Bismarck, The Hohenzollern Candidacy, And The Origins Of The Franco-German War Of 1870. Cambridge, MA: Harvard University Press.

The Quest Study Bible, New International Version. (1994). Grand Rapids, MI: Zondervan Publishing House.

Triandis, H.C., Bontempo, R., Villareal, M.J., Asai, M., & Lucca, N. (1988). Individualism And Collectivism: Cross-Cultural Perspectives On Self-Ingroup Relationships. Journal Of Personality And Social Psychology, 54, 323-338.

Van Creveld, M. (1991). The Transformation Of War. New York: The Free Press.

Wheatley, Dennis. The Deception Planners: My Secret War, 1980.

Wood, J.R.T. (1995). Rhodesian Insurgency [Essay posted on the Selous Scouts Web Site]. Retrieved 18 October 2001 from the World Wide Web: http://members.tripod.com/sleousscouts/rhodesian_insurgency_2.htm.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. MR Andrew Marshall
   Director, Net Assessment
   The Pentagon, Room 3A930
   Alexandria, VA

4. Carol Dumaine
   Director, Global Futures Partnership
   Central Intelligence Agency
   Alexandria, VA

5. Winston Wiley
   Deputy Director, Intelligence
   Central Intelligence Agency
   Alexandria, VA

6. Deputy Chief of Staff for Operations, US Army
   ATTN: MAJ Scott Taylor
   The Pentagon
   Alexandria, VA

7. Superintendent
   ATTN: Professor Gordon McCormick
   Special Operations Academic Group
   Monterey, CA

8. Jennifer Duncan
   Special Operations Academic Group
   Monterey, CA