WARNING OF TERROR:

EXPLAINING THE FAILURE OF INTELLIGENCE AGAINST TERRORISM

Master of Arts in Law and Diplomacy Thesis

Submitted by Erik J. Dahl

January 2004

Under the advisement of Professor Richard H. Shultz

http://fletcher.tufts.edu

THE FLETCHER SCHOOL

ABSTRACT

Many scholars have studied intelligence failure and developed theories to explain disasters such as the attack on Pearl Harbor. Others have examined the rising threat of terrorism, and see it as posing a particularly difficult challenge for the intelligence community. But little work has been done to integrate the earlier literature on intelligence failure with the newer threat of terrorist attack. This thesis attempts to answer the question: How well do traditional theories of intelligence failure and strategic surprise account for the inability of the intelligence community to warn of terrorist attacks?

Three schools of thought can be found in the literatures on intelligence and on terrorism, and for each school several hypotheses will be developed and tested against a particular case study: the bombing of the U.S. Marine Barracks in Lebanon in 1983. While the Beirut bombing does appear to confirm several of these hypotheses, none of these schools of thought will be shown to satisfactorily explain the limitations of the intelligence community in the fight against terrorism. While the factors that produce surprise in terrorist attacks are familiar, the nature of that surprise, and the effects created, can be very different.

Instead, an alternative approach toward the study of intelligence failure will be briefly introduced. This is what sociologist Charles Perrow has called *normal accident theory*. Accident theory suggests that while traditional theories of intelligence may be sufficient to explain the *causes* of intelligence failure, the *inevitability* of that failure may arise from the complex nature of the intelligence system. In addition, normal accident theory suggests that much of the literature on intelligence failure, which focuses on the problems caused by human perception and cognition, may be misguided and even counterproductive.

TABLE OF CONTENTS

1. Introduction

The study of intelligence failure has been popular among academics and intelligence analysts since well before the attacks of September 11, 2001. Beginning with Roberta Wohlstetter's classic book on Pearl Harbor, scholars have attempted to determine how it can be possible that the most capable intelligence system in the world appears to be frequently taken by surprise.[1] In the 1980s a literature grew around the subject of strategic surprise, as scholars such as Richard Betts and Michael Handel developed theories to explain not only Pearl Harbor, but also other disasters such as the American intelligence failures in Korea and the Israeli surprise in the 1973 Yom Kippur war. The end of the Cold War and the opening of archives on both sides of the iron curtain resulted in a burgeoning literature on intelligence in general. But the concern among academics about strategic surprise and surprise attack waned, with most scholars concluding that in the difficult job of intelligence warning, failure was inevitable.

In addition, a largely separate literature grew in the 1980s and 1990s concerning the rising threat of terrorism. Although some of this work examined the difficulty that terrorism presented for the intelligence community, there was relatively little integration between the scholars studying strategic surprise and those studying the terrorist threat. After the 9/11 attacks, of course, the problem of the intelligence failure quickly became a national concern, and the official U.S. government commission continues today to study where blame may lie for the failure of intelligence and law enforcement agencies in that disaster.

But for understandable reasons, most of the work on intelligence failure sparked by the 2001 terror attacks has focused on operational matters, such as seeking to identify specific indicators that were missed. While 9/11 has been frequently compared with Pearl Harbor, there

[1] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

has been little work done to examine how the earlier literature on intelligence failure might help us understand the problems of today. This thesis represents a preliminary attempt at such an examination, and will seek to answer the question: How well do traditional theories of intelligence failure and strategic surprise account for the inability of the intelligence community to warn of terrorist attacks?

I will begin in section two by examining the relevant literatures on intelligence failure (in particular the subset of strategic surprise), and on terrorism and intelligence. I will show that in these writings we can find three general schools of thought:

- The *traditional view*, which holds that intelligence is inherently difficult and susceptible to error;
- The view held by thinkers whom I describe as *information age optimists*, who believe the limitations of intelligence can to a significant degree be overcome by the use of modern information and communications technology;
- And the view held by many *terrorism analysts*, which is that the problem of terrorism presents particularly difficult challenges for the intelligence community, but that these can be overcome at least in part by a greater focus on human intelligence.

In order to test how well these schools of thought account for the performance of the U.S. intelligence community against the threat of terrorism, I will derive a set of hypotheses for each, and in section three I will test these hypotheses using the case of the Marine Barracks bombing in Beirut in 1983. Although the use of a single case study can only provide tentative conclusions, I believe the Beirut bombing presents a useful case study, particularly because a large amount of primary and secondary source material is available. While any open-source, academic study of intelligence matters is of course limited by the exclusion of classified materials--and this thesis is no exception-- I believe sufficient material is available about this case to make a study grounded in intelligence theory quite feasible.[2] The bombing has been examined by an official commission, several Congressional committees, and many academic and other authors. Published studies have examined the interaction among the intelligence community supporting the U.S. Marines in Beirut, the military commanders on the scene and elsewhere in the chain of command, and the policy makers in Washington. These studies have attempted to answer a question that sounds familiar in the post-9/11 world: How could the Marines have been so completely surprised by the attack, especially following the massive car bomb attack earlier in the year that destroyed the U.S. embassy in Beirut?

While many writers have studied the limitations of intelligence in dealing with terrorism in terms of what might be called *substantive* limits, this thesis will focus on *theoretical* limitations. It is not my intent to develop specific indicators to be used in analyzing terrorist attacks; but rather to examine the Beirut bombing through the lens of various theories of intelligence failure and surprise, in the hopes of gaining a better understand of the limitations of intelligence. As a preview of my conclusions, I believe this case study demonstrates that none of these theories explains satisfactorily the limitations of the intelligence community in the fight against terrorism.

The traditional theory appears to do the best job of providing a set of hypotheses that are confirmed by our case, but it leaves the analyst as well as the policy maker unsatisfied. As Elliot Cohen has complained, the traditional view among many intelligence professionals can be described as the “no fault” school—after all, this view holds, no one can expect an intelligence

[2] Although I am a retired naval intelligence officer, I was not involved in the Beirut operation, and I did not specialize in terrorist analysis.

analyst to predict the future or foresee what is fundamentally unforeseeable.[3] The problem of terrorist attacks certainly seems to fit this model, and as we will see, a consensus among many who studied the Beirut attack was that it had been impossible to predict that terrorists would use such a devastating weapon to such terrible effect. But no military commander or political decision maker can be expected to accept the conclusion that terrorist attacks are simply too difficult a problem. Additionally, post-mortem investigations of terrorist attacks have often produced the same finding seen after Pearl Harbor and other conventional surprise attacks: that there were indications of the threat available ahead of time, but for various reasons they were not heeded.

In section four, I will briefly introduce another model that may be more useful than these theories in understanding the limitations of intelligence in providing warning of terrorist attacks. This is based on the literature on accident and disaster theory, and specifically the concept that Charles Perrow has called a *normal accident*.[4] Perrow studied disasters in complex systems such as nuclear power plants, and concluded that in such systems accidents are not just a likely result of human or mechanical error, but can occur even when all reasonable safety precautions are taken and personnel follow the required procedures. Although several intelligence scholars have briefly discussed the relationship between Perrow's theory and intelligence failure, little in-depth work has been done to link the two concepts, and in this thesis I will attempt to begin such a study.

Just as it is not enough to conclude that intelligence work is naturally prone to error, it is also not sufficient to find simply that intelligence failures resemble complex system disasters. The question must be asked, so what? Even if a particular theory or school of thought appears to

[3] Eliot A. Cohen, "The 'No Fault' View of Intelligence," in *Intelligence Requirements for the 1990's: Collection, Analysis, Counterintelligence, and Covert Action*, ed. Roy Godson (Lexington, MA: Lexington Books, 1989).
[4] Charles Perrow, *Normal Accidents: Living With High-Risk Technologies*. New York: Basic Books, 1984.

explain how or why failures have occurred in the past, a policy maker or intelligence analyst needs to know what lessons that theory holds for today and for the threats of tomorrow. In my concluding section I will attempt to draw together the lessons suggested by the various schools of thought as they apply to the Beirut bombing case study, and propose possible avenues for further research.

First however, we should define what we mean by "intelligence failure." The place to start is by posing the question, what is intelligence? Classic definitions of intelligence vary widely. Sherman Kent, the founder of modern intelligence scholarship, defined it as encompassing knowledge, organization, and activities of intelligence agencies—too broad a definition for a limited study such as this one.[5] Others see intelligence as "secret information about the enemy,"[6] but that appears to be too narrow in this age of open source intelligence. Mark Lowenthal provides a more useful definition in arguing that *information* is anything that can be known, and "*intelligence* refers to information that meets the stated or understood needs of policy makers and has been collected, refined, and narrowed to meet those needs."[7] As we will see in this case study, the two relationships of intelligence to information, and intelligence to policy, are key, and any definition that neglects those relationships cannot be complete.

From this definition we can next determine, what is the *function* of intelligence? This is an important question, for a failure of intelligence is likely to involve a failure to fulfill this function. Scholars of intelligence generally agree that intelligence analysts should not be expected to predict the future. While some policy makers might object, this seems to be a

[5] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949).
[6] See for example, Hans Mark, *The Doctrine of Command, Control, Communications, and Intelligence: A Gentle Critique* (Harvard University: Program on Information Resources Policy Guest Presentations, 2000).
[7] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2d ed. (Washington, DC: CQ Press, 2003), 1 (emphasis added).

reasonable assumption. For one thing, intelligence simply can't perform such a function: history and hard experience have shown, in the words of Schlomo Gazit, "The intelligence man cannot predict the future."[8] Such a task is also not their job—or at least it should not be. Joseph Nye puts it this way: "the job of intelligence is not to predict the future, but to help policymakers think about the future."[9] William Colby sets the bar high, but provides the most useful definition: "the true function of intelligence is to help make decisions to bring about a better future and avoid the dangers that an intelligence projection might present—to change rather than merely to know the future."[10]

What, then, is an intelligence failure? The very concept is a sensitive one with intelligence personnel, and Lt Gen Paul Van Riper echoed the feelings of many analysts when he lamented after 9/11: "The Intelligence Community does a damn good job. It troubles me that people always speak in terms of operational successes and intelligence failures."[11] But whether or not intelligence personnel are unfairly or too frequently blamed for mistakes, it is important to agree on what is meant by intelligence failure. Mark Lowenthal provides a good start: "An intelligence failure is the inability of one or more parts of the intelligence process—collection, evaluation and analysis, production, dissemination—to produce timely, accurate intelligence on an issue or event of importance to national interests."[12]

[8] Schlomo Gazit, "Intelligence Estimates and the Decision-Maker," in *Leaders and Intelligence*, ed. Michael I. Handel (London: Frank Cass, 1989), 273.

[9] Joseph S. Nye, Jr., "Peering into the Future," *Foreign Affairs* (July/August 1994): 88.

[10] William E. Colby, "Deception and Surprise: Problems of Analysts and Analysis," in *Intelligence Policy and National Security*, ed. Robert L. Pfaltzgraff, Jr., Uri Ra'anan, and Warren Milberg (Hamden, CT: Archon Books, 1981), 94. Willmoore Kendall made much the same argument years ago, when he criticized the classical thinking of Sherman Kent, who seemed to feel that if only intelligence analysts were smart enough, they could foresee the future just like reading a ticker tape as it rolls out. Willmoore Kendall, "The Function of Intelligence," *World Politics*, July 1949. A good discussion of these issues is Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence*, no date 2002.

[11] "Reinventing War," *Foreign Policy*, Nov/Dec 2001, 32.

[12] Mark M. Lowenthal, "The Burdensome Concept of Failure," in *Intelligence: Policy and Process*, ed. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle (Boulder, CO: Westview Press, 1985), 51.

But Lowenthal's definition neglects the link between intelligence and policy; surely an intelligence failure can also arise when recipients misuse the intelligence they are given. Abram N. Shulsky and Gary J. Schmitt focus on those who receive intelligence, writing "An intelligence failure is essentially a misunderstanding of the situation that leads a government (or its military forces) to take actions that are inappropriate and counterproductive to its own interests."[13] The best definition is probably a combination of this with Lowenthal's, for failure can involve either a failure of the intelligence community to produce the necessary intelligence, or a failure of decision makers to act on it appropriately.[14]

We will focus here on a particular subset of intelligence failure: the failure to detect or otherwise prevent a surprise attack. Writers on strategic surprise have examined the failure of intelligence services to prevent a wide variety of unexpected events that pose a threat to national security, such as American intelligence's inability to foresee the fall of the Shah of Iran, or to detect the Cuban missile crisis until it was nearly too late. At the military operational level, cases such as the invasion of Grenada have been studied as examples of intelligence failure. But the failure to detect indications of a surprise attack is by far the most widely studied example of intelligence failure, and it is this type of failure we will focus on here.

Two arguments might be made against this focus on surprise attack. One is that there is too much emphasis in the intelligence community--and especially among its critics--on avoiding surprise. Willmoore Kendall wrote soon after World War II that intelligence was too dominated by a wartime concept, leading in part to a "compulsive preoccupation with *prediction*, with the

[13] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence, 3d Ed* (Washington, DC: Brassey's, 2002), 63.
[14] Another good discussion of intelligence failure is Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), chapter 13, 223-239.

elimination of 'surprise' from foreign affairs."[15] Kendall was right then, and his point continues to hold today; but especially after the 2001 attacks it appears clear that if a key function of intelligence is to help decisionmakers plan for possible futures, then it must help anticipate future terrorist attacks.

A second criticism of the approach taken in this thesis is occasionally heard from those who believe there actually isn't any major problem with failure in the American intelligence system today. In the view of some, especially those in or close to the intelligence community, the system works better than most people might think. Arthur S. Hulnick, for example, has written, "The track record of American intelligence in detecting surprise is actually quite good." Hulnick adds, however, that it is hard to prove his point, because in many cases warning helps to avert problems—it's hard to study intelligence success—and he also concedes that surprise is always possible.[16] This complaint of the intelligence community may have merit, but it is not supported by the case study examined here. This thesis demonstrates that in the Beirut bombing, the intelligence community did a poor job of helping decision makers bring about a better future; and it looks to intelligence theory to help understand that failure.

[15] Kendall, 549.

[16] Arthur S. Hulnick, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century* (Westport, CT: Praeger, 1999), 48. A former National Intelligence Officer for Warning, Robert Vickers, also holds a relatively sanguine view about intelligence's capabilities: Robert D. Vickers, Jr., "The State of Warning Today," *Defense Intelligence Journal* 7, no. 2 (Fall 1998).

2. THEORIES OF INTELLIGENCE FAILURE AND TERRORISM

Although scholars and intelligence analysts have put forward numerous theories to explain the persistence of failure and strategic surprise, most of these theories concern the problem of surprise attack by a conventional military force. Few writers on intelligence have attempted to apply these theories to the problem of surprise attack by terrorists. At the same time, although many scholars and security specialists have studied the problem of terrorism, few of these writings have attempted to incorporate the literature on intelligence into their work. This section will review these two literatures—on intelligence failure and on terrorism—and describe three major theories, or schools of thought, that can be found to explain intelligence failure. I have called these theories the *traditional* view, the *information age optimists* view, and the *terrorism analysts'* view. In order to test these theories, I then develop a set of hypotheses that will be used in the next section to test against the case study of the 1983 Marine Barracks bombing in Beirut.

First, it should be noted that while the writings on intelligence theory and terrorism are generally not well integrated, some authors have attempted to analyze terrorist threats using the traditional theories of intelligence. In particular, a number of academics and others have made careful comparisons of the 9/11 attacks with Pearl Harbor. A good example of such a comparison is by James J. Wirtz, who has written that many of the problems found after Pearl Harbor, such as the existence of signals that were found after the fact to have been missed, were also evident in the case of the September 11 attacks.[1] Parker and Stern have examined 9/11 through the lens of the literature on strategic surprise, and while their article does not contain

[1] James J. Wirtz, "Deja Vu? Comparing Pearl Harbor and September 11," *Harvard International Review* (Fall 2002). As we will see below, this explanation fits easily into the traditional view of intelligence failure.

many surprises itself, the authors find the various approaches taken by intelligence theorists useful in understanding the recent failure.[2]

The Traditional View

The predominant view in the literature on intelligence failure and strategic surprise is a pessimistic one: intelligence is intrinsically difficult, and not likely to get better. Academics and intelligence professionals who subscribe to this traditional or orthodox view tend to disagree with the two other schools of thought: unlike the information age optimists, they do not believe intelligence is likely to get much better through the use of information systems or other technology, and unlike the writers who focus on terrorism, they believe the problems facing intelligence arise from factors that apply no matter what the issue or enemy being analyzed.

The traditional school of thought is broad, and its adherents do not necessarily agree on any specific cause of intelligence failures. But most tend to analyze the problem of intelligence failure at two levels of analysis: First is the level of *responsibility*, of "who is at fault." This is where discussions about policy matters typically focus, and it is this level of analysis that divides theorists within the traditional school into three sub-schools. Most writers on intelligence failures tend to believe the primary fault most often lies with *decision makers* at the policy level. Another, relatively small group in the traditional school tends to assign fault to the *intelligence community*, while a third group believes that surprise is most often the result of deception or other actions taken by the *enemy*.

Most traditional intelligence theorists, however, also analyze failure and surprise at the *functional* level, where the search is for the cause of the mistakes that might have been made by

[2] Charles F. Parker and Eric K. Stern, "Blindsided? September 11 and the Origins of Strategic Surprise," *Political Psychology* 23, no. 3 (September 2002). Also very useful are Fred L. Borch, "Comparing Pearl Harbor and '9/11': Intelligence Failure? American Unpreparedness?," *Journal of Military History* 67, no. 3 (July 2003); Malcolm Gladwell, "Connecting the Dots," *The New Yorker*, March 10 2003.

policy, intelligence, or the enemy. These causes include information and communications problems such as the ratio of signal to noise; cognitive problems such as misperception by analysts or policy makers; or organizational and bureaucratic difficulties. These two levels of analysis are crosscutting—cognitive factors, for example, can apply no matter who one believes might be primarily responsible for the mistakes—but most intelligence theorists tend to agree that these functional difficulties all play a role in intelligence failure. The real distinction between theorists lies in the question of who is responsible for the failure, and that is where our discussion will focus.

What is now the orthodox school of intelligence theory developed partly as a corrective to the classical school of Sherman Kent, who saw intelligence as a form of academics that could be done well, if performed by the best minds applying rigorous social science methods.[3] But Kent's optimistic view was countered by Roberta Wohlstetter's pessimistic analysis of Pearl Harbor. She concluded that the problem was not a failure of intelligence collection—which might be correctable—but rather of analysis, largely because of the large signal to noise ratio. "In short, we failed to anticipate Pearl Harbor not for want of the relevant materials, but because of a plethora of irrelevant ones."[4] Intelligence analysts and military leaders were not guilty of negligence, for they had faced ambiguous data. No intercepted messaged had announced, "Air Raid on Pearl Harbor," Wohlstetter pointed out, adding that "perhaps one of the important lessons to learn from Pearl Harbor is that intelligence will always have to deal with shifting signals. Its evidence will never be more than partial, and inference from its data will always be hazardous."[5]

[3] Kent.
[4] Wohlstetter, 387.
[5] Ibid., 227.

Unlike later theorists of intelligence failure, Wohlstetter did not closely examine the psychological or other functional reasons behind the disaster, and she did not assign blame to any particular actor. But her book represented a clear break from the classical school, for it suggested that failure had been unavoidable. She also anticipated the later arguments of the traditional school concerning the relative unimportance of information technology. Writing at the beginning of the computer age, she considered the question of whether such a disaster could occur again: "In spite of the vast increase in expenditures for collecting and analyzing intelligence data and in spite of advances in the art of machine decoding and machine translation, the balance of advantage seems clearly to have shifted since Pearl Harbor in favor of a surprise attacker."[6]

The decision-maker at fault

Richard Betts made the case for the major sub-school among traditional intelligence theorists in a much-cited 1978 article in which he wrote, "Intelligence failures are not only inevitable, they are natural."[7] Betts actually made two main arguments. First, echoing Wohlstetter, he argued that intelligence is inherently difficult, not because intelligence data is absent, but because the information analysts work with is largely ambiguous. But second, Betts went on to point his finger at *policy makers* as most often responsible for failure, for not having taken the advice given by intelligence. "In the best-known cases of intelligence failure, the most crucial mistakes have seldom been made by collectors of raw information, occasionally by professionals who produce finished analyses, but most often by the decision makers who consume the products of intelligence services."[8]

[6] Ibid., 399.
[7] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (October 1978): 88.
[8] Ibid.: 61.

In his later book *Surprise Attack*, Betts made this point about the responsibility of decision makers even more strongly: "The principal cause of surprise is not the failure of intelligence but the unwillingness of political leaders to believe intelligence or to react to it with sufficient dispatch."[9] This failure to react, he added, is not necessarily through incompetence, but because leaders may be concerned that an overreaction on their part could worsen the crisis. Betts focused on sudden attacks that start wars, and wrote that while the common view is that surprise attacks occur because intelligence fails to warn, that is not usually the case. In fact, we worry too much about warning, he argued, and not enough about the response to the warning we do receive. This resulted in what he decried as a fixation on organizational and technical solutions: "The United States has reached the point of diminishing returns from organizational solutions to intelligence problems."[10]

Betts described three phases of warning: *political*, in which tensions are increasing; *strategic*, in which the enemy is mobilizing and deploying forces; and *tactical*, which involves detection of the initial movements of the attack itself. He wrote that while tactical warning was still a concern, there would always be *some* warning evident as tensions increase; there are, he wrote in a comment frequently heard among traditional theorists of intelligence failure, no significant "bolts from the blue."[11] He described various types of surprise, such as concerning the timing, location, and strength and performance of an enemy attack, and examined various cognitive and analytical difficulties faced by analysts, such as the "cry wolf" problem and deception on the part of the enemy. Innovation is likely to produce successful attacks, and can involve either technical or doctrinal surprise. But Betts argued that technical surprise is rarely a

[9] Richard K. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, DC: Brookings, 1982), 4.
[10] Ibid., 17.
[11] Ibid., 18.

significant factor in war, while doctrinal surprise, such as seen in the German Blitzkrieg, can be very important.[12]

How, then, can the analyst or policy maker resolve these problems and avoid a surprise attack? Betts could offer little comfort, and argued that the common solutions were likely to just create more problems. Flexibility, for example, was the usual prescription for avoiding surprise, but Betts pointed out that making one's self open to more hypotheses could lead to more mistakes. Establishing a position of "devil's advocate" could help, but might end up aggravating the cry wolf problem, and result in the devil's advocate being marginalized. Many recommendations after intelligence failures, Betts wrote, "tend to be hortatory, homiletic, and repetitive." After Pearl Harbor, for example, the Congressional investigation concluded among other things that analysts should be flexible, should share intelligence, and should have more imagination—recommendations Betts found minimally useful.[13]

Betts studied surprise attacks ranging from World War II through the Korean War to the 1973 Yom Kippur War, and found that in most cases someone was ringing the alarm, but it was not heard. The problem was usually that there existed a conceptual consensus among decision makers that rejected the alarm, or else false alarms had dulled the impact of the alarm at the moment of crisis. It was better, he concluded, to make plans to deal with surprise, than to try to reduce its likelihood.

The second key proponent of the traditional school of intelligence failure is Michael Handel, who frequently argued, as in a 1977 article, "Studies of military surprise have reached the point of diminishing returns."[14] By this he meant that case studies had demonstrated that

[12] Ibid., 113-115.

[13] Ibid., 286.

[14] Michael I. Handel, "The Yom Kippur War and the Inevitability of Surprise," *International Studies Quarterly* 21, no. 3 (September 1977): 461.

despite the presence of sufficient indicators—and even despite the sage advice from academics—intelligence professionals and decision makers often failed to arrive at the correct conclusion. Happily for the student of intelligence today, Handel did not let this problem of diminishing returns stop him from continuing to publish on the subject of surprise and intelligence. He often branched out from the subject of pure military surprise, to study, for example, how diplomatic surprise differed from military surprise,[15] but he returned frequently enough to the problem of military surprise and surprise attack to leave a considerable literature.

Handel wrote that his study of military surprise strengthened his "pessimistic conclusion that there is little chance, despite the availability of adequate information, ultra-sophisticated technologies, and all the human effort invested, to prevent or forestall impending surprise attack."[16] He described intelligence failures, and thus surprise, as inevitable—but he also pointed out that the advantage gained by surprise attack is often limited. The one conducting the attack often loses the war, and in fact Handel found there appears to be no correlation between achieving surprise and achieving victory.[17]

Handel found it possible to distinguish between intelligence failures that are caused by:

- Deliberate actions by the enemy, such as efforts at secrecy or deception. He did not focus on this cause of failure, but as we will see below, some theorists believe it is the principle cause.

- Inherent difficulties with intelligence—such as in attempting to predict the future actions of an enemy who hasn't yet decided what he will do next. Because intelligence works with human nature, it is not a science, and can never be perfect, no matter how much information is acquired.

[15] On diplomatic surprise, see Michael I. Handel, "Surprise and Change in International Politics," *International Security* 4, no. 4 (Spring 1980); Michael I. Handel, "Surprise in Diplomacy," in *Intelligence Policy and National Security*, ed. Robert L. Pfaltzgraff, Jr., Uri Ra'anan, and Warren Milberg (Hamden, CT: Archon Books, 1981).
[16] Michael I. Handel, "Perception, Deception and Surprise: The Case of the Yom Kippur War," in *International Violence: Terrorism, Surprise and Control*, ed. Yair Evron (Jerusalem: The Hebrew University of Jerusalem, 1979), 25.
[17] Michael I. Handel, "Intelligence and the Problem of Strategic Surprise," *Journal of Strategic Studies* 7, no. 3 (September 1984): 230.

- Self-generated problems, like rigid conceptions in the minds of decision makers or analysts that compounded the problem of excessive noise.[18]

This list of problems suggests Handel believed intelligence failure could occur as a result of a wide variety of factors. But he felt the most common *functional* cause of intelligence failure was based in the psychological limitations of human nature: “Most intelligence failures occur because intelligence analysts and decisionmakers refuse to adapt their concepts to new information.”[19]

At the level of *responsibility*, Handel agreed with Betts that the most common culprit was the decision maker, who refused to accept the analysis provided by intelligence. He saw intelligence work as divided into the three levels of acquisition, analysis, and acceptance, and wrote, “Historical experience confirms that intelligence failures were more often caused by a breakdown on the level of acceptance than on the acquisition or analysis levels.”[20] The Israeli experience in the 1973 war was a key example for Handel, as Israeli leaders deceived themselves through a too rigid adherence to their “concept,” too much faith in their own deterrent power and military capabilities, and an unwillingness to believe the Arabs would attack.[21]

Handel also agreed with Betts about the relative unimportance of *technological surprise*. He argued that although technological surprise was likely to be common of future wars, it would not cause as serious a problem as other types of surprise, such as strategic or doctrinal surprise. Intelligence services should be able to detect technological surprise reasonably well, because such determination relies on analysis of capabilities, which is relatively straightforward, as

[18] This list of problems is found in Michael I. Handel, "Avoiding Political and Technological Surprise in the 1980's," in *Intelligence Requirements for the 1980's: Analysis and Estimates*, ed. Roy Godson (New Brunswick, NJ: Transaction Books, 1980).
[19] Ibid., 103. Another useful discussion of psychological and other problems with intelligence is Michael I. Handel, "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty," in *Intelligence: Policy and Process*, ed. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle (Boulder, CO: Westview Press, 1985).
[20] Handel, "Avoiding Political and Technological Surprise in the 1980's," 98.
[21] See for example, Handel, "The Yom Kippur War and the Inevitability of Surprise."; Handel, "Perception, Deception and Surprise: The Case of the Yom Kippur War."

opposed to the analysis of intentions, which is always difficult. In addition, Handel wrote, technological breakthroughs can often be easily defeated; they take a long time to develop; and in any case, history has shown that the enemy often fails to take advantage of a technological superiority. But even here, intelligence personnel can have trouble getting decision makers to listen: "Intelligence organizations often have more problems convincing their own governments or armed forces to use the information collected than they do in collecting the information itself."[22]

So, what to do? Handel's advice is very similar to that of Betts. Since intelligence failure is inevitable, he wrote, we must learn to live with ambiguity. Trying to fix one aspect of intelligence often simply leads to new problems, and "the next best thing to *avoiding* surprise is being able to *cope* with it once it has taken place."[23]

Although Betts and Handel are the most significant writers on intelligence failure and strategic surprise, they are by no means the only theorists who fall into this school of thought. Another important study is by Ephraim Kam, who agreed with the consensus that surprise attacks are very difficult to prevent, arguing that there are almost no instances of such an attack in which there was a single, definitive indicator that told defending forces what they need to know.[24] But Kam disagreed with the conventional view that capabilities are easier to discern than intentions; he found that most cases of surprise attack showed how easy it is to make mistakes in discerning capabilities.[25]

Other scholars who fit into the consensus view include Klaus Knorr, who wrote in 1964, in a phrase that has been since echoed by others, "it seems clear that the practical problem is to

[22] Handel, "Avoiding Political and Technological Surprise in the 1980's," 93. See also Michael I. Handel, "Technological Surprise in War," *Intelligence and National Security* 2, no. 1 (January 1987).
[23] Handel, "Avoiding Political and Technological Surprise in the 1980's," 105. (Emphasis in original.)
[24] Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988), 38.
[25] Ibid., 56.

improve the 'batting average'—say, from .275 to .301—rather than to do away altogether with surprise."[26] A number of writers have studied specific case studies of intelligence failure and surprise, including the Korean War, the Falklands conflict, and others, and generally support the conventional views as expressed by Betts and Handel.[27] Most of these scholars of intelligence agree that decision makers bear at least a major portion of the responsibility for intelligence failure. Mark M. Lowenthal argues that in nine out of the ten cases he examined, policymakers played a significant role in the failure.[28] Loch Johnson has written that the unwillingness of policy makers to accept the judgments of the intelligence community is a central problem in intelligence, and he has termed this phenomenon the "paradox of rejection."[29]

Intelligence professionals—perhaps not surprisingly—have also expressed the view that policy makers need to accept at least part of the blame. Charles E. Allen, the National Intelligence Officer for Warning from 1988-94, describes the numerous warnings his office issued prior to the Iraqi invasion of Kuwait in 1990. He writes that these warnings went unheeded by senior intelligence as well as policy officials, who did not think an attack was likely. These senior officials, Allen argues, were subject to the same sort of cognitive distortions

[26] Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics* 16, no. 3 (April 1964): 460. Robert Jervis made a similar comment in a very useful article: Robert Jervis, "What's Wrong with the Intelligence Process?," *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986). For other orthodox analyses of intelligence failure, see Christopher Brady, "Intelligence Failures: Plus Ca Change..." *Intelligence and National Security* 8, no. 4 (October 1993); Richard Brody, "The Limits of Warning," *The Washington Quarterly* 6, no. 3 (Summer 1983); Steve Chan, "The Intelligence of Stupidity: Understanding Failures in Strategic Warning," *American Political Science Review* 73, no. 1 (March 1979); Janice Gross Stein, "'Intelligence' and 'Stupidity' Reconsidered: Estimation and Decision in Israel, 1973," *Journal of Strategic Studies* 3, no. 2 (September 1980); Janice Gross Stein, "Military Deception, Strategic Surprise, and Conventional Deterrence: A Political Analysis of Egypt and Israel, 1971-73," *Journal of Strategic Studies* 5, no. 1 (March 1982).

[27] Katarina Brodin, "Surprise Attack: The Case of Sweden," *Journal of Strategic Studies* 1, no. 1 (May 1978); H. A. DeWeerd, "Strategic Surprise in the Korean War," *Orbis* 6, no. 3 (Fall 1962); Johan Jorgen Holst, "Surprise, Signals and Reaction: The Attack on Norway April 9th 1940--Some Observations," *Cooperation and Conflict* (vol I 1986); Gerald W. Hopple, "Intelligence and Warning: Implications and Lessons of the Falkland Islands War," *World Politics* 36, no. 3 (April 1984); Avi Shlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics* 28, no. 3 (April 1976); Yaacov Vertzberger, "India's Strategic Posture and the Border War Defeat of 1962: A Case Study in Miscalculation," *Journal of Strategic Studies* 5, no. 3 (September 1982).

[28] Lowenthal, "The Burdensome Concept of Failure."

[29] Loch K. Johnson, "Analysis for a New Age," *Intelligence and National Security* 11, no. 4 (October 1996): 663.

experienced by Israeli officials in 1973, as they underestimated the aggressor's intentions, downplayed the significance of military indicators, and gave excessive weight to the opinion of foreign leaders and intelligence services.[30] William H. J. Manthorpe Jr. writes that the job of avoiding surprise and achieving effective warning should be split evenly between the intelligence community and policy makers. "As long as surprise and warning failure are characterized as 'intelligence failures,' as they have been in the past, they will continue to occur. It is now time for the institutions and policymakers of the wider national security apparatus to accept some of the responsibility for avoiding surprise and achieving warning."[31]

Intelligence at fault

While the dominant view among scholars of intelligence is that policy makers deserve more responsibility for failure than they usually receive, there is a smaller but still significant body of writing on intelligence failure that argues the fault usually begins with the intelligence community. As might be expected, this sub-school is frequently found among policy makers who claim the intelligence community has let them down. Such complaints often come from the top. Former CIA Director Robert M. Gates has written that presidents are often unhappy with intelligence, both in office and afterward; presidential memoirs, he found, tend to say very little

[30] Charles E. Allen, "Warning and Iraq's Invasion of Kuwait: A Retrospective Look," *Defense Intelligence Journal* 7, no. 2 (Fall 1998).

[31] William H. J. Manthorpe, Jr., "From the Editor," Defense Intelligence Journal 7, no. 2 (Fall 1998): 7. Other intelligence community critics of policy makers include Willard C. Matthias, *America's Strategic Blunders: Intelligence Analysis and National Security Policy, 1936-1991* (University Park, PA: Pennsylvania State University, 2001); Eugene Poteat, "The Use and Abuse of Intelligence: An Intelligence Provider's Perspective," Diplomacy and Statecraft 11, no. 2 (July 2000); George H. Poteat, "The Intelligence Gap: Hypotheses on the Process of Surprise," International Studies Notes 3, no. 3 (Fall 1976). A variant on this critique of policy makers is that failures are caused by a lack of attention to, or budgets for, intelligence, not necessarily because of specific failures of policy to heed advice. The point is that intelligence could have given better advice, if only it had been given more priority and emphasis beforehand. For example, Lyman B. Kirkpatrick, Jr., *Captains without Eyes: Intelligence Failures in World War II* (London: Macmillan, 1969).

about intelligence, and what they do say is usually critical, such as Jimmy Carter's comment that "I am not satisfied with the quality of our political intelligence."[32]

But not all critiques of the intelligence community come from frustrated policy makers—a number of analysts and other members of the intelligence community have complained about mistakes and incompetence within intelligence. Patrick J. McGarvey argued during the Vietnam War that the Defense Intelligence Agency (DIA) did a poor job as a result of attempting to justify itself through worst-case guesses, succumbing to command influence, and attempting to please everybody and inform nobody.[33] Mary O. McCarthy, another former National Intelligence Officer for Warning, has argued more recently that "the likelihood of a cataclysmic warning failure is growing," and the intelligence community needs more analytical rigor and imagination.[34]

The debate over whether failure is more often the responsibility of analysts or decision makers is often carried out in the broader literature on the relationship between intelligence and policy. For many writers sympathetic to the intelligence community, the challenge lies in ensuring decision makers understand and trust the warnings issued by intelligence. Kent argued the classical view, that while it might be unfortunate that policy makers will often do what they want anyway, the job of intelligence is to do the best it can, and let the policy maker feel "thoroughly uncomfortable" if he or she decides not to listen to the warning.[35] Although Kent's

[32] Robert M. Gates, "An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House," *The Washington Quarterly*, Winter 1989, 35.

[33] Patrick J. McGarvey, "DIA: Intelligence to Please," in *Readings in American Foreign Policy: A Bureaucratic Perspective*, ed. Morton H. Halperin and Arnold Kanter (Boston, MA: Little, Brown, 1973).

[34] Mary O. McCarthy, "The Mission to Warn: Disaster Looms," *Defense Intelligence Journal* 7, no. 2 (Fall 1998): 18. Other thoughtful critiques of the intelligence community, although not written by intelligence personnel, are Robert F. Ellsworth and Kenneth L. Adelman, "Foolish Intelligence," *Foreign Policy* 36 (Fall 1979); Allan E. Goodman, "Dateline Langley: Fixing the Intelligence Mess," *Foreign Policy* 57 (Winter 1984-85).

[35] Sherman Kent, "Estimates and Influence," *Foreign Service Journal* 46, no. 5 (April 1969): 16.

argument comes across as sounding more than a little whiney today, his view continues to be reflected among many of the traditional writers on intelligence failure.

Although the scope of this thesis does not permit a thorough review of the literature on the relationship between intelligence and policy, it is worth noting that not all intelligence theorists see this relationship as a one-sided battle by clear-eyed analysts fighting for the attention of overworked and inattentive policy makers. Cynthia M. Grabo turns the argument around, writing that it is an axiom of intelligence that warning does not exist until it has been conveyed to the policymaker, who must understand that he or she has been warned. She argues that when the policymaker doesn't get the message, the fault is often with intelligence, for not having been loud or clear enough.[36] Harry Howe Ransom holds a more balanced view of the intelligence-policy relationship, arguing that while decision makers tend to hear what they want no matter what intelligence says, intelligence agencies tend to report what they think their leaders want to hear, no matter what the facts suggest.[37]

In addition, a significant school of thought challenges the traditional notion that intelligence and policy should be carefully separated from each other. These writers are often critical of what they see as the typical mindset among intelligence analysts, and argue that intelligence must do a better job not only of understanding how the enemy thinks, but also what

[36] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College, 2002), 14.

[37] Harry Howe Ransom, "Strategic Intelligence and Foreign Policy," *World Politics* 27, no. 1 (October 1974). A good review of the intelligence-policy relationship is Mark M. Lowenthal, "Tribal Tongues: Intelligence Consumers, Intelligence Producers," *The Washington Quarterly* 15, no. 1 (Winter 1992). Also useful: Schlomo Gazit, "Estimates and Fortune-Telling in Intelligence Work," *International Security* 4, no. 4 (Spring 1980); Alexander L. George, "Warning and Response: Theory and Practice," in *International Violence: Terrorism, Surprise and Control*, ed. Yair Evron (Jerusalem: The Hebrew University of Jerusalem, 1979); Glenn P. Hastedt, "The New Context of Intelligence Estimating: Politicization or Publicizing?," in *Intelligence and Intelligence Policy in a Democratic Society*, ed. Stephen J. Cimbala (Dobbs Ferry, NY: Transnational Publishers, Inc., 1987); Thomas L. Hughes, *The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making* (Foreign Policy Association Headline Series No. 233, 1976); Arthur S. Hulnick, "Relations between Intelligence Producers and Policy Consumers: A New Way of Looking at an Old Problem," in *Intelligence and Intelligence Policy in a Democratic Society*, ed. Stephen J. Cimbala (Dobbs Ferry, NY: Transnational Publishers, Inc., 1987); Robert Jervis, "Intelligence and Foreign Policy," *International Security* 11, no. 3 (Winter 1986-1987).

the decision makers need. In an early and still useful expression of this view, Benno Wasserman criticized the intelligence community for an unwise emphasis on current intelligence and the accumulation of data. Instead, he argued, intelligence should focus on longer-term and analytic efforts, shaped by a closer understanding of what policy makers believe and care about.[38] More recently, writers associated with the Consortium for the Study of Intelligence have argued that the conventional paradigm of strict separation between intelligence and policy may need to be changed, and the intelligence community should move away from the pessimistic focus on intelligence as academics.[39] Some have even made the argument—heretical to intelligence traditionalists—that political leaders can make as good or better assessments of the enemy than the "experts" in intelligence. Ernest May, in his recent book *Strange Victory*, makes this argument about France in 1940, and argues that intelligence analysis could be improved by integrating it better with policy and decision making.[40]

The enemy at fault: theories of deception

A third sub-school among traditional intelligence theorists concentrates not on the failure of either the intelligence agencies or policy makers, but by the actions of the *attacker*. These writers most commonly focus on deception, and the most prominent example is Barton Whaley, whose *Codeword Barbarossa* examined the Nazi invasion of the Soviet Union in 1941. Whaley writes that he began his study of that operation by consulting the secondary works, which all concluded that the fault lay with Stalin's paranoia and mistakes. But as he continued his

[38] Benno Wasserman, "The Failure of Intelligence Prediction," *Political Studies* 8, no. 2 (June 1960).

[39] Consortium for the Study of Intelligence, *The Future of U.S. Intelligence* (Report Prepared for the Working Group on Intelligence Reform, 1996). Of note, these writers also advocate a greater role for counter-intelligence and covert action in intelligence—another break from the classical view, and more in line with the views of terrorism specialists.

[40] Ernest R. May, *Strange Victory: Hitler's Conquest of France* (New York, NY: Hill and Wang, 2000), 461.

research, he found that it was *Hitler's deceptions* that actually caused the surprise, not mistakes on the part of the Soviets.[41]

Whaley argues that the critical factor in surprise attacks is what he calls *stratagem*: "a coordinated campaign of deception to mislead the victim's analysis."[42] He finds that the Wohlstetter model doesn't work in Barbarossa and in many other cases: the surprise was not the result of ambiguous signals or noise, but rather caused by the deliberate insertion of *false* signals by one side. In later writings Whaley took his argument even further, criticizing the intelligence community for its pessimistic view that deception is practically impossible to detect. He argued that this view was little more than an excuse for failure: "How handy then for intelligence professionals to be able to cite theories which claim that deception is undetectable and surprise is inevitable."[43] These analysts are wrong, because "In theory, deception can always be detected, and in practice often detected, sometimes even easily."[44] Whaley describes the rough outlines of what he calls a theory of deception, and how it can be detected through techniques such as the use of multiple sensors, and through an understanding of how deception is conducted by magicians and other practitioners. Unfortunately for the intelligence analyst, he does not explain his counter-detection procedures, but he note that he describes these techniques in the classes and seminars he leads on deception.[45]

[41] Barton Whaley, *Codeword Barbarossa* (Cambridge, MA: The MIT Press, 1973).
[42] Ibid., 171.
[43] Barton Whaley and Jeffrey Busby, "Detecting Deception: Practice, Practitioners, and Theory," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz (New Brunswick, NJ: Transaction Publishers, 2002), 182.
[44] Ibid.
[45] On Whaley's ideas, see also Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies* 5, no. 1 (March 1982); Barton Whaley, "Conditions Making for Success and Failure of Denial and Deception: Authoritarian and Transition Regimes," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz (New Brunswick, NJ: Transaction Publishers, 2002). Other useful sources on intelligence and deception include J. Bowyer Bell, "Toward a Theory of Deception," *International Journal of Intelligence and Counterintelligence* 16, no. 2 (Summer 2003); Roy Godson and James J. Wirtz, eds., *Strategic Denial and Deception: The Twenty-First Century Challenge* (New Brunswick, NJ: Transaction Publishers, 2002); Katherine L. Herbig and Donald C. Daniel, "Strategic Military Deception," in *Intelligence: Policy and*

Most intelligence theorists agree that deception can present a serious problem for intelligence analysts. Richards J. Heuer Jr. has written that deception is effective largely because it builds upon the cognitive problems that intelligence personnel and policy makers have in interpreting data.[46] But writers who follow the orthodox approach tend to differ from Whaley and others in this branch of the school, in that they believe deception is usually not a primary cause of surprise. Handel, for example, cited Whaley's work in writing that "the deceiver is almost always successful regardless of the sophistication of his victim in the same art."[47] This leads to a paradox for Handel: if one attempts to try to anticipate deception, one must treat all information as potentially invalid, and thus may reach even worse conclusions. But in later articles Handel did not appear to be very worried about deception, pointing out that it has frequently failed in war, and on occasion even proved counterproductive. He felt that while deception would always remain a part of military operations, technological advances in intelligence would tend to make it more difficult to conduct in the future.[48]

Critiques of the orthodox view

Several writers have critiqued this orthodox approach toward intelligence failure and surprise, and before we consider alternative approaches it will be useful to review these critiques. Elliott Cohen has been perhaps the strongest critic of the conventional school, calling it the "no fault" view of intelligence. He has written that former intelligence officers often find fault with

Process, ed. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle (Boulder, CO: Westview Press, 1985); Walter Jajko, "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning," *Comparative Strategy* 21, no. 5 (October-December 2002).

[46] Richards J. Heuer, Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981).

[47] Handel, "The Yom Kippur War and the Inevitability of Surprise," 467.

[48] Michael I. Handel, "Intelligence and Deception," *Journal of Strategic Studies* 5, no. 1 (March 1982): 22; Michael I. Handel, "Introduction: Strategic and Operational Deception in Historical Perspective," *Intelligence and National Security* 2, no. 3 (July 1987): 35. Other students of intelligence who are skeptical about the danger of deception include Kam, 143-146; Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic Books, 1985), 286-291.

policy makers, and "such a view implies that the fault for failure . . . rests not with the intelligence organizations, but with those dyspeptic, dogmatic, and uninformed politicians who resent the sting of dispassionate analysis."[49] Others, often academics, Cohen writes, claim the problem lies with the intractability of the intelligence problem itself (here Cohen cites Betts and Lowenthal). But Cohen argues that intelligence analysts commit flaws themselves, and recommends that analysts be better trained—to the same level as required for a PhD—and take steps to correct flawed mindsets that can lead to mirror imaging and other problems.

Cohen and John Gooch discuss this further in their book *Military Misfortunes*, arguing that many appear to expect too much from intelligence, apparently believing it should be able to foretell the future. That is the reason, they write, why the problem of surprise appears so prominent for many writers—because they expect intelligence to prevent it. But Cohen and Gooch argue that surprise is actually not so critical; for example, they argue that Pearl Harbor had only negligible strategic consequences,[50] and they quote Clausewitz on the point that surprise only rarely determines success or failure in war. I believe they dispose of surprise too easily here; while it is widely recognized that the Pearl Harbor attack was not militarily decisive, it clearly had clear and lasting strategic consequences, both for the U.S. in World War II and for the U.S. intelligence community to this day. I am more persuaded by Handel's approach to the question of surprise in military history; he argues that while strategic surprise may still not be necessarily decisive, it is becoming more important than it was in Clausewitz's day.

Cohen and Gooch also make the point that writers on Pearl Harbor (and presumably on other supposed failures) have tended to concentrate on the question of who was to blame, rather than on what was the nature of the failure. They acknowledge that someone must undertake the

[49] Cohen, 72.

[50] Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Vintage Books, 1991), 48.

"distasteful and essential" task of assigning responsibility, but they say that as they are satisfied that none of the principals at Pearl Harbor were incompetents, they will focus on the reasons *behind* the failure—which they find in organizational matters.[51] This logic is compelling, but I believe our focus on fault and responsibility is worthwhile. First, because much of the discussion in the theoretical literature under review focuses on this question, as does much of the debate concerning intelligence matters in America today. But also, I believe it is not enough to be satisfied that our leaders and policy makers are *not incompetent*. Competent leaders (and analysts) can make grave mistakes, especially under great pressures and when facing new and extreme challenges—such as the challenges of enemy and terrorist attack—and we should not avoid the question of responsibility.

Another perceptive critic of the orthodox school of intelligence is Abraham Ben-Zvi, who argues that other than Whaley's discussion of deception, thinking on intelligence and surprise attacks has not come very far since Wohlstetter. He argues that intelligence analysts are not as limited by cognitive and perceptual blinders as theorists often portray them to be. His study of surprise attack suggests that in many cases, analysts were able to provide tactical warning; at Pearl Harbor, for example, misperceptions and assumptions did not prevent the U.S. military from raising the alert level. While Wohlstetter and other theorists tend to attribute all action to cognitive limitations and minimize the role of conscious will, Ben-Zvi writes, in cases such as Pearl Harbor those cognitive limitations can be outweighed by a growing perception of the threat.[52]

[51] Ibid., 47.

[52] Abraham Ben-Zvi, "Misperceiving the Role of Perception: A Critique," *The Jerusalem Journal of International Relations* 2, no. 2 (Winter 1976-77): 76-77. See also Abraham Ben-Zvi, "Surprise: Theoretical Aspects," in *International Violence: Terrorism, Surprise and Control*, ed. Yair Evron (Jerusalem: The Hebrew University of Jerusalem, 1979), 94.

Ben-Zvi actually does not differ from the orthodox school very much concerning the question of responsibility: after studying a variety of cases of surprise attack, he concludes that tactical intelligence was usually available, but was not listened to, because decision makers did not believe the intelligence fit into their strategic assumptions.[53] This conclusion sounds as if it might have come from Betts or Handel, and Ben-Zvi's proposed solution—that tactical information must be analyzed on its own, and not in terms of prevailing strategic assumptions—sounds commonplace today. But his work remains useful and refreshing because Ben-Zvi argues that failures such as at Pearl Harbor cannot be blamed on any particular functional factor. The problem is not just a cognitive one, or an excess of signals over noise; "the Pearl Harbour [sic] surprise resulted from an accumulation of various bureaucratic, organizational, technical, communications, political, and perceptual factors, and cannot be attributed to a single cluster of considerations."[54]

The last challenger to the orthodox school we will consider is Ariel Levite, who disagrees with the dominant view that intelligence failures are natural and inevitable, and that efforts to reduce surprise are only marginally useful.[55] He believes the literature on intelligence failure dating back to Wohlstetter is wrong in believing that surprise occurs despite the existence of warning by intelligence, and that the problem lies in poor receptivity and in analytical and cognitive factors that may be resistant to improvement. He argues that "no credible or conclusive warning . . . was available prior to many historical cases of strategic surprise, arguments to the contrary notwithstanding."[56] But where sufficient intelligence is available,

[53] Abraham Ben-Zvi, "Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks," *World Politics* 28, no. 3 (April 1976).
[54] Abraham Ben-Zvi, "The Study of Surprise Attacks," *British Journal of International Studies* 5, no. 2 (July 1979): 144.
[55] Ariel Levite, *Intelligence and Strategic Surprise* (New York: Columbia University Press, 1987).
[56] Ibid., 26.

reliable warning *can* occur, and can induce the side being attacked to take appropriate defensive actions. The problem at Pearl Harbor, for Levite, was that U.S. intelligence capabilities were actually much more limited than is often believed, and there were actually fewer pieces of hard evidence than is thought. But this was not the case prior to the battle for Midway; in that case there was sufficient intelligence about Japanese intentions, it was used to warn, and the key decision maker—Admiral Nimitz—took action that was successful.[57]

Because the problem in the past was a lack of intelligence, Levite argues, improved collection systems and dedicated efforts may be able to enable intelligence to provide warning at least as good, and possibly better, than in the past.[58] His argument is not persuasive, largely because it is based on the dubious assertion that significant warning intelligence was not available prior to Pearl Harbor.[59] But if one *does* accept the idea that the main problem lies in a lack of intelligence, rather than an overabundance of it, then his conclusion appears logical: a better effort at collection should be able to produce better results. Although Levite does not focus on technology and changes that might be brought about by the information age, he does provide support for the next school of thought we will consider, the information age optimists.

The Information Age Optimist View

This second major school of thought holds that intelligence can be improved through the use of technology, in particular the tools of the information revolution. As in the orthodox school, there is a wide range of views among the writers and thinkers included here, and it would be unfair to characterize any of these theorists as starry-eyed optimists. But in general, they

[57] Ibid., 114-126.
[58] Ibid., 183-186.
[59] Richard Betts has provided a thorough critique of Levite's book, and Levite offers a response: Richard K. Betts, "Surprise, Scholasticism, and Strategy: A Review of Ariel Levite's *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987)," *International Studies Quarterly* 33, no. 3 (September 1989); Ariel Levite, "*Intelligence and Strategic Surprise* Revisited: A Response to Richard K. Betts's 'Surprise, Scholasticism, and Strategy'," *International Studies Quarterly* 33, no. 3 (September 1989).

share the view that intelligence can and should get better—that it can reduce the fog of war—if only the intelligence community would make better use of the tools available to it.

Joseph Nye and William Owens are among the most prominent information age optimists, arguing that improved intelligence is a significant part of what they call American's information edge: "Fusing and processing information—making sense of the vast amount of data that can be gathered—will give U.S. forces what is called dominant battlespace knowledge, a wide asymmetry between what Americans and opponents know."[60] They argue these improved capabilities will work against terror threats as well as against conventional military opponents. "Information has always been the best means of preventing and countering terrorist attacks, and the United States can bring the same kind of information processing capabilities to bear abroad that the FBI used domestically to capture and convict the terrorists who bombed the World Trade Center."[61]

The official U.S. military view is strongly in line with the information age optimists. *Joint Vision 2020* argues that "the ongoing 'information revolution' is creating not only a quantitative, but a qualitative change in the information environment that by 2020 will result in profound changes in the conduct of military operations."[62] Information superiority is seen as a key enabler of victory, but in order to do so it must be translated into superior decisions. New information technology, especially what is called a global information grid, will support warfighters and policy makers; while it will not eliminate the fog of war and can even add its own friction, on balance the U.S. military believes it will lead to decision superiority and better command and control.

[60] Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge," *Foreign Affairs* 75, no. 2 (March-April 1996): 23-24.
[61] Ibid.: 32-33. Although this analysis can rather easily be criticized today—after all, FBI capabilities clearly did not prevent either the first WTC bombing, or 9/11--their argument is still worth considering.
[62] U.S. Joint Chiefs of Staff Chairman, *Joint Vision 2020* (Washington, DC: GPO, 2000), 8.

There are relatively few academics among this school, and even these writers are generally not as optimistic as the military—which is perhaps understandable, as they are not primarily advocating a certain set of policies, but attempting to analyze them. Some, in fact, explicitly deny that the information age will improve intelligence. Walter Laqueur wrote in 1985, "The intelligence community has now used computers and related techniques for almost three decades, but few will argue that there has been a striking improvement in foreign intelligence during this period."[63]

But a number of thoughtful commentators believe that the capability of U.S. intelligence can be improved. Bruce Berkowitz, for example, a prominent proponent of better and more aggressive use of intelligence and information systems, argues: "The underlying problem is that the intelligence community has failed to keep up with changes in how modern society uses information and how information technology develops in modern society."[64] Michael Herman has expressed a rather sanguine view of American intelligence capabilities today: "Satellites' scope is ever-increasing, as is the capability of high-flying aircraft and drones. So too are the opportunities provided by the electronic world in which every detachment commander, insurgent leader, terrorist director, hostage-taker or international drug-dealer seems to have his mobile phone or communicate via the Internet."[65]

David Kahn, a prominent historian of intelligence, has expressed enthusiasm for the prospects of intelligence in the information age: "Today, the near blanketing of the theater of war with Buck Rogers collections devices . . . renders the far side of the hill almost as visible as the

[63] Laqueur, 315.

[64] Bruce D. Berkowitz, "Information Age Intelligence," *Foreign Policy* 103 (Summer 1996): 37. Note that although Berkowitz frequently advocates technological solutions, he also acknowledges that the intelligence community must address organizational and other problems; Bruce D. Berkowitz, "Better Ways to Fix U.S. Intelligence," *Orbis* 45, no. 4 (Fall 2001).

[65] Michael Herman, *Intelligence Services in the Information Age: Theory and Practice* (London: Frank Cass, 2001), 207.

near side."[66] He concedes that mistakes will still happen, but dismisses the "perennial issue" of sensors creating a problem by collecting more raw data than can be used.[67] Concerning Pearl Harbor, Khan takes a view similar to Levite's, arguing flatly that "American intelligence had failed."[68] The failure was not of analysis, as is commonly believed, but of collection. Wohlstetter may believe the failure was caused by too much information, "But she errs. There was a dearth of intelligence materials. Not one intercept, not one datum of intelligence ever said a thing about an attack on Pearl Harbor. There was, in Wohlstetter's terms, no signal to be detected."[69] Because the failure was in collection, the U.S. might have been able to foresee the attack if it had years before put spies in place, flown regular reconnaissance of the Japanese Navy, sailed intercept ships close to Japan, or recruited a network of naval observers to report on Japanese ship movements. Kahn argues that new technologies and intelligence methods will tend to make another Pearl Harbor less likely, but he believes they cannot preclude surprise attacks altogether.

David Steele is another thinker who appears to fit into the information age optimist school. Although he is best known as an advocate for open source intelligence (OSINT), he describes a broad vision of the threats facing America and the West in the 21st Century from a wide variety of non-traditional sources such as water scarcity, failed states, criminals, and terrorists. To deal with these threats, he argues, the intelligence community must realize that intelligence is much more than just secret information from spies and satellites; it also includes information that may be publicly, or at least semi-publicly, available. While Steele's views are

[66] David Kahn, "Toward a Theory of Intelligence," *Military History Quarterly*, Winter 1994, 96.
[67] Of note: in a later article Kahn continues to strike this optimistic tone, but cautions that cheap cryptographic systems pose a serious threat to intelligence. David Kahn, "An Historical Theory of Intelligence," *Intelligence and National Security* 16, no. 3 (Autumn 2001): 88.
[68] David Kahn, "The Intelligence Failure at Pearl Harbor," *Foreign Affairs* 70, no. 5 (Winter 1991/1992): 147.
[69] Ibid.: 147-148.

different from those of many intelligence analysts and scholars, he does appear to fit into the information optimist school through his belief that intelligence analysis can be improved through better use of information technology to automate investigations, translate documents, and integrate all-source data streams.[70]

Despite the writings of these optimists, however, the belief that intelligence can be significantly improved through the application of information technology remains relatively rare among scholars of intelligence, and it is somewhat surprisingly heard only rarely in the published work of intelligence professionals.[71] Some thinkers seem to have been initially in the optimist camp, but over time have moved toward the traditional view. A prominent example is Klaus Knorr, who in 1980 suggested we might in the future be able to rely on new systems to limit the incidence of surprise: “It is plausible, it seems to me, that certain strategic crises of the past could not have happened in the presence of these new warning systems. I imagine the Japanese attack on Pearl Harbor could not have happened, for example.”[72] But writing just a few years later, in 1983, he was considerably less optimistic. He argued that although technology would likely have made some surprises less possible—such as the Pearl Harbor attack—others would have occurred anyway. Providing warning of strategic surprise “is not only an exceedingly difficult task, it looks to be close to hopeless,” he wrote, unless statecraft somehow manages to improve.[73]

[70] See in particular his forward, written after 9/11, to Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World* (Oakton, VA: OSS International Press, 2001). See also Robert David Steele, "Crafting Intelligence in the Aftermath of Disaster," *International Journal of Intelligence and Counterintelligence* 15, no. 2 (Summer 2002).
[71] For example, an early but subdued example of the optimistic view among intelligence personnel is Thomas G. Belden, "Indications, Warning, and Crisis Operations," *International Studies Quarterly* 21, no. 1 (March 1977). Belden described the early efforts being made to improve the management of warning through the use of modern communications technology such as remote conferencing.
[72] Handel, "Avoiding Political and Technological Surprise in the 1980's," 116. Knorr’s comment was part of a discussion in this volume following Handel’s article.
[73] Klaus Knorr, "Lessons for Statecraft," in *Strategic Military Surprise: Incentives and Opportunities*, ed. Klaus Knorr and Patrick Morgan (New Brunswick, NJ: Transaction Books, 1983), 256.

Another analyst who appears to have moved from the optimist to a largely pessimistic view is Loch Johnson. In an early article he argued that most intelligence theorists—both orthodox pessimists such as Kam, and analysts such as Levite who focus on the problem of poor intelligence collection—underestimate "the amazing capabilities of new high-tech intelligence hardware."[74] While new intelligence systems may not eliminate surprise, they can help stabilize relations between the superpowers, and "as the skies and the lands continue to fill with mechanical eyes and ears, the risks of surprise are likely to diminish further."[75] A few years later, he wrote that U.S. commanders in the 1991 Gulf War "enjoyed a better understanding of the battlefield situation than any leaders in the history of armed conflict," a result largely of high tech intelligence systems.[76] But by 2000, Johnson seemed to have moved into the orthodox school, chiding U.S. intelligence for being too fascinated with technological tools and describing the "paradox of rejection" in which failures occur often as a result of policymakers' "unwillingness to accept the facts and judgments of the intelligence experts."[77]

The Terrorism Analysis View

The third school of thought is found among analysts of terrorism. Although there are many differences of opinion among experts and analysts on terrorism, most scholars and analysts in this field do appear to share several general assumptions regarding intelligence. First, that terrorism presents a particularly difficult problem for intelligence (as well as for policy and operations). Because terrorist groups are often small, dispersed, and do not rely on the large

[74] Loch K. Johnson, "Challenges of Strategic Intelligence," *Intelligence and National Security* 5, no. 3 (July 1990): 224.
[75] Ibid.
[76] Johnson, "Analysis for a New Age," 658.
[77] Loch K. Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security* (New York, NY: New York University Press, 2000), 191. He also explains his views in Loch K. Johnson, "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy* 22, no. 1 (January-March 2003): 6-12.

infrastructure of a conventional state-based threat, intelligence is limited in its ability to use traditional tools and techniques to gain insight on terrorist intentions and capabilities.

Second, the primary limitation for intelligence is its lack of human intelligence (HUMINT) capability. For example, terrorism experts even today frequently complain that former CIA Director Stansfield Turner turned the community away from HUMINT and toward technical intelligence decades ago. The implication of these criticisms, often unstated, is that improvements in information technology are not likely to result in better intelligence against terrorist threats. Third, terrorist attacks are not likely to be preceded by tactical warning. The Crowe Commission, for example, found this to have been the case in the Kenya and Tanzania bombings, and it criticized the intelligence and policy communities for having relied too much on tactical intelligence to determine threat levels.[78]

And fourth, in a point related to the stress on human intelligence, writers on terrorism tend to pay relatively little attention to the importance of intelligence analysis, focusing instead on the need for better collection, particularly from human sources. Not that intelligence in general isn't considered important: the National Commission on Terrorism, for example, concluded that "no other single policy effort is more important for preventing, preempting, and responding to attacks" than intelligence.[79] But most discussions of intelligence and terrorism have stressed the need for more and better collection, in the form of HUMINT, and for increased

[78] *Report of the Accountability Review Board on the Embassy Bombings in Nairobi and Dar Es Salaam on August 7, 1998* (ADM William J. Crowe (ret), Chairman, available at www.fas.org/irp/threat/arb/board_overview.html, 1999). On the lack of tactical warning, and the problem this poses for intelligence, see also Paul R. Pillar, "Fighting International Terrorism: Beyond September 11th," *Defense Intelligence Journal* 11, no. 1 (Winter 2002); John Prados, *America Confronts Terrorism: Understanding the Danger and How to Think About It* (Chicago: Ivan R. Dee, 2002), 275.

[79] National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Report of the Congressionally mandated commission chaired by L. Paul Bremer III, June 7, 2000, available at: w3.access.gpo.gov/nct), 7.

counter-terrorist operations in the form of counter-intelligence and covert action.[80] James B. Motley presents this conventional view in arguing “It is human intelligence—clandestine agents, informers—that is the key to coping with terrorism.”[81] The importance of HUMINT has been emphasized by analysts both of intelligence, such as Richard Betts, and of terrorism, such as Paul Pillar.[82]

Although the belief in the importance of human intelligence in fighting terrorism has become conventional wisdom, it should be noted that not all analysts dismiss the gain from technical intelligence. A strong cautionary—and not disinterested--voice is that of Stansfield Turner, who has written of the claims that human intelligence is the only way to discern intentions: “As a general proposition, that is simply not true.”[83] Communications intercepts, he wrote, may be even more useful in discerning intentions than second-hand HUMINT reports.

The debate over the importance of human intelligence continues in the information age. Ian O. Lesser has suggested that while HUMINT remains important, the increasing reliance by terrorists on information technology today introduces new possibilities for surveillance.[84] Chris Dishman, on the other hand, argues that human intelligence is still the best—and that it doesn’t require operatives to penetrate to the core of the terrorist group, which is often seen by critics as

[80] A few writers and official reports have, however, stressed the importance of analysis in the fight against terrorism. See for example the Report to the President from the Secretary of Defense based on the Downing assessment of the Khobar Barracks bombing, and retired Admiral Harold W. Gehman’s report on the attack on the USS Cole, both in Prados, 290-291 and 353. See also Robert L. Hubbard, "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements," *Defense Intelligence Journal* 11, no. 1 (Winter 2002); Wayne A. Kerstetter, "Terrorism and Intelligence," *Terrorism: An International Journal* 3, no. 1-21979).

[81] James Berry Motley, "Coping with the Terrorist Threat: The U.S. Intelligence Dilemma," in *Intelligence and Intelligence Policy in a Democratic Society*, ed. Stephen J. Cimbala (Dobbs Ferry, NY: Transnational Publishers, Inc, 1987), 169.

[82] Richard K. Betts, "Fixing Intelligence," in *Terrorism and Counterterrorism*, ed. Russell D. Howard and Reid L. Sawyer (Guilford, CT: McGraw-Hill/Dushkin, 2003), 475; Paul R. Pillar, *Terrorism and U.S. Foreign Policy* (Washington: Brookings, 2001), 111. See also Mark V. Kauppi, "Counterterrorism Analysis 101," *Defense Intelligence Journal* 11, no. 1 (Winter 2002).

[83] Stansfield Turner, "Intelligence for a New World Order," *Foreign Affairs* 70, no. 4 (Fall 1991): 154. It is worth noting that Turner is not completely critical of HUMINT, arguing here that it remains necessary, but should be done better, such as through more extensive use of non-official cover.

[84] Ian O. Lesser, *Countering the New Terrorism* (Santa Monica, CA: RAND, 1999), 134.

a requirement beyond the capability of most intelligence services. Sources on the periphery, Dishman believes, can also provide useful intelligence, much as informants are used successfully by law enforcement.[85]

Other analysts provide a more balanced discussion of the relative merits of HUMINT, SIGINT, and other sources. John Deutch and Jeffrey Smith, for example, describe the contributions that can be made by various sources, and argue that human and technical intelligence can augment and support one another, making both stronger: “human intelligence is not a silver bullet than can be separated from other intelligence activities and improved overnight.”[86] Schlomo Gazit and Michael Handel describe the value that can be gained from the interrogation of captured terrorists, and Campbell and Flournoy provide a useful discussion of the limitations of all sources of intelligence in the fight against terrorism.[87]

The limitations of human intelligence are not the only problems facing intelligence in grappling with the problem of terrorism. Even before the 9/11 attacks, Bruce Berkowitz argued that much of the problem lies in the bureaucratic nature of the intelligence community, which makes it less able to adapt to new threats.[88] Bruce Hoffman has provided a useful review of the problems intelligence has with terrorism, including the observation that modern, religious, and amateur terrorists leave small footprints that are hard to detect.[89] In one important aspect, Hoffman’s views appear to be in line with the orthodox school: he believes the main problem is

[85] Chris Dishman, "Trends in Modern Terrorism," *Studies in Conflict and Terrorism* 22, no. 4 (October-December 1999): 360.

[86] John Deutch and Jeffrey H. Smith, "Smarter Intelligence," *Foreign Policy* (January/February 2002): 66.

[87] Kurt M. Campbell and Michele A. Flournoy, *To Prevail: An American Strategy for the Campaign Against Terrorism* (Washington, DC: CSIS Press, 2001), 86-88; Schlomo Gazit and Michael Handel, "Insurgency, Terrorism, and Intelligence," in *Intelligence Requirements for the 1980s: Counterintelligence*, ed. Roy Godson (New Brunswick, NJ: Transaction Books, 1980). Another balanced source on the value of HUMINT is Frank J. Cilluffo, Ronald A. Marks, and George C. Salmoiraghi, "The Use and Limits of U.S. Intelligence," *The Washington Quarterly* 25, no. 1 (Winter 2002). For a good discussion of the merits of the various “Int’s,” see Shulsky and Schmitt.

[88] Berkowitz, "Better Ways to Fix U.S. Intelligence."

[89] Bruce Hoffman, "Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post-Cold War Era," *Intelligence and National Security* 11, no. 2 (April 1996).

that intelligence officials have difficulty convincing authorities that a threat exists. But in general Hoffman, and other writers who specialize on terrorism, see it as a uniquely difficult problem for intelligence—and one unlikely to be solved easily.[90]

Hypotheses Based on These Theories

If these theories are correct in their analysis of intelligence failure and the reasons why even the most capable intelligence services and military forces can be surprise, what do they suggest we should find in studying cases of failure and surprise due to terrorism? The following are hypotheses derived from each of these schools of thought, which will be tested in the next section against the case study of the 1983 Beirut bombing.

The orthodox school. This is the richest school of thought, and suggests the largest number of testable hypotheses.

1. Despite advances in information technology and intelligence systems, the ability of intelligence to warn against terrorist attacks is not likely to get any better with time.

2. After terror attacks occur, numerous indicators will be found, but these will have been missed because of the classic problems of intelligence analysis—in particular the signal to noise ratio, and psychological or cognitive limitations on human analysts and decision makers.

3. The involvement of nonstate actors in terrorist attacks is likely to compound the cognitive problems for intelligence, because analysts will find it more difficult to understand the enemy and anticipate his future actions.

4. Advances in information technology will tend to increase the amount of noise in the system, making it even harder for analysts to find the indicators of terrorist attacks. This is

[90] For a useful recent review of the problems intelligence faces with terrorism see chapter 7, “Intelligence: The Long Pole in the Tent,” in Campbell and Flournoy, 77-89. Also see Bruce D. Berkowitz, "Intelligence and the War on Terrorism," *Orbis* 46, no. 2 (Spring 2002); Fritz Ermath, "Signs and Portents: The 'I & W' Paradigm Post - 9/11," *The National Interest*, October 2 2002.

because the chief difficulty in intelligence is not in getting information, but in analyzing it and getting decisionmakers to understand it and take action.

4. The principal sub-school of thought among orthodox analysts suggests that the primary responsibility for the failure to anticipate terrorist attacks will lie with policy makers, who will be unreceptive to the intelligence they receive. Others suggest the fault will lie principally with the intelligence community itself, while the third sub-school suggests that the reasons for disaster will be terrorist use of surprise and deception.

The information age optimists.

1. Even these thinkers would not be so rash as to argue that the intelligence community will be able to use improved technology to foresee and prevent most future terrorist attacks. But this view does suggest that improved technology should aid in the detection of attack indicators, and that even in cases where attacks do occur, advanced information processing and intelligence technology should make post-attack analysis and investigation easier than it had been in an earlier age.

2. The main problem for the intelligence community will be collection, not analysis, of intelligence on terrorist capabilities and intentions.[91]

The view of terrorism analysts. Because these theories are developed based on analysis of terrorist groups and attacks, we might expect that they will fit our case study quite well. The key question is whether or not these theories can explain the failure of intelligence to anticipate terror attacks better than the other two schools of thought.

[91] We should note that even if this school is correct, new technology might not translate into intelligence success for two major reasons. First, the U.S. intelligence community may not invest sufficiently in advanced technology systems; and second, even if intelligence does improve, decision makers may still resist or misuse the intelligence they are given.

1. Although there may be strategic indicators of terrorist threats, we should expect to see fewer *tactical* intelligence indicators of terrorist attacks.

2. Technical sources of intelligence will be less useful against terrorist threats than they are against conventional threats.

3. The most useful source of intelligence—possible the only significant source—is human intelligence.[92]

[92] This hypothesis is especially difficult to test, both because HUMINT is extremely sensitive, and because it is tempting to claim after every intelligence failure that it could have been avoided, if only the intelligence community had devoted itself to developing human sources. Given this limitation, we must look for indicators either that human intelligence has in fact been useful against terrorist threats, or that other sources have *not*.

3. The Marine Barracks Bombing in Beirut

On October 23, 1983, a truck laden with the equivalent of over 12,000 pounds of TNT crashed into the compound of the U.S. contingent of the Multinational Force at Beirut International Airport, penetrating the Battalion Landing Team Headquarters building and detonating, killing 241 U.S. military personnel. Almost simultaneously, a similar truck bomb exploded at the French MNF headquarters, killing some 56 soldiers. These attacks had been preceded by a car bomb attack on the U.S. Embassy in Beirut on April 18, 1983, that killed 17 U.S. citizens and over 30 others. And they were followed on September 20, 1984, by a third attack that destroyed the newly occupied U.S. Embassy Annex in East Beirut and killed two Americans and at least ten Lebanese.

How could such a series of devastating attacks have taken place? The Beirut bombings have been studied by an official investigating commission, several Congressional committees, and numerous individual writers and scholars. This chapter will review the results of these studies, and consider whether or not these tragedies can be explained by the theories of intelligence failure set out in section 2.[1]

[1] The official investigation was conducted by the Long Commission, named for its chairman, and its report is U.S. Department of Defense, *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983* (Washington: GPO, 1984). The House Armed Services Committee examined the circumstances behind the bombing, and its report is U.S. Congress, House, "Adequacy of U.S. Marine Corps Security in Beirut," (Committee on Armed Services, Investigations Subcommittee. Washington: GPO, December 19, 1983). The House investigation hearings were published separately: U.S. Congress, House, "Review of Adequacy of Security Arrangements for Marines in Lebanon and Plans for Improving That Security," (Committee on Armed Services, Investigations Subcommittee, November-December 1983. Washington: GPO, 1985). The other most useful studies of the bombing are Benis M. Frank, *U.S. Marines in Lebanon 1982-1984* (Washington DC: History and Museums Division, Headquarters U.S. Marine Corps, 1987); Glenn P. Hastedt, "Intelligence Failure and Terrorism: The Attack on the Marines in Beirut," *Conflict Quarterly* VIII, no. 2 (Spring 1988); David C. Martin and John Walcott, *Best Laid Plans: The Inside Story of America's War Against Terrorism* (New York: Harper & Row, 1988); Shaun P. McCarthy, *The Function of Intelligence in Crisis Management: Towards an Understanding of the Intelligence Producer-Consumer Dichotomy* (Aldershot, England: Ashgate, 1998); Philip Taubman and Joel Brinkley, "The U.S. Marine Tragedy: Causes and Responsibility," *New York Times*, December 11 1983.

For a personalized account, see Eric Hammel, *The Root: The Marines in Beirut August 1982-February 1984* (San Diego, CA: Harcourt Brace Jovanovich, 1985). An account centering on bureaucratic and political issues is Ralph

The Long Commission findings

The Department of Defense commission that investigated the October 23 Marine barracks bombing[2] found that the attack "was tantamount to an act of war using the medium of terrorism."[3] The commission's findings concerning intelligence appeared to follow the conventional view among terrorism analysts that a lack of human intelligence (HUMINT) was the primary intelligence failure. The report stated that specific data on the terrorist threats, "data which could best be provided by carefully trained intelligence agents," could have enabled the U.S. commander to better prepare for and blunt the effectiveness of the attack. Part of the reason why effective HUMINT support was not available was due to decisions taken previously to reduce HUMINT worldwide, and the report stated flatly, "The lesson of Beirut is that we must have better HUMINT to support military planning and operations."[4] The Commission recommended that the Secretary of Defense establish an all-source terrorism intelligence fusion center to support military commanders, and that the policy on HUMINT support be re-examined.

While these stark conclusions were listed in the report's executive summary, the body of the report painted a more complex picture of uncoordinated intelligence and threat assessment: "It is difficult to overstate the magnitude of the intelligence problem in a milieu where high casualty terrorist acts are relatively easy to perpetrate yet hard to stop."[5] Intelligence provided

A. Hallenbeck, *Military Force as an Instrument of U.S. Foreign Policy: Intervention in Lebanon, August1982-February 1984* (New York: Praeger, 1991). For a look at the national-level debates between the intelligence and policy communities, see David Kennedy and Leslie Brunetta, *Lebanon and the Intelligence Community* (Harvard University Kennedy School of Government Case C15-88-859.0, 1988). (This last case study is also available in an abridged version, as David Kennedy and Leslie Brunetta, "Lebanon and the Intelligence Community: A Case Study," *Studies in Intelligence* 37, no. 5 (nd 1994).

The first Embassy bombing is discussed in Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism* (NY: Crown Publishers, 2002). Baer, a former CIA DO officer who was not in Beirut at the time of the April 1983 bombing, says it became "a lifelong obsession" of his to find the perpetrators.

[2] Although the building attacked was actually the Battalion Landing Team headquarters, and thus more than a barracks, it has come to be referred to as the "Marine barracks," and I have adopted this convention.

[3] U.S. Department of Defense, 4.

[4] Ibid., 5.

[5] Ibid., 62.

over 100 warnings of car bombings between May and 23 October, but specific threats seldom materialized, and "there was no specific intelligence on the where, how and when of the 23 October bombing."[6]

There had been an indication in the earlier Embassy bombing that those terrorists had employed a particularly dangerous method of attack, using a gas-enhancement process along with explosive-activated gas bottle bombs. An FBI report said this technique was simple to employ and resulted in a sizeable blast multiplier effect, but this report stayed in FBI, CIA and State channels. The Long Commission report stated that if DOD had been given this data about the 18 April bombing, the USMNF commander might have better understood "the catastrophic potentialities arrayed against him."[7] The Marine barracks bombing was, however, much larger than the earlier Embassy explosion. The Commission reported that "FBI forensic experts have stated that it was the largest non-nuclear blast they have ever examined, perhaps six to nine times the magnitude of the Embassy bombing."[8] An FBI Special Agent from the explosives unit later testified to the House Armed Service Committee that as "a very conservative estimate" the explosion had an equivalent yield of 12,000 pounds of TNT.[9]

The Long Commission reported that two surveys had been conducted prior to the bombing to determine whether security measures were appropriate. One survey was conducted by DOD from 13-27 May looking at intelligence support to the U.S. Multinational Force (MNF), but the section of the Commission report that lists this survey's recommendations is blank—suggesting the list of recommendations did not survive a security review process. More information is available in the commission report about a survey conducted by the European

[6] Ibid., 63.
[7] Ibid., 65.
[8] Ibid., 63.
[9] U.S. Congress, "Review of Adequacy of Security Arrangements for Marines in Lebanon and Plans for Improving That Security," 402.

Command (EUCOM) Headquarters Office of the Special Assistant for Security Matters. The director of that office evaluated the 18 April bombing, and concluded that the Embassy bombing was the prelude to a more spectacular attack, for which the U.S. military forces presented the "most defined and logical target."[10] As a result, the Office of Military Cooperation dispersed its personnel in Beirut in order to reduce their attractiveness as a target. But that survey had not been chartered to look at Marine security, and made no comments or recommendations concerning the threat to Marines.

The Long Commission report describes a U.S. force that had been focused on its difficult mission, and which had never even considered the possibility of such a massive truck bomb attack. Even though the U.S. Embassy had been attacked only months before, and despite receiving regular reports of car bomb and other terrorist threats, the Marines believed they were secure: "The USMNF units at the airport, behind their guarded perimeter, perceived the terrorist threat as secondary and could not envision a terrorist attack that could penetrate their base and cause massive destruction."[11] And even after the attack, when the Commission members visited Beirut, they found that insufficient security measures were being taken, suggesting just how serious the lack of appreciation for the terrorist threat was among the Marines in Beirut.

The House Armed Services Committee Investigation

The most detailed examination of the intelligence situation prior to the Marine bombing appears to be the investigation conducted by the House Armed Services Committee (HASC), which resulted in an extensive committee report and several hundred pages of testimony. Although this investigation looked at all aspects of the bombing and aftermath, we will focus on

[10] U.S. Department of Defense, 130.
[11] Ibid., 131.

the sections of the report and testimony concerning intelligence, which provide more detail than is available in the Long Commission report.[12]

The HASC report found that "The MAU [Marine Amphibious Unit, the overall Marine command] in Lebanon did not receive adequate intelligence support dealing with terrorism. Serious intelligence inadequacies had a direct effect on the capability of the unit to defend itself against the full spectrum of threat." But responsibility for the failure was shared with the chain of command, which failed to consider the possibility of a large, bomb-laden truck, despite the fact that a security survey appeared to have addressed it: "The failure is particularly inexplicable in view of numerous other threats considered . . . and in view of the fact that an intelligence survey in the summer of 1983 recommended that *trucks* be visually inspected for explosive devices."[13] This survey is described as a counterintelligence survey conducted for the MAU commander, and it is not clear whether this was the same survey whose findings were blanked out of the Long report.

The committee report identified two major problems with intelligence: the Marines did not have the ability to analyze the massive amount of data coming in, and the intelligence that was available was generally non-specific and of little use in planning defenses.[14] But still, the report suggested that the intelligence community could have done more to support the Marines. "In spite of the fact that Lebanon is often described as the 'car bomb capital of the world,' and in view of all the terrorist training suspected of being conducted there, the subcommittee found no

[12] The committee's investigations subcommittee produced a "Summary of findings and Conclusions," as well as a full report, which are published together as a committee print; the committee's hearing testimony has been printed separately. In addition, the summary is reprinted as "Adequacy of U.S. Marine Corps Security in Beirut," *Terrorism: An International Journal* 7, no. 3 (nd 1984). It is also excerpted on at least one web site, hyperwar.com.
[13] U.S. Congress, "Adequacy of U.S. Marine Corps Security in Beirut," Summary p 2. Emphasis added.
[14] Ibid., 55.

evidence of a concerted effort by any intelligence organization to bring terrorism experts together to support the marines."[15]

Captain Morgan France, USN, the commander of the Naval forces offshore supporting the Marines (Task Force 61), testified, "The problem was the intelligence basically was the sky-is-falling type of information. I think that that is intelligence, but that is on the ragged edge of intelligence," and it wasn't specific enough to act on.[16] An intelligence officer on his staff testified to the subcommittee that "In a situation like this, you can never afford to overlook anything, and if a truck was not considered, why it was not considered, I can't tell you." But when asked if this was a failure of intelligence, he answered that it would have been a failure if there had been indications that a truck was to be used, but he had only seen reports on cars.[17]

Colonel Timothy J. Geraghty, the commander of the 24th MAU at the time of the bombing, testified that he believed the intelligence community was partly to blame for not indicating that a threat of this magnitude existed. "Obviously, we had no indication that we would have a threat of this magnitude, both in delivery and in explosive force," he said. "So I guess if you have to point the finger at failure, part of it is intelligence because we weren't told."[18]

Geraghty's view was supported by the testimony of General P. X. Kelly, Commandant of the Marine Corps, who said that "car bombs—and I emphasize car bombs—were viewed as a likely form of attack,"[19] and that between June 1 and the 23 October attack the Marines had received reports of roughly one hundred possible car bombs. When asked whether or not a

[15] Ibid., 56.
[16] U.S. Congress, "Review of Adequacy of Security Arrangements for Marines in Lebanon and Plans for Improving That Security," 491.
[17] Ibid., 159, 163. This officer was CDR Joel Foote, staff intelligence officer for CTF 61, which was the Naval task force off shore supporting the Marines in Beirut.
[18] Ibid., 559-560.
[19] Ibid., 20.

commander should have anticipated the attack, he answered no, that the two attacks were too different. "Both of these instances involve a terrorist bombing from a motor vehicle, but that is where the similarity ends. The delivery systems were totally different, as was every other aspect of the two incidents."[20]

What Intelligence was Available Prior to the October Attack?

Although an unclassified study such as this cannot hope to provide a full account of what intelligence information was—or should have been—available to the Marines prior to the October bombing, the record of the many official and unofficial investigations into the incident suggests that the picture we have is fairly complete. As Benis M. Frank has described in a study conducted for the Marine Corps history office, during the spring and summer of 1983 the Marines were extremely concerned about the terrorist threat, but also frustrated that they did not have enough intelligence. Even prior to the Embassy bombing in April, "The MAU's primary concern remained the terrorist threat. The primary need was for intelligence, more intelligence, and still more intelligence."[21] The Marines had from the beginning realized they faced an imminent terrorist threat, and while they recognized HUMINT was invaluable, they knew they didn't have enough of it. The BLT Commander in May, Lt Col Anderson, was very concerned about the shortfall in HUMINT: "My 2 [intelligence officer] can tell me what's going on in the Bekaa Valley and he can tell me what's going on in Tripoli . . . . We have no foggy idea of what's going on right outside our gate."[22]

Although the Marines expected any further attack would come from a car bomb such as was used against the Embassy, we have seen that at least one survey team recommended precautions be taken concerning trucks, as well. Further information about security and

[20] Ibid., 25.
[21] Frank, 55.
[22] Ibid., 56. This interview was conducted May 25 1983.

intelligence assist visits is available from David C. Martin and John Walcott, whose book *Best Laid Plans: The Inside Story of America's War Against Terrorism* provides details and interview data not available elsewhere. They report that Colonel William Corbett, special assistant for security matters for EUCOM Headquarters, had inspected the defenses for the 120 American soldiers assigned to the Office of Military Cooperation (OMC). He reported on April 27 that "Following Amembassy attack, U.S. military forces represent the most defined and logical terrorist target. . . . U.S. interests in Lebanon can expect an attack more spectacular than the action against the U.S. embassy."[23] Martin and Walcott also report that DOD dispatched a small team from a secret organization called the Intelligence Support Agency, which recommended, among other things, the creation of a fusion center for analysis of terrorist plots. EUCOM's response, they report, was to assign an intelligence officer to the OMC, but no increased security measures appear to have been taken on the part of the Marine force.[24]

A *New York Times* investigation reported that, according to intelligence officials, the CIA's top-level intelligence product the *National Intelligence Daily* contained several reports on threats in Beirut during the summer and fall of 1983, including one published on October 20 that specified American forces in Beirut might soon be the target of a major terrorist attack.[25] In addition, Kennedy and Brunetta write that a Special National Intelligence Estimate (SNIE) was published in Washington in October before the bombing. It described the situation in Lebanon as hopeless, but evidently concentrated on the overall political situation, not the threat to the U.S. forces on the ground.[26]

[23] Martin and Walcott, 108.

[24] Ibid., 109. They also report that another ISA team was sent after the October bombing, but without the knowledge of EUCOM Headquarters, and the Deputy CINCEUR, Gen Richard Lawson, ordered them out of Lebanon when he learned they were there; 133-134.

[25] Taubman and Brinkley. The *New York Times* report is cited in Hastedt's book, and I am grateful to him for guiding me toward it.

[26] Kennedy and Brunetta, *Lebanon and the Intelligence Community*.

The 1984 Embassy Bombing

While studies of the Marine barracks attack suggest it occurred as a result of a combination of intelligence and operational failings, the third bombing in this series has been described as a clear operational and command failure: the necessary security measures had simply not been put into place. This was the conclusion of an examination by the Senate Foreign Relations Committee staff, which issued a report blaming the attack on the failure of embassy personnel who felt the new location in East Beirut was safe. As a result, they failed to ensure that simple movable vehicular barriers, which were available but not yet installed, were complete before moving in to the recently occupied building.[27]

Even in this case, the intelligence prior to the attack was by no means perfect; it was frustratingly vague, and did not provide credible identification of a threat against a certain target at a specific time. Following the 1984 bombing, news accounts reported that a Defense Intelligence Agency (DIA) report had warned of the attack ahead of time. The Senate report found that although the DIA report had supposedly been prepared to support the Defense Attaché Office (DAO) in Beirut, at the time of the bombing the Attaché had not seen it, nor had the appropriate State Department security officials. But in any case, the staff report concluded, the DIA report was too general to have been of little use even if it had been seen: "Even if circulated to those who were its proper recipients, the report's potential contribution to the security process is difficult to conceive. Based upon a July visit by a DIA team to Beirut, the report contained no intelligence findings or specific recommendations on security measures, and indeed did little

[27] U.S. Congress, Senate, *The Security of American Personnel in Lebanon* (Committee on Foreign Relations, Staff Report, October 1984. Washington: GPO, 1984), 9. Although the building was officially known as the Embassy Annex, it housed the majority of embassy employees.

more than recite what all concerned already knew: that Beirut is a dangerous place and buildings such as the Baaklini Annex are vulnerable to terrorist attack."[28]

But even if the intelligence support prior to the 1984 bombing was not perfect, available records suggest it was considerably better than that provided to the Marines the year before. The House Permanent Select Committee on Intelligence also studied the 1984 bombing, and issued a report on the performance of the U.S. intelligence community in this incident.[29] The report concluded that unlike the situation reported by the Long Commission, in which the local commander was inundated by intelligence reports that were of little use, in this case there were several specific threat reports that highlighted the danger of terrorist attacks. The visit in July 1984 by the DIA security team, the report stated, "found the threat to the new U.S. Embassy facilities in both East and West Beirut to be 'exceedingly high.'"[30] This assessment had been conveyed both to Embassy officials in Beirut and to the State Department upon the return of the team to Washington. Overall the intelligence community performance was considered adequate, but the committee reported it was "distressed that intelligence contributions were not given more attention by the State Department." The report continued, "In particular, it is the view of the Committee that the probability of another vehicular bomb attack was so unambiguous that there is no logical explanation for the lack of effective security countermeasures at the East Beirut annex to thwart such an attack."[31] In what may have been a reference to the DIA report, *The Washington Post* reported on October 18, 1984, that the U.S. government had received specific

[28] Ibid., 10.

[29] U.S. Congress, House, *U.S. Intelligence Performance and the September 20, 1984, Beirut Bombing* (Permanent Select Committee on Intelligence, October 3, 1984. Washington: GPO, 1984).

[30] Ibid., 3.

[31] Ibid., 4.

intelligence warnings ahead of time that either the U.S. Ambassador's residence or the Embassy Annex would be targeted.[32]

Of note, Stansfield Turner has written that this bombing demonstrated how technical intelligence can provide clues as to an opponent's intentions. Satellite photos taken before the bombing, according to Turner, showed a mock-up of the annex and its defenses had been built, and terrorists had practiced driving trucks through them, but this was overlooked.[33] Shaun McCarthy describes a similar situation prior to the first Embassy bombing in 1983, stating that imagery indicated a mock-up of the embassy at a terrorist training base in the Bekaa Valley, but imagery analysts were not aware enough of the situation in Beirut to realize the significance of this information.[34]

The Lessons of Beirut

Surprisingly, the intelligence community has largely escaped serious criticism for the series of disasters in Beirut. Analysts have either blamed the U.S. political and bureaucratic forces that put the Marines in an impossible situation, or found it to be mostly a lesson for the operational chain of command. Lt Gen Bernard Trainor took the latter position in 1996, when he testified before a Senate Select Committee on Intelligence hearing that looked for lessons in comparing the Beirut experience with the just-occurred Khobar Towers bombing: "I have to say to myself, do we never learn?"[35] Edward Luttwak has taken a similar approach, arguing strongly

[32] Cited in Motley, 175 note 20. Motley has also discussed the 1984 Embassy attack in James Berry Motley, "International Terrorism: A Challenge for U.S. Intelligence," *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986).
[33] Turner: 154-155.
[34] McCarthy, *The Function of Intelligence in Crisis Management: Towards an Understanding of the Intelligence Producer-Consumer Dichotomy*, 112-113.
[35] U.S. Congress, Senate, *Saudi Arabia and Beirut: Lesson Learned on Intelligence Support and Counterterrorism Programs* (Select Committee on Intelligence, Hearings July 9, 1996. Washington: GPO, 1996), 4.

that the Beirut disaster revealed deep structural defects in our military institutions.[36] Some analysts have derived lessons from Beirut for the study of terrorism in general; Frederic Hof, for example, has argued that the bombing was not an act of terrorism, "but an unconventional military assault against a military target."[37]

One perceptive analyst, Daniel P. Bolger, has described three possible explanations for the failure in Beirut. Although he does not focus on intelligence support, these explanations all fit within the mainstream intelligence theories we have considered. The first explanation, offered by Secretary of Defense Casper Weinberger and Marine Corps Commandant P. X. Kelley, echoes the "no fault" explanations associated with mainstream theorists such as Betts and Handel. Military leaders at the time, Bolger writes, "explained the disaster as an unconventional bolt out of the blue, unanticipated by rational men who had done their best to prepare themselves for more ordinary direct and indirect fire threats. . . . In such a view, the exceptional nature of the attack made defense impossible, and hence, no officers were held accountable." If anyone was at fault, it was the enemy—certainly not the American forces or their leaders"[38]

Bolger describes the second explanation as held by Eric Hammel and others who blame the civilian leadership for giving the Marines a mission a rules of engagement that turned them into easy targets. "In this interpretation, the MAU leadership had been placed in a hopeless situation, fraught with perils, with both hands tied. Diplomats, civilian security advisers, and other nonmilitary decision makers and staffers supposedly hung the marines out on a limb and then allowed "terrorists" to saw off that branch."[39]

[36] Edward N. Luttwak, *The Pentagon and the Art of War* (NY: Simon and Schuster, 1984).
[37] Frederic C. Hof, "The Beirut Bombing of October 1983: An Act of Terrorism," *Parameters* XV, no. 2 (Summer 1985): 67.
[38] Daniel P. Bolger, *Americans at War, 1975-1986: An Era of Violent Peace* (Novato, CA: Presidio, 1988), 238-239.
[39] Ibid., 239.

But Bolger believes neither of these common explanations is sufficient—it is not enough to blame either the enemy, or the civilian leadership. Instead, "it appears that the greatest part of the responsibility for this unfortunate incident rests squarely on the shoulders of the 24th MAU and BLT 1/8 commanders. Their misapprehension of the mission, incomplete deployment and defensive preparations, and permission of deviations from established security regimens certainly exacerbated difficult conditions and expedited the work of a resourceful enemy."[40]

Most academics who have studied the question of intelligence failure in the Marine barracks bombing agree with the official studies that avoid strong criticism of the intelligence community. Glenn Hastedt concluded that while there were numerous failings in tasking, collection, and processing of information, "Far more significant were the attitudes and actions (or lack of action) of the consumers of intelligence."[41] David Kennedy and Leslie Brunetta studied the views of the national-level intelligence community, in particular the CIA, and found that CIA analysts had been attempting to warn all along that the U.S. policy in Lebanon was doomed to fail.[42] Shaun McCarthy drew similar conclusions, finding that the failings lay largely in a lack of interaction between policymakers and analysts, especially at the Washington level. The problem was compounded by the physical distance between the various intelligence centers that were responsible for supporting the Marines in Beirut, and by the "bureaucratic labyrinth" that intelligence reports had to go through before reaching consumers.[43]

A few analysts, including McCarthy, have argued that the failure of Beirut suggests the intelligence community must become more proactive, engaging in what is known as

[40] Ibid., 239-240.
[41] Hastedt, "Intelligence Failure and Terrorism: The Attack on the Marines in Beirut," 21.
[42] Kennedy and Brunetta, *Lebanon and the Intelligence Community;* Kennedy and Brunetta, "Lebanon and the Intelligence Community: A Case Study."
[43] McCarthy, *The Function of Intelligence in Crisis Management: Towards an Understanding of the Intelligence Producer-Consumer Dichotomy*, 118-119, 128.

"opportunity analysis." McCarthy writes that while tactical, specific intelligence on terrorist intentions may have been nearly impossible to collect, the intelligence community could have and should have made a better effort to make a comprehensive socio-political estimate of the situation in Lebanon, even though policy makers did not ask for one. The analysts were set in the traditionalist approach of policy-intelligence relations, with a mindset of not speaking unless spoken to; but if they had followed a more activist approach, McCarthy believes, "history may have been different."[44]

James Motley has made a similar argument, that the primary lesson from the 1984 Beirut bombing is that the U.S. government and the intelligence community must take a more pro-active stance, increasing the role played by HUMINT and emphasizing counter-terrorist operations. That bombing not only demonstrated the difficulty of deterring terrorism, "but, more importantly, reflected the U.S. government's seeming inability and lack of urgency to mount a concerted, coordinated, sustained, offensive antiterrorist effort."[45]

Explaining the failure

Which of the theories of intelligence failure seems to best explain the disaster in Beirut? As we have seen, the official investigations and several other studies seem to confirm the hypotheses that our first school, orthodox theory, suggested we would find:

- Numerous indicators of the terrorist threat were present, but were missed;
- The unconventional nature of the non-state terrorist threat appeared to confound the Marine commanders, who failed to understand what they were facing and continued to prepare for a conventional threat;

[44] Ibid., 140.

[45] Motley, "International Terrorism: A Challenge for U.S. Intelligence," 85. He makes the same argument in Motley, "Coping with the Terrorist Threat: The U.S. Intelligence Dilemma."

- Information technology failed to help, and may instead have overwhelmed analysts and decision makers;
- And while the intelligence community did the best it could in a difficult situation, collecting and passing on a multitude of threat warnings, policy makers and military commanders failed to take the necessary precautions and were ultimately responsible for the disaster.

The Beirut disasters, and in particular the Marine barracks bombing, appear to fit the orthodox model of intelligence failure particularly well because the failure was largely one of *cognition*, a failure of all involved to imagine the scale of the threat they were facing. In the summer and fall of 1983, the intelligence community (as well as the operational chain of command) failed to anticipate the threat, despite the critical warning of the Embassy bombing, because it was something new, innovative, and outside their expectations.

At first glance, the Marine barracks bombing might not seem to have been anything new or innovative, as it was conducted via the relatively traditional method that the intelligence community refers to as an "improvised explosive device." But the case study reveals that the massive size of the blast, and even the delivery mechanism—a truck, rather than a car—represented enough innovation to be beyond the imagination of the Marines who were killed. Terrorism analysts have agreed that the Marine bombing was indeed something new. Bruce Hoffman has described the weapon used as "not of the sort found in the typical terrorist group's arsenal."[46] Neil Livingstone described the bombing as an application of imagination to technology, resulting in an innovation: "Acetylene enhanced and possessing an explosive force of something between 12,000 and 18,000 pounds of TNT, it was—pound for pound—one of the

[46] Lesser, footnote pp 14-15.

most powerful conventional bombs ever built, and perhaps the largest terrorist bomb in history."[47]

The limitation of cognition and imagination helps us understand how so many involved failed to anticipate in the fall of 1983 that the next attack against the American presence in Beirut might be similar to, but much larger than, the last one. The problem was a conceptual one. As Thomas Friedman put it: "Even once they recognized they were embroiled in a tribal war . . . the Marines failed to take all the necessary precautions against something as unusual as a suicide car bomber, because such a threat was outside the boundaries of their conventional American training."[48]

The Beirut bombing also appears to have confirmed the expectations of the third school of analysts, that of terrorism specialists.

- In terrorism the Marines in Beirut faced a new, particularly dangerous type of threat, against which intelligence was unable to collect useful, specific tactical warning.
- Modern intelligence and information technology could provide no help.
- Only HUMINT could have provided the type of actionable warning the Marines needed, and it was not available.

This school's most specific hypothesis, that the challenge of terrorism can best be met by HUMINT, is difficult to prove, but experts who have studied the Beirut bombing firmly believe this case demonstrates the importance of HUMINT. Brian Jenkins, a widely recognized terrorism expert, testified before the Long Commission, "terrorist groups are hard to predict, hard

[47] Neil C. Livingstone, "The Impact of Technological Innovation," in *Hydra of Carnage: The International Linkages of Terrorism and Other Low-Intensity Operations*, ed. Uri Ra'anan, et al (Lexington, MA: Lexington Books, 1986), 140.
[48] Thomas L. Friedman, *From Beirut to Jerusalem* (New York: Anchor Books, 1990), 203.

to penetrate. It is mainly a matter of human intelligence."[49] Admiral Long himself later testified before a U.S. Senate hearing after the bombing of the Khobar Tower barracks in Saudi Arabia, "The lesson of Beirut is that we must have better HUMINT to support military planners and operations." Even the best intelligence, he said, will not guarantee security, but specific data of the type that can best be provided by human sources could have enabled the chain of command to be better prepared.[50]

The only theory of intelligence failure that appears to be discounted by the Beirut case study is that of the second school, the information optimists. The lessons concerning this theory are limited, because this case study represents only a single snapshot in time and intelligence and information processing systems have of course advanced tremendously since 1983. But it does appear that while the intelligence systems in use at that time were able to produce a great deal of reporting relatively quickly, that intelligence flow may have just been enough to *hinder*, rather than *help* the Marines in their mission. McCarthy wrote in his study of the case, "Intelligence management and technology are currently not in harmony. This was certainly the case during the Lebanon crisis, where the Marines were inundated with unmanageable quantities of intelligence information which lacked specific details."[51]

A failure of analysis

The case study of the Marine barracks bombing, then, seems to provide a result that would be familiar to most orthodox students of intelligence failure: as far as the intelligence community is concerned, there was indeed "no fault." The disaster appears to have occurred

[49] Brian Michael Jenkins, *The Lessons of Beirut: Testimony before the Long Commission* (RAND Note N-2114-RC, available at www.beirut-memorial.org/history, 1984).

[50] U.S. Congress, *Saudi Arabia and Beirut: Lesson Learned on Intelligence Support and Counterterrorism Programs*, 9.

[51] McCarthy, *The Function of Intelligence in Crisis Management: Towards an Understanding of the Intelligence Producer-Consumer Dichotomy*, 99.

because the chain of command facing a terrible new threat, and failed to listen to repeated warnings from intelligence. But while this conclusion may fit the orthodox view of intelligence theory, it is not supported by a closer look at the evidence. The bombing instead appears to have been as much the result of a failure of intelligence analysis as of a mistake in policy and command judgment.

A major part of that failure may have been that the intelligence system was better equipped to produce large volumes of raw information, rather than to sort through and interpret that data; intelligence was better at warning than analyzing. Colonel Pat Lang, USA (ret), a former Defense Intelligence Officer for the Middle East, testified before the Senate committee in 1996 that better analysis could in fact have helped the Marines in Beirut, and that would have meant more than simply passing on threat information, "so that you don't just give them a thousand reports that there may be bombings in Beirut. You tell them what this means, and what is really likely to happen."[52]

A *New York Times* investigation into the Beirut bombing concluded that the problem "was not insufficient intelligence, but insufficient evaluation."[53] BGEN James M. Mead, who as a Colonel had been the senior Marine officer in Beirut at the time of the first Embassy bombing, described the problem of over-warning:

> I was told by my intel officer, 'Hey boss, we've had another warning.' You got that every day. 'You're gonna get it, you're gonna get it, you're gonna get it.' Initially, after the American Embassy went, we went into a condition-one-type situation. I had my men on alert all the time. But then I began thinking I had to have more specificity, I'm wearing my men down without more specificity of a threat. So we had to take them out of that condition.[54]

[52] U.S. Congress, *Saudi Arabia and Beirut: Lesson Learned on Intelligence Support and Counterterrorism Programs*, 16. Stansfield Turner argues that a major reason for failure in Lebanon was not that a specific bit of human intelligence was missed, but because "U.S. intelligence failed to detect the depth of animosity to this American military presence." Turner, 156.

[53] Taubman and Brinkley, section 1, p 51. The part of the *Times* special report concerning intelligence is entitled "The Marine Tragedy: Intelligence: Too Much Information, Too Little Evaluation."

[54] Ibid.

The problem of over-warning in Beirut closely resembles the situation described by Wirtz in his book *The Tet Offensive*. Wirtz writes that when intelligence analysts produced more and more warnings prior to the Tet Offensive in 1968, this over warning had an unusual effect: intelligence ended up shifting the responsibility for discriminating among the warnings to field commanders. In response, commanders placed units on alert nearly 50 percent of the time in the months preceding Tet--and this in turn reduced commanders' responsiveness to warnings.[55]

A post-attack study by the Office of Naval Intelligence (ONI) suggested that better analysis might have been able to warn of the attack. Martin and Walcott report that several months after the Marine bombing, ONI conducted a review of all the data that had been collected beforehand. "We concluded the chances were pretty good we would have been able to predict," said RADM John Butts, the Director of Naval Intelligence. But the reason naval intelligence failed to provide warning, Martin and Walcott conclude, was simple: not a single analyst was assigned to work full time on the terror threat to the Marines in Lebanon.[56]

Although it is impossible to be sure without access to a full, classified account, it does appear that failures of intelligence support deserve a greater share of the blame for the Beirut disaster than previous assessments have indicated. The first mistake was largely procedural: intelligence officials should carry at least a share of the responsibility for having produced an overload of intelligence reporting that numbed the consumer. The second mistake was analytical. Not that the intelligence community should have been able to divine the exact bombing plans when no specific information was available; not even an increased HUMINT effort would necessarily have provided such actionable intelligence. But there seems to have been a deadly lack of *imagination* among the intelligence analysts supporting the Marines in

[55] James J. Wirtz, *The Tet Offensive: Intelligence Failure in War* (Ithaca, NY: Cornell University Press, 1991), 274.
[56] Martin and Walcott, 130. It is not clear whether this quote reflects Butts' view, or that of Martin and Walcott.

Beirut—for that is what it would have taken to warn against the threat that everyone expected, but no one could imagine.

The series of bombings in Beirut provides two very different pictures of failure against the threat of terrorist attacks. The 1984 bombing against the embassy serves as a model for what can clearly be labeled as a failure of policy: the intelligence threat in that case was as clear as it will ever be, absent the extremely unlikely acquisition of terrorists' actual targeting plans, and yet the needed defensive measures were not taken and the attack succeeded in causing significant destruction. Few cases of terrorist warning are likely to be so clear-cut in the future, but the 1984 bombing gives us a benchmark against which to judge future failures of command.

The 1983 Marine barracks bombing, on the other hand, presents a much more complicated case, and thus may be more representative of future attacks. No incompetence or dereliction of duty were found or even suggested. Most of the classical problems associated with warning and surprise were, however, evident: cognitive limitations prevented analysts and decisionmakers from even imagining what they were facing, while modern intelligence and communications technology produced a numbing overabundance of information. The official investigations, and thus the verdict of history, have largely cleared the intelligence community of significant blame in this case, supporting the orthodox view that warning of terrorist attack is extraordinarily difficult and failure can only be expected. But this study has suggested that failures by the intelligence community played a larger role in the disaster than was previously believed.

This study suggests that none of the conventional theories of intelligence failure is sufficient to explain the disaster. No single actor—not intelligence, not policy, and not even the terrorists—can reasonably be assigned the lion's share of blame. But if the fault is spread so widely—if everyone was to blame—how then can we explain the disaster? We are led back to the our initial question: how, in the "car bomb capital of the world," could the intelligence community and the Marine commanders not have learned more from the earlier bombing of the U.S. embassy and anticipated the coming attack? It may be that there is simply no overall explanatory framework or theory that can explain what happened in Beirut. Perhaps it can be understood only as a tragedy in which multiple actors, struggling against a common enemy, all contributed to their own failure. But the language we commonly use in discussing intelligence failure—disaster, tragedy—suggests there is another approach that may be useful in seeking to understand why such failures occur. This is through theory that examines other tragedies in which either no one, or everyone, may be at fault: theories of disaster and accidents. In the next section we will briefly consider one such theory that promises to explain at least as much, and maybe more, than traditional intelligence theory.

4. An Alternative Theory: Intelligence Failure as a "Normal Accident"

The previous section suggested that an attempt to analyze the 1983 Beirut bombing through the lens of traditional theories concerning intelligence failure and terrorism is ultimately unsatisfactory. Many aspects of the case seem to fit with orthodox theory as well as with the views of terrorism experts, and many of the classic problems of intelligence appear to have existed in Beirut. But overall, this does not tell us much. This study has suggested that the study of strategic surprise may have indeed reached diminishing returns—perhaps the problem of intelligence, especially against the extraordinarily difficult challenge of international terrorism, is simply a "hard slog," and theory can offer little help or understanding. But it could be the case that the available theory is lacking, and this section will suggest another approach that may be more useful in understanding the failures of intelligence in this new age.

This approach is what sociologist Charles Perrow has termed "normal accident theory." Accident theorists, including Perrow, often cite intelligence failures in their work, and students of intelligence often make an analogy with disasters and accidents. But little work has been done to systematically link these two schools of thought. This section will briefly introduce normal accident theory; examine what a few intelligence theorists have written about it; and then consider how it may apply to the problem of intelligence failure and the disaster of the Marine Barracks.

Perrow and Normal Accident Theory

Perrow argues that accidents and failures in complex, tightly coupled systems are inevitable, largely because it is impossible to anticipate all possible failures. He also writes that we seem unable to learn from disasters such as accidents and explosions, noting in a comment reminiscent of Handel's statement about intelligence: "We may have reached a plateau where our learning curve is nearly flat."[1]

But he is not simply arguing that in any large organization or system, mistakes will happen. For Perrow, mistakes are more likely in systems that meet two criteria. First, they are *complex*, meaning they contain multiple sub-systems that interact in many ways, leading to complex interactions that have multiple paths, producing unplanned or unexpected results. The opposite of such a system is a linear system, in which most interactions are understood and expected. And second, systems most vulnerable to failure are *tightly coupled*. This means that what happens in one part of the system directly affects another part. Little flexibility is possible, and processes tend to work only in one direction. The opposite type of system is loosely coupled, in which processes contain more slack and flexibility, and there are many ways to do things.

Perrow argues that because failures in such systems are so complicated, and because no one individual can possibly understand all the possible interactions of subsystems that may lead to an accident, no individual can be held fully accountable. The problem lies more in the system itself than in individual mistakes or incompetence. This suggests that his theory may parallel the orthodox, "no fault" school of intelligence failure. Preventing all accidents may be akin to predicting future surprises: it simply cannot be done. Perrow does not focus on military systems, arguing that while what he calls "military adventures" tend to be complex, they are loosely coupled, so do not fit his theory.[2] The examples he cites include the Challenger shuttle disaster, airline mishaps, and the Three Mile Island (TMI) nuclear accident. He argues that TMI represents the "essence" of a normal accident, in which multiple failures of subsystems

[1] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York, NY: Basic Books, 1984), 12.
[2] Ibid., 97.

interacted in ways that were largely incomprehensible to the technicians and operators on duty.[3] He even makes the analogy with Pearl Harbor, writing that at TMI the important signals that might have prevented the accident got lost in the noise.[4]

Scholars who have applied this theory to additional cases include Scott Snook, who studied the accidental shoot down of two Black Hawk helicopters over Northern Iraq in 1994; Diane Vaughan, who studied the Challenger disaster; and Scott D. Sagan, who examined the question of why there has never been an accidental or unauthorized nuclear weapon detonation in the U.S. system.[5] Of note, Sagan devotes a chapter to intelligence and warning during the Cuban Missile Crisis, and is the only accident theorist of whom I am aware who has specifically applied this theory to intelligence matters (although his conclusions deal more with command and control than with the classical problems of intelligence failure we have been examining). Sagan focuses not on the imagery and other intelligence that most case studies look at, but at the operation of the ballistic missile warning system, BMEWS, during the crisis. He finds that several serious command and control incidents occurred in that system during the crisis, suggesting that normal accident theory applies to that warning system.

There is a group of academics who disagree with Perrow, known as High Reliability Organization (HRO) theorists. These thinkers believe that organizations can compensate for the human frailties that often lead to accidents and disasters. To some extent, this is a "glass half-full, glass half-empty" debate. HRO thinkers, for example, tend to see TMI more benignly than Perrow, as a major disaster averted: "By all accounts, Three Mile Island was the worst reactor

[3] Ibid., 23.

[4] Ibid., 30.

[5] Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, NJ: Princeton University Press, 1993); Scott A. Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*, Paperback ed. (Princeton, NJ: Princeton University Press, 2002); Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago, IL: University of Chicago Press, 1996).

mishap in the history of the American nuclear industry, and it was a financial disaster for the utility that owned the plant. But from a safety perspective, the accident was about the equivalent of a car accident."[6] HRO theorists do, however, provide a very different and useful perspective, and are of particular interest to this study because they tend to focus on military organizations. Scott Sagan has summarized what this school believes are four critical factors that can lead to higher levels of safety:

- Prioritization of safety and reliability as a goal by political elites and the organization's leadership;
- High levels of redundancy in personnel and technical safety measures;
- Development of a "high reliability culture" in decentralized and continually practiced operations;
- And the use of sophisticated forms of trial and error organizational learning.[7]

Authors associated with this school have frequently cited U.S. Navy aircraft carrier flight operations as an example of a highly complex system that works with a remarkably high level of safety.[8] In part, they argue this impressive safety record comes from the fact that while the Navy is a very hierarchical organization, flight operations are run as a relatively "flat" and collegial structure, with more flexibility than an observer might expect. There are also multiple redundancies—both in terms of mechanical systems and necessary supplies and parts, but also "decision/management redundancy," in that many individuals are on the same communications

[6] Joseph G. Morone and Edward I. Woodhouse, *Averting Catastrophe: Strategies for Regulating Risky Technologies* (Berkeley, CA: University of California Press, 1986), 5.

[7] Sagan, 17. Sagan provides a useful summary of both HRO and normal accident theories, pp 9-49. For other useful discussions of these theories, from authors favorable toward the normal accident school, see Snook and Vaughan.

[8] Todd R. La Porte and Paula M. Consolini, "Working in Practice but Not in Theory: Theoretical Challenges of 'High Reliability Organizations'," *Journal of Public Administration Research and Theory* 1, no. 1 (January 1991); Gene I. Rochlin, Todd R. La Porte, and Karlene H. Roberts, "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea," *Naval War College Review* LI, no. 3 (Summer 1998); Karl E. Weick and Karlene H. Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* 38, no. 3 (September 1993).

net, watching the same operation, and trained and ready to step in if they see something wrong or unsafe.[9]

Previous Comparisons Between Intelligence Failure and Accidents

Most intelligence theorists, like most social scientists, tend to minimize the role of accidents or luck. As Walter Laqueur put it, “accidents are unrewarding material for theory building.”[10] But a few analysts have suggested accident theory may apply, even though they have not specifically cited Perrow’s theory. The orthodox argument that intelligence failures are natural appears to echo Perrow’s work, and the language used by students of intelligence and accidents is often the same; Richard Betts, for example, has written that in the face of unavoidable failure, what may be needed is “tolerance for disaster.”[11] Several scholars of intelligence, including Ephraim Kam, have described the cognitive failings of policy makers as resembling those of people facing natural disasters: both tend to resist warnings of terrible events, and fail particularly to react to gradual warnings, such as of a flood, as opposed to warnings that appear quickly, such as of a tornado.[12]

Pearl Harbor shows clearly how the language and concepts of normal accident theory can apply to cases of intelligence failure. Roberta’s Wohlstetter’s detailed description of the many actors involved, the numerous intelligence organizations and offices, and the multitude of types of signals present, all suggest that the American intelligence gathering system in 1941 was

[9] Rochlin, La Porte, and Roberts: 104-108. Useful discussions of this debate from the point of view of HRO theorists are Morone and Woodhouse; Karlene H. Roberts, "The Significance of Perrow's *Normal Accidents: Living with High-Risk Technologies*," *The Academy of Management Review* 14, no. 2 (April 1989). From an author supportive of normal accident theory, Lee Clarke, "Drs. Pangloss and Strangelove Meet Organizational Theory: High Reliability Organizations and Nuclear Weapons Accidents," *Sociological Forum* 8, no. 4 (nd 1993). A balanced approach is Denise M. Rousseau, "Review of *the Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, by Scott D. Sagan," *Administrative Science Quarterly* 41, no. 1 (March 1996).

[10] Laqueur, 271.

[11] Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," 89.

[12] Kam, 9.

complicated and complex. But the analogy with Perrow's theory is clear even before Wohlstetter's description of the circumstances behind the disaster. In his foreword to *Pearl Harbor: Warning and Decision*, Thomas Schelling writes: "It would be reassuring to believe that Pearl Harbor was just a colossal and extraordinary blunder. What is disquieting is that it was a supremely *ordinary* blunder."[13]

A few students of intelligence have made an explicit link between normal accident theory and intelligence failure. Michael Handel appears to have gone the furthest along this line of thought, and in an appendix to a 1984 article he cited Perrow's work and wrote that "the student of strategic surprise is struck by the similarities" between what he called man-machine accidents and surprise.[14] Just as in intelligence, Handel argued, one would have expected that the use of computers would have been able to help prevent accidents. But such prevention has proved impossible, largely because it is the human element that is weakest, least predictable factor in causing accidents as well as intelligence failure. Handel did not develop these ideas further, but suggested, "there is still much more that strategic analysts can learn from man-machine accidents and disaster theory."[15]

Other writers on intelligence failure have drawn the parallel with normal accident theory, but have not been so confident that it can teach us much. Elliot Cohen and John Gooch, in their book *Military Misfortune*, describe Perrow's ideas and use them to argue that military disasters may be better understand by thinking in terms of systems and organizations. But they do not

[13] Wohlstetter, viii. Ephraim Kam also appears to conclude that Pearl Harbor was a quite normal accident, and uses language that sounds as if it comes from Perrow's theory: "On the morning of December 7, 1941, almost everyone in Pearl Harbor behaved as usual." Kam, 177.

[14] Handel, "Intelligence and the Problem of Strategic Surprise," 273. The appendix, pages 272-274, is entitled "Complex Man-Machine Accidents."

[15] Ibid.: 274. Handel also cited Perrow in Handel, "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty."

take the analogy very far.[16] Robert Jervis has cited Perrow in an article in which he argues that the intelligence community can be seen as forming an "error-inducing system." In this system, the interlocking norms, incentives, and habits of intelligence officials tend to decrease the quality of analysis, and make it hard to change any one part of the system without upsetting other parts.[17]

More recently, several analysts have discussed the 9/11 attacks in the context of normal accident theory. Malcolm Gladwell has argued that intelligence failures are different from accidents such as the Challenger and Columbia shuttle disasters. In those normal accidents, he believes, even though it is impossible to absolutely rule out a future disaster, engineers and others are able to learn from previous accidents and make future disasters less likely. But with intelligence work, the learning process does not work the same way, because the more new information that is acquired, the harder it becomes to find the signals amidst the noise.[18] Charles F. Parker and Eric K. Stern have quoted Perrow and Sagan in suggesting the 9/11 attacks may have represented a "normal" failure, but they have not developed the analogy further.[19]

Testing the Analogy

Normal accidents resemble intelligence failures in several important ways:

- Accidents are considered ordinary events that can have catastrophic consequences.
- They are largely caused by the accumulation of many small mistakes.
- There is a tendency after accidents to blame the operator, not the system itself.
- Problems in cognitive psychology and human perception are seen as the key to understanding complex system accidents.

[16] Cohen and Gooch, *Military Misfortunes: The Anatomy of Failure in War*, 22-23.
[17] Jervis, "What's Wrong with the Intelligence Process?," 34-35.
[18] Malcolm Gladwell, "The Epistemology of Surprise," *The New Yorker (online version)*, March 10 2003.
[19] Parker and Stern: 622.

But can we really compare the intelligence community to the complex system that operates a nuclear power plant? A full answer to this question is beyond the scope of this thesis, but it does appear that there may be value in this analogy. First, the U.S. intelligence community appears to clearly meet Perrow's test of *complexity*. With its many organizations, and compartmented sub-organizations at all levels, the comparison with a nuclear plant does seem apt. The fundamental importance of secrecy within the intelligence community may tend to exacerbate this complexity, reinforcing the point that Perrow makes about complex systems: no one person within the system is able to see the entire picture. This appears to have happened in Beirut, where several different organizations conducted security evaluations, providing their assessments to specific customers but not necessarily sharing them with the policy makers who needed the information.

The second test appears harder to apply: can the intelligence community be considered a *tightly coupled system*? The very compartmentalization that produces extreme complexity would seem to make the intelligence system more flexible and loosely coupled. But we may be seeing that the advances of the information age are making the intelligence community more tightly coupled and less flexible. When the system produces vast quantities of information, and that information is available nearly instantaneously to the entire community, the pressure increases to pass that data on immediately to the commanders and decision makers. The stream of intelligence reporting acts as a one-way flow, leaving little time for analysis or for competing evaluation to take place. This effect was seen in Beirut, where the Marine commanders on the scene had more intelligence reporting than they could use, but not the analysis they needed.

But even if we can demonstrate that the intelligence community is a complex, tightly coupled system, can we reasonably compare the challenges faced by the intelligence community, which is working against a thinking, hostile enemy capable of deception and surprise, with the task of operating a nuclear power plant or other complex system, no matter how complex or dangerous it might be? Handel wrote that accidents are different from intelligence work in that accidents are not caused by the actions of a conscious enemy.[20] But I argue that the two situations are more alike than one might expect. In both cases, the task is to deter, detect, prevent, and contain a hostile force.

In the case of intelligence, the hostile force may be a conventional military threat or a terrorist group. For the complex systems Perrow studied, the enemy was quite different, but just as real. A nuclear power plant is in a very real sense attempting to overheat and even explode, unless the operators and control systems are vigilant in monitoring the systems (collecting intelligence) and taking corrective action as necessary (analysis and decision making). A space shuttle, and even a civilian airliner, is also essentially a system that is constantly attempting to destroy itself, through explosion, crash, or other disaster. While the destruction of the Marine barracks in Beirut might well have been described as a "disaster waiting to happen," complex and dangerous systems such as nuclear plants are precisely that. By comparing the two situations, we can see that "predicting the future" is for intelligence what "preventing accidents" is for safety and complex systems engineers: a worthwhile, but never completely obtainable goal.

Can Normal Accident Theory Tell us Anything Useful?

It cannot be enough, of course, to merely point out ways in which intelligence failures might resemble complex system accidents. The important question for this thesis is, does this school of thought contain any lessons, useful analysis, or prescriptions that might apply to the problem of intelligence in dealing with terrorist attacks? I believe it does—but unfortunately

[20] Handel, "Intelligence and the Problem of Strategic Surprise," 272.

those lessons are no more comforting for the intelligence community than Perrow's theory is for the nuclear power industry.

It is possible—but I believe unlikely—that the lessons and prescriptions from either the normal accident or HRO theories may help reduce the incidence of intelligence failures in the future. Perrow's view is largely pessimistic, and his prescriptions do not seem to apply to the problem of intelligence and terrorism.[21] HRO theory, on the other hand, suggests lessons that appear sound, but familiar, such as that the intelligence community could do a better job of developing what it calls a "collective mind," communicating better within the community and with its customers.[22] But while I do not believe these specific prescriptions are satisfactory, I do believe normal accident theory offers a theoretical basis for a greater understanding of intelligence failure. First, it highlights a problem that may actually be the primary reason why failure in a complex system such as the U.S. intelligence system is inevitable: efforts to improve the system are just as likely to make things worse as to improve them. And second, it suggests that much of current intelligence theory may be misguided in its emphasis on psychological factors and problems of cognition.

The first problem builds on one of Perrow's findings concerning attempts to increase safety in complex systems: adding more safety measures may not prevent accidents, and may paradoxically make mistakes even more likely. The addition of redundant monitoring systems,

[21] He argues that complex systems can be made safer if they are more loosely coupled—adding more time and flexibility, with people "in the loop" to be able to correct errors. But he acknowledges that some systems, such as nuclear power plants, cannot be made looser, and dismisses the argument that nuclear plants might be operated along a military model, arguing the U.S. Navy's system is not as safe as some believe and the military's structure is incompatible with American freedoms. These points seem clearly debatable, especially after 9/11. Instead, he believes steps must be taken to eliminate the use of nuclear power, for such plants can never be made sufficiently safe. No such solution is available for problem of intelligence analysis against the terrorist threat; we cannot simply eliminate the intelligence community because it is prone to failure.

[22] See for example Weick and Roberts. HRO theory might also suggest the intelligence community should develop the combination of hierarchy but collegial structure found on the flight deck, while ensuring the existence of carefully designed redundancy in critical subsystems such as analytical nodes.

for example, may just increase the likelihood of a mechanical fault in an ever-more complex system; while employing additional safety observers may encourage all safety personnel to relax, because they believe others will catch problems they miss. Intelligence theorists have often noted that a similar syndrome may occur in the attempts to reduce surprise or improve the detection of enemy attacks. Adding more analysts may not make intelligence any better, especially if, as in Beirut, most of those analysts were far from the scene of action an unlikely to have a good understanding of the local conditions. Lowering the threshold for warning may increase the number of alarms transmitted, but that volume may encourage decision makers to disregard the warnings. Becoming more alert to deception may cause analysts to dismiss all information for fear it is the product of a deception effort, and establishing a position of "devil's advocate" may mean that alternative views become routinely isolated and disregarded.

This insight from normal accident theory suggests that while intelligence failures may be caused by the classic problems of intelligence, the *inevitability* of failure may be the result of the complex nature of the intelligence system. As in Beirut, even when intelligence is successful in its task of collecting more information, the result may be to perversely make it more difficult to anticipate surprise. This can occur because the intelligence system and the minds of decision makers become overloaded—the traditional problem of too much noise. But as Richards Heuer has argued, it can also occur because as psychological studies have shown, the accumulation of more information often does not help one make a better decision; at best it may simply add more data about variables already understood, and at worst it will simply be adjusted to fit the existing beliefs of the analyst.[23]

[23] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: CIA Center for the Study of Intelligence, 1995). Heuer described a medical study that showed that the collection of additional data by physicians does not necessarily lead to increased diagnostic accuracy. For a similar example of a psychological experiment in which attempting to fix the problem only makes it worse, see Gladwell, "Connecting the Dots." These ideas have

The second insight from normal accident theory may be even more significant, because it sheds new light on a key concept in the study of intelligence failure—that of irrationality and human cognition. The analogy with accidents and disasters suggests that much of the intelligence literature, which focuses on the problems caused by human perceptions and cognitive failures, may be misguided.

Much of the literature on risk and decision-making focuses on the cognitive limitations that prevent the public and policy makers from weighing risks properly and making good decisions. Perrow argues, however, that such limitations are not necessarily a bad thing. This is partly because such irrational cognition is part of our humanity: "Our cognitive limits may make us human in ways we treasure."[24] But he also argues that these limitations may actually produce better decision-making than a strictly rational approach might. He develops the concept of "social rationality," arguing that because each of us is limited in different ways—my cognitive defects are not the same as yours—humans are forced to work together, resulting in a better process than would be reached otherwise.

I believe this concept can be extended to the problem of intelligence analysis. Much of intelligence theory seeks to reduce the human aspect, by either eliminating humans from the loop or by developing more mechanistic and objective methods for determining and predicting threats. But Perrow's theories suggest that this focus might be turned around: these human frailties may actually be useful, and eliminating them might be harmful. I will consider this in the final section.

direct relevance to the intelligence post-mortems following 9/11: they suggests that the "connect the dots" imagery of intelligence is faulty, because it implies that if only the "missing" information could be found, the picture would be seen with clarity. Heuer and Gladwell might suggest that additional information would just make the dots clearer—while only analysis can fill in the missing connections.

[24] Perrow, 321.

5. Conclusion

This study appears to confirm that the orthodox view of intelligence failure holds true against the problem of terrorism, for despite the information revolution and advances in technology, intelligence is not getting any better at detecting surprise. Ernest May described the phenomenon that appears to have been demonstrated in Beirut: "Like people growing old, governments may have been acquiring more and more powerful glasses but nevertheless becoming able to see less and less."[1]

The reasons for the failure of intelligence in Beirut were for the most part familiar. Above all, analysts and decision makers faced a cognitive limitation that prevented them from being able to anticipate the tactics the enemy would use. This was compounded by the problem that an overabundance of general warnings had dulled all actors to the reality of the threat. Additional classic intelligence problems at work included an overemphasis on current intelligence, the accumulation of data at the expense of longer-term analysis, and a lack of deep cultural awareness of the enemy.

But the Beirut disaster demonstrated that the main stream of intelligence theory is wrong in suggesting that the predominance of blame for such a failure should fall to decision makers in Washington and commanders on the scene. As we have seen, the major post-attack investigations took precisely this view and largely exonerated the intelligence community; but they were wrong. Our study indicates the intelligence community must share an equal portion of the responsibility, both for passing on a flood of intelligence data without conducting the necessary analysis, and—just as important—for not ensuring that the intelligence was being received and understood properly by command.

[1] Ernest R. May, "Conclusions: Capabilities and Proclivities," in *Knowing One's Enemies: Intelligence Assessment before the Two World Wars*, ed. Ernest R. May (Princeton: Princeton University Press, 1984), 532.

This study sheds light on a question discussed in the literature on intelligence and terrorism: whether terrorists would be expected to use *deception* more or less effectively than would traditional militaries. We might expect that nonstate actors—or any less powerful foe for that matter—might be naturally drawn to deception as a form of asymmetric warfare. But the Beirut attacks do not appear to indicate any use of sophisticated deception planning by the terrorists. This may have been because they simply did not need it, but it also tends to confirm the argument of several students of deception that, in the words of Godson and Wirtz, "sustained and coordinated deception campaigns often exceed the resources of nonstate actors."[2] Shulsky describes the requirements needed in order to carry out a successful deception, and it appears that these may be beyond the reach of most terrorist groups: strategic coherence, an understanding of the adversary, an operational infrastructure, channels through which to reach the adversary, and means of obtaining feedback.[3]

J. Bowyer Bell argues that although nonstate actors such as terrorists use denial and secrecy routinely, they rarely have the skills and resources to conduct more than tactical deception. Terrorists such as the World Trade Center 1993 bombers demonstrate that even inept terrorists are able to inflict surprise, while their inability to deceive makes them relatively easy to catch after the fact. But he suggests that some groups may be sufficiently capable: "Terrorist organizations most likely to pursue deception in operational matters beyond denial are those engaged in protracted campaigns that allow experience to be acquired, opportunities noted, and

[2] Godson and Wirtz, eds., 6.

[3] Abram N. Shulsky, "Elements of Strategic Denial and Deception," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz (New Brunswick, NJ: Transaction Publishers, 2002). See also Donald C. Daniel and Katherine L. Herbig, "Propositions on Military Deception," *Journal of Strategic Studies* 5, no. 1 (March 1982).

time invested."[4] Whether the planners behind the Beirut bombing fit into the first category, because they did not attempt deception, or in the second, because they have never been caught, remains an open question.

What to Make of the Information Age Optimist Argument?

This case study, although only a single snapshot in time, has offered little to suggest that the information age optimists are correct in believing intelligence will be able to use modern technology to improve its chances against terrorist threats. Examination of later cases of terror attacks may demonstrate improvements brought about by intelligence and information technology, but this study suggests that such systems will only add to the information collected, and not increase the understanding of the threat.

What About the Terrorism Analysis School?

We have seen that the series of bombings in Beirut supports many of the views of terrorism experts that the new, non-state threat magnified the traditional difficulties of intelligence analysis. But we have also seen that prior to the Marine barracks bombing the threat was just as evident, and the intelligence data nearly as voluminous, as before the attack on Pearl Harbor. Although the terrorist enemy was a shadowy and frustrating target for the Marines, there was sufficient intelligence available prior to the bombing to indicate a clear threat, even without specific intelligence from human or other sources. The challenge for intelligence was a tactical one of determining where and how an attack would come, which is little different from the challenge faced by intelligence services of the U.S. in 1941, or of Israel in 1973. This tends to contradict the belief of terrorism analysts that only greatly improved human intelligence offers hope to counter the terror threat. In Beirut, at least, both intelligence and policy makers had all

[4] J. Bowyer Bell, "Conditions Making for Success and Failure of Denial and Deception: Nonstate and Illicit Actors," in *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson, James J. Wirtz (New Brunswick, NJ: Transaction Publishers, 2002), 149-150.

the intelligence they needed to predict the attack; the failure was not of collection, as terrorism experts typically suggest, but of analysis and policy.

Additional Lessons to be Learned

We have seen that in many ways, the challenges terrorism presents for intelligence are quite familiar. But while the problems that lead to surprise are much the same, the *nature* of that surprise, and the *effects* it creates, can be very different.[5] Richard Betts has written that in the past, while the immediate cause of surprise against conventional enemies has concerned questions such as where, when, or how the attack would come, the fundamental problem has been determining *whether* the enemy will attack. But against a terrorist enemy such as the Marines faced in Beirut in the fall of 1983, there was little doubt that an attack would come, and yet it was still terribly surprising and effective. The main difference appears to lie first in the fact that against the threat of terrorism the relationship between capabilities and intentions is reversed; and second, in the fact that in the case of terror attack, tactical considerations often have strategic consequences.

The traditional intelligence paradigm has held that an enemy's *capabilities* are easier to assess than its *intentions*, and it is usually capabilities—hard facts—that military commanders and decision makers demand of intelligence. Intelligence professionals and theorists, however, often felt that *intentions* were actually more important, even though they couldn't so easily be discerned. Now, terrorism may be turning this model on its head. Decision makers demand to know, where will the terrorists strike next? What are their intentions? But our study of Beirut suggests that especially after an initial attack, the enemy's intentions are clear, and the crucial question is, what capabilities do they have? The Marines understood that their faceless, nameless enemy intended to attack; what they could not fathom is *how* the attack would come.

[5] I am grateful to Professor Tom Mahnken of the Naval War College for suggesting this line of thought.

Another break from the traditional paradigm can be seen in that today tactical actions can more easily have strategic consequences. The increased significance of tactical actions has three important implications for intelligence and warning. The first is that the effect of surprise is magnified. In the past, surprise attacks have often produced little more than tactical success. As Betts has written, "the good news from history is that attackers often fail to win the wars that they start with stunning surprises."[6] But terrorist attackers may not need or want to spark a clearly defined war that can be won or lost; the tactical success of the attack itself is enough for victory, as when the Beirut bombings led to the U.S. withdrawal from Lebanon.

Second, the nature of the surprise is different. In terror attacks the surprise is often in the tactical specifics of the attack, such as the technology or methodology used. While orthodox intelligence theorists have typically held that technological surprise is of secondary importance, the Beirut disaster demonstrates that the use of an unexpected tactic, combined with a deadly technology, can have a lasting strategic impact.

And the Beirut case suggests a third way in which terror attacks are more dangerous and difficult for intelligence than conventional surprise attacks. While conventional surprise attacks are usually difficult to carry out in succession because, as Betts writes, "the original surprise puts the victim on unambiguous notice,"[7] the Beirut bombings suggest that it may be more difficult to learn useful lessons from prior terrorist attacks. This could result from a number of factors, including the cognitive difficulties we have examined, but also because following terrorist attacks, nations rarely mobilize to the extent they do after a conventional attack.

[6] Betts, "Fixing Intelligence," 481.

[7] Ibid.

Lessons from Normal Accident Theory

We have seen that normal accident theory provides a greater understanding of a limitation that intelligence theorists have often noted: trying to fix the problem of intelligence failure may just make it worse. But its second lesson may be even more useful, and may merit further study. This is the idea that the conventional approach to reducing intelligence failures, which attempts to eliminate the human element in analysis and replace it with rational analytical and decision making techniques, may be counterproductive.

Not that all students of intelligence failure believe conceptions are uniformly harmful. Klaus Knorr has pointed out that without conceptions or theories that help guide our analysis, "the current stream of information would be unmanageable and often paralyzingly ambiguous."[8] But Knorr nonetheless takes the conventional approach, attempting to find ways to limit the shortcomings that these conceptions provide. Walter Laqueur is one of the few who has taken a different tack, arguing that the factor of perceptions and the psychological dimension of intelligence failure have been overrated.[9] Normal accident theory suggests we may be able to take Laqueur's argument even further.

Although Perrow's concept of "social rationality" may not apply to intelligence work, the idea that a focus on cognitive factors is misguided suggests additional propositions that might be tested against cases of intelligence failure. Theorists have argued that purely rational analysis, not subject to emotional or cognitive bias, is the best approach in attempting to prevent intelligence failure and surprise. But what if the conventional view is wrong, and too much rational analysis might itself be part of the problem? For example, our study of the Beirut bombings demonstrated that highly competent commanders and analysts, applying what they

[8] Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," 462.
[9] Laqueur, 269-286.

considered to be logical thinking against a critical problem, were completely unable to comprehend the nature of the threat they faced. It is possible that their failure was not caused by a lack of rational thinking, but by too much of it.

An effort to eliminate psychological factors from intelligence analysis might not only be ultimately unsuccessful, but to the extent that it did succeed it could very well result only in greater failure. For example, cognitive limitations are often seen as preventing analysts from raising the alarm in time. But if those limitations were removed, the opposite problem could appear: too many alarms. And if decision makers responded to alarms in a mechanistic, rational, and unbiased way, they also might react too often, mobilizing against unjustified threats and possibly creating a crisis where none had existed. Surprise attacks, after all, are rare, and indications of attacks are quite common. Just as analysts frequently complain that the problem of intelligence success is neglected, the problem of "false alarms" is little studied—and might indicate that attempting to apply a rational, essentially automatic approach to responding to these alarms might very well create more problems than it solves.[10]

From Secrets to Mysteries to Unknowns

Warning of terrorist attack could present as great a problem for intelligence as the earlier transition from secrets to mysteries. As Joseph Nye explained, in the more complex world after the end of the Cold War sheer facts became less useful in answering the needs of decisionmakers. This meant that *secrets*, questions to which a concrete answer based on facts was available—such as the number of ICBMs an enemy has—were no longer sufficient. In their

[10] Loch Johnson quotes former secretary of state Dean Rusk as accusing the CIA of frequently overreacting—raising a false alarm--noting that "the Agency predicted twelve of the last four" crises. Johnson, "Bricks and Mortar for a Theory of Intelligence," 19.

place, analysts and policy makers were faced with *mysteries*, which Nye described as puzzles to which no one could be sure of an answer.[11]

Mysteries clearly present a challenge for intelligence, but even more difficult and more descriptive of today's threats may be the challenge of what Anthony G. Oettinger has described as "unknown-unknowns," or *unk-unks*: the things we don't even know we don't know.[12] When the nature of future threats is undetermined, intelligence analysts will not even know today the questions they may be required to answer tomorrow. Facing such threats, intelligence analysts and decision makers may find that the traditional lessons from intelligence theory are less useful. In their place, new lessons may need to be discovered based on other concepts such as normal accident theory. But whatever the lessons and wherever they are found, it appears clear that in the 21st Century the study of intelligence failure and strategic surprise has not reached the point of diminishing returns.

[11] Nye, "Peering into the Future," 88.
[12] Anthony G. Oettinger, "Knowledge Innovations: The Endless Adventure," *Bulletin of the American Society for Information Science and Technology* 27, no. 2 (December/January 2001): 13.

BIBLIOGRAPHY

"Adequacy of U.S. Marine Corps Security in Beirut." *Terrorism: An International Journal* 7, no. 3 (nd 1984): 341-345.

Allen, Charles E. "Warning and Iraq's Invasion of Kuwait: A Retrospective Look." *Defense Intelligence Journal* 7, no. 2 (Fall 1998): 33-44.

Baer, Robert. *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism*. NY: Crown Publishers, 2002.

Belden, Thomas G. "Indications, Warning, and Crisis Operations." *International Studies Quarterly* 21, no. 1 (March 1977): 181-198.

Bell, J. Bowyer. "Conditions Making for Success and Failure of Denial and Deception: Nonstate and Illicit Actors." In *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson, James J. Wirtz, 129-162. New Brunswick, NJ: Transaction Publishers, 2002.

________. "Toward a Theory of Deception." *International Journal of Intelligence and Counterintelligence* 16, no. 2 (Summer 2003): 244-279.

Ben-Zvi, Abraham. "Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks." *World Politics* 28, no. 3 (April 1976): 381-395.

________. "Misperceiving the Role of Perception: A Critique." *The Jerusalem Journal of International Relations* 2, no. 2 (Winter 1976-77): 74-93.

________. "The Study of Surprise Attacks." *British Journal of International Studies* 5, no. 2 (July 1979): 129-149.

________. "Surprise: Theoretical Aspects." In *International Violence: Terrorism, Surprise and Control*, ed. Yair Evron, 86-104. Jerusalem: The Hebrew University of Jerusalem, 1979.

Berkowitz, Bruce D. "Information Age Intelligence." *Foreign Policy* 103 (Summer 1996): 35-50.

________. "Better Ways to Fix U.S. Intelligence." *Orbis* 45, no. 4 (Fall 2001): 609-619.

________. "Intelligence and the War on Terrorism." *Orbis* 46, no. 2 (Spring 2002): 289-300.

Betts, Richard K. "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (October 1978): 61-89.

________. *Surprise Attack: Lessons for Defense Planning*. Washington, DC: Brookings, 1982.

________. "Surprise, Scholasticism, and Strategy: A Review of Ariel Levite's *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987)." *International Studies Quarterly* 33, no. 3 (September 1989): 329-343.

________. "Fixing Intelligence." In *Terrorism and Counterterrorism*, ed. Russell D. Howard and Reid L. Sawyer, 473-483. Guilford, CT: McGraw-Hill/Dushkin, 2003.

Bolger, Daniel P. *Americans at War, 1975-1986: An Era of Violent Peace*. Novato, CA: Presidio, 1988.

Borch, Fred L. "Comparing Pearl Harbor and '9/11': Intelligence Failure? American Unpreparedness?" *Journal of Military History* 67, no. 3 (July 2003): 845-860.

Brady, Christopher. "Intelligence Failures: Plus Ca Change..." *Intelligence and National Security* 8, no. 4 (October 1993): 86-96.

Brodin, Katarina. "Surprise Attack: The Case of Sweden." *Journal of Strategic Studies* 1, no. 1 (May 1978): 98-110.

Brody, Richard. "The Limits of Warning." *The Washington Quarterly* 6, no. 3 (Summer 1983): 40-48.

Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign Against Terrorism*. Washington, DC: CSIS Press, 2001.

Chairman, U.S. Joint Chiefs of Staff. *Joint Vision 2020*. Washington, DC: GPO, 2000.

Chan, Steve. "The Intelligence of Stupidity: Understanding Failures in Strategic Warning." *American Political Science Review* 73, no. 1 (March 1979): 171-180.

Cilluffo, Frank J., Ronald A. Marks, and George C. Salmoiraghi. "The Use and Limits of U.S. Intelligence." *The Washington Quarterly* 25, no. 1 (Winter 2002): 61-74.

Clarke, Lee. "Drs. Pangloss and Strangelove Meet Organizational Theory: High Reliability Organizations and Nuclear Weapons Accidents." *Sociological Forum* 8, no. 4 (nd 1993): 675-689.

Cohen, Eliot A. "The 'No Fault' View of Intelligence." In *Intelligence Requirements for the 1990's: Collection, Analysis, Counterintelligence, and Covert Action*, ed. Roy Godson, 71-96. Lexington, MA: Lexington Books, 1989.

Cohen, Eliot A., and John Gooch. *Military Misfortunes: The Anatomy of Failure in War*. New York: Vintage Books, 1991.

Colby, William E. "Deception and Surprise: Problems of Analysts and Analysis." In *Intelligence Policy and National Security*, ed. Robert L. Pfaltzgraff, Jr., Uri Ra'anan and Warren Milberg, 91-97. Hamden, CT: Archon Books, 1981.

Consortium for the Study of Intelligence. *The Future of U.S. Intelligence*. Report Prepared for the Working Group on Intelligence Reform, 1996.

Daniel, Donald C., and Katherine L. Herbig. "Propositions on Military Deception." *Journal of Strategic Studies* 5, no. 1 (March 1982): 155-177.

Deutch, John, and Jeffrey H. Smith. "Smarter Intelligence." *Foreign Policy* (January/February 2002): 64-69.

DeWeerd, H. A. "Strategic Surprise in the Korean War." *Orbis* 6, no. 3 (Fall 1962): 435-452.

Dishman, Chris. "Trends in Modern Terrorism." *Studies in Conflict and Terrorism* 22, no. 4 (October-December 1999): 357-362.

Ellsworth, Robert F., and Kenneth L. Adelman. "Foolish Intelligence." *Foreign Policy* 36 (Fall 1979): 147-159.

Ermath, Fritz. "Signs and Portents: The 'I & W' Paradigm Post - 9/11." *The National Interest*, October 2 2002, accessed on line at www.intheneationalinterest.com.

Frank, Benis M. *U.S. Marines in Lebanon 1982-1984*. Washington DC: History and Museums Division, Headquarters U.S. Marine Corps, 1987.

Friedman, Thomas L. *From Beirut to Jerusalem*. New York: Anchor Books, 1990.

Gates, Robert M. "An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House." *The Washington Quarterly*, Winter 1989, 35-44.

Gazit, Schlomo. "Estimates and Fortune-Telling in Intelligence Work." *International Security* 4, no. 4 (Spring 1980): 36-56.

________. "Intelligence Estimates and the Decision-Maker." In *Leaders and Intelligence*, ed. Michael I. Handel, 261-281. London: Frank Cass, 1989.

Gazit, Schlomo, and Michael Handel. "Insurgency, Terrorism, and Intelligence." In *Intelligence Requirements for the 1980s: Counterintelligence*, ed. Roy Godson, 125-158. New Brunswick, NJ: Transaction Books, 1980.

George, Alexander L. "Warning and Response: Theory and Practice." In *International Violence: Terrorism, Surprise and Control*, ed. Yair Evron, 12-24. Jerusalem: The Hebrew University of Jerusalem, 1979.

Gladwell, Malcolm. "Connecting the Dots." *The New Yorker*, March 10 2003, accessed at http://www.newyorker.com.

________. "The Epistemology of Surprise." *The New Yorker (online version)*, March 10 2003, interview available online only at http://www.newyorker.com.

Godson, Roy, and James J. Wirtz, eds. *Strategic Denial and Deception: The Twenty-First Century Challenge*. New Brunswick, NJ: Transaction Publishers, 2002.

Goodman, Allan E. "Dateline Langley: Fixing the Intelligence Mess." *Foreign Policy* 57 (Winter 1984-85): 160-179.

Grabo, Cynthia M. *Anticipating Surprise: Analysis for Strategic Warning*. Washington, DC: Joint Military Intelligence College, 2002.

Hallenbeck, Ralph A. *Military Force as an Instrument of U.S. Foreign Policy: Intervention in Lebanon, August1982-February 1984*. New York: Praeger, 1991.

Hammel, Eric. *The Root: The Marines in Beirut August 1982-February 1984*. San Diego, CA: Harcourt Brace Jovanovich, 1985.

Handel, Michael I. "The Yom Kippur War and the Inevitability of Surprise." *International Studies Quarterly* 21, no. 3 (September 1977): 461-502.

________. "Perception, Deception and Surprise: The Case of the Yom Kippur War." In *International Violence: Terrorism, Surprise and Control*, ed. Yair Evron, 25-85. Jerusalem: The Hebrew University of Jerusalem, 1979.

________. "Avoiding Political and Technological Surprise in the 1980's." In *Intelligence Requirements for the 1980's: Analysis and Estimates*, ed. Roy Godson, 85-111. New Brunswick, NJ: Transaction Books, 1980.

________. "Surprise and Change in International Politics." *International Security* 4, no. 4 (Spring 1980): 57-85.

________. "Surprise in Diplomacy." In *Intelligence Policy and National Security*, ed. Robert L. Pfaltzgraff, Jr., Uri Ra'anan and Warren Milberg, 187-211. Hamden, CT: Archon Books, 1981.

________. "Intelligence and Deception." *Journal of Strategic Studies* 5, no. 1 (March 1982): 122-154.

________. "Intelligence and the Problem of Strategic Surprise." *Journal of Strategic Studies* 7, no. 3 (September 1984): 229-281.

________. "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty." In *Intelligence: Policy and Process*, ed. Alfred C. Maurer, Marion D. Tunstall and James M. Keagle, 239-269. Boulder, CO: Westview Press, 1985.

________. "Introduction: Strategic and Operational Deception in Historical Perspective." *Intelligence and National Security* 2, no. 3 (July 1987): 1-91.

________. "Technological Surprise in War." *Intelligence and National Security* 2, no. 1 (January 1987): 5-53.

Hastedt, Glenn P. "The New Context of Intelligence Estimating: Politicization or Publicizing?" In *Intelligence and Intelligence Policy in a Democratic Society*, ed. Stephen J. Cimbala, 47-67. Dobbs Ferry, NY: Transnational Publishers, Inc., 1987.

________. "Intelligence Failure and Terrorism: The Attack on the Marines in Beirut." *Conflict Quarterly* VIII, no. 2 (Spring 1988): 7-22.

Herbig, Katherine L., and Donald C. Daniel. "Strategic Military Deception." In *Intelligence: Policy and Process*, ed. Alfred C. Maurer, Marion D. Tunstall and James M. Keagle, 270-293. Boulder, CO: Westview Press, 1985.

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

________. *Intelligence Services in the Information Age: Theory and Practice*. London: Frank Cass, 2001.

Heuer, Richards J., Jr. "Strategic Deception and Counterdeception: A Cognitive Process Approach." *International Studies Quarterly* 25, no. 2 (June 1981): 294-327.

________. *Psychology of Intelligence Analysis*. Washington, DC: CIA Center for the Study of Intelligence, 1995.

Hof, Frederic C. "The Beirut Bombing of October 1983: An Act of Terrorism." *Parameters* XV, no. 2 (Summer 1985): 69-74.

Hoffman, Bruce. "Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post-Cold War Era." *Intelligence and National Security* 11, no. 2 (April 1996): 207-223.

Holst, Johan Jorgen. "Surprise, Signals and Reaction: The Attack on Norway April 9th 1940--Some Observations." *Cooperation and Conflict* (vol I 1986): 31-45.

Hopple, Gerald W. "Intelligence and Warning: Implications and Lessons of the Falkland Islands War." *World Politics* 36, no. 3 (April 1984): 339-361.

Hubbard, Robert L. "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements." *Defense Intelligence Journal* 11, no. 1 (Winter 2002): 71-80.

Hughes, Thomas L. *The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making*: Foreign Policy Association Headline Series No. 233, 1976.

Hulnick, Arthur S. "Relations between Intelligence Producers and Policy Consumers: A New Way of Looking at an Old Problem." In *Intelligence and Intelligence Policy in a Democratic Society*, ed. Stephen J. Cimbala, 129-144. Dobbs Ferry, NY: Transnational Publishers, Inc., 1987.

________. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*. Westport, CT: Praeger, 1999.

Jajko, Walter. "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning." *Comparative Strategy* 21, no. 5 (October-December 2002): 351-363.

Jenkins, Brian Michael. *The Lessons of Beirut: Testimony before the Long Commission*. RAND Note N-2114-RC, available at www.beirut-memorial.org/history, 1984.

Jervis, Robert. "What's Wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 28-41.

________. "Intelligence and Foreign Policy." *International Security* 11, no. 3 (Winter 1986-1987): 141-161.

Johnson, Loch K. "Challenges of Strategic Intelligence." *Intelligence and National Security* 5, no. 3 (July 1990): 215-225.

________. "Analysis for a New Age." *Intelligence and National Security* 11, no. 4 (October 1996): 657-671.

________. *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*. New York, NY: New York University Press, 2000.

________. "Bricks and Mortar for a Theory of Intelligence." *Comparative Strategy* 22, no. 1 (January-March 2003): 1-28.

Kahn, David. "The Intelligence Failure at Pearl Harbor." *Foreign Affairs* 70, no. 5 (Winter 1991/1992): 138-152.

________. "Toward a Theory of Intelligence." *Military History Quarterly*, Winter 1994, 92-97.

________. "An Historical Theory of Intelligence." *Intelligence and National Security* 16, no. 3 (Autumn 2001): 79-92.

Kam, Ephraim. *Surprise Attack: The Victim's Perspective*. Cambridge, MA: Harvard University Press, 1988.

Kauppi, Mark V. "Counterterrorism Analysis 101." *Defense Intelligence Journal* 11, no. 1 (Winter 2002): 39-53.

Kendall, Willmoore. "The Function of Intelligence." *World Politics*, July 1949, 542-552.

Kennedy, David, and Leslie Brunetta. *Lebanon and the Intelligence Community*. Harvard University Kennedy School of Government Case C15-88-859.0, 1988.

________. "Lebanon and the Intelligence Community: A Case Study." *Studies in Intelligence* 37, no. 5 (nd 1994): 37-51.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1949.

________. "Estimates and Influence." *Foreign Service Journal* 46, no. 5 (April 1969): 16-18, 45.

Kerstetter, Wayne A. "Terrorism and Intelligence." *Terrorism: An International Journal* 3, no. 1-21979): 109-115.

Kirkpatrick, Lyman B., Jr. *Captains without Eyes: Intelligence Failures in World War II*. London: Macmillan, 1969.

Knorr, Klaus. "Failures in National Intelligence Estimates: The Case of the Cuban Missiles." *World Politics* 16, no. 3 (April 1964): 455-467.

________. "Lessons for Statecraft." In *Strategic Military Surprise: Incentives and Opportunities*, ed. Klaus Knorr and Patrick Morgan, 247-265. New Brunswick, NJ: Transaction Books, 1983.

La Porte, Todd R., and Paula M. Consolini. "Working in Practice but Not in Theory: Theoretical Challenges of 'High Reliability Organizations'." *Journal of Public Administration Research and Theory* 1, no. 1 (January 1991): 19-47.

Laqueur, Walter. *A World of Secrets: The Uses and Limits of Intelligence*. New York: Basic Books, 1985.

Lesser, Ian O. *Countering the New Terrorism*. Santa Monica, CA: RAND, 1999.

Levite, Ariel. *Intelligence and Strategic Surprise.* New York: Columbia University Press, 1987.

________. "*Intelligence and Strategic Surprise* Revisited: A Response to Richard K. Betts's 'Surprise, Scholasticism, and Strategy'." *International Studies Quarterly* 33, no. 3 (September 1989): 345-349.

Livingstone, Neil C. "The Impact of Technological Innovation." In *Hydra of Carnage: The International Linkages of Terrorism and Other Low-Intensity Operations*, ed. Uri Ra'anan, et al. Lexington, MA: Lexington Books, 1986.

Lowenthal, Mark M. "The Burdensome Concept of Failure." In *Intelligence: Policy and Process*, ed. Alfred C. Maurer, Marion D. Tunstall and James M. Keagle, 43-56. Boulder, CO: Westview Press, 1985.

________. "Tribal Tongues: Intelligence Consumers, Intelligence Producers." *The Washington Quarterly* 15, no. 1 (Winter 1992): 157-168.

________. *Intelligence: From Secrets to Policy*. 2d ed. Washington, DC: CQ Press, 2003.

Luttwak, Edward N. *The Pentagon and the Art of War*. NY: Simon and Schuster, 1984.

Manthorpe, William H. J., Jr. "From the Editor." *Defense Intelligence Journal* 7, no. 2 (Fall 1998): 5-8.

Mark, Hans. *The Doctrine of Command, Control, Communications, and Intelligence: A Gentle Critique*. Harvard University: Program on Information Resources Policy Guest Presentations, 2000.

Martin, David C., and John Walcott. *Best Laid Plans: The Inside Story of America's War Against Terrorism*. New York: Harper & Row, 1988.

Matthias, Willard C. *America's Strategic Blunders: Intelligence Analysis and National Security Policy, 1936-1991*. University Park, PA: Pennsylvania State University, 2001.

May, Ernest R. "Conclusions: Capabilities and Proclivities." In *Knowing One's Enemies: Intelligence Assessment before the Two World Wars*, ed. Ernest R. May, 503-542. Princeton: Princeton University Press, 1984.

________. *Strange Victory: Hitler's Conquest of France*. New York, NY: Hill and Wang, 2000.

McCarthy, Mary O. "The Mission to Warn: Disaster Looms." *Defense Intelligence Journal* 7, no. 2 (Fall 1998): 17-31.

McCarthy, Shaun P. *The Function of Intelligence in Crisis Management: Towards an Understanding of the Intelligence Producer-Consumer Dichotomy*. Aldershot, England: Ashgate, 1998.

McGarvey, Patrick J. "DIA: Intelligence to Please." In *Readings in American Foreign Policy: A Bureaucratic Perspective*, ed. Morton H. Halperin and Arnold Kanter, 318-328. Boston, MA: Little, Brown, 1973.

Morone, Joseph G., and Edward I. Woodhouse. *Averting Catastrophe: Strategies for Regulating Risky Technologies*. Berkeley, CA: University of California Press, 1986.

Motley, James Berry. "International Terrorism: A Challenge for U.S. Intelligence." *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 83-96.

________. "Coping with the Terrorist Threat: The U.S. Intelligence Dilemma." In *Intelligence and Intelligence Policy in a Democratic Society*, ed. Stephen J. Cimbala, 165-175. Dobbs Ferry, NY: Transnational Publishers, Inc, 1987.

National Commission on Terrorism. *Countering the Changing Threat of International Terrorism*. Report of the Congressionally mandated commission chaired by L. Paul Bremer III, June 7, 2000, available at: w3.access.gpo.gov/nct.

Nye, Joseph S., Jr. "Peering into the Future." *Foreign Affairs* (July/August 1994): 82-93.

Nye, Joseph S., Jr., and William A. Owens. "America's Information Edge." *Foreign Affairs* 75, no. 2 (March-April 1996): 20-36.

Oettinger, Anthony G. "Knowledge Innovations: The Endless Adventure." *Bulletin of the American Society for Information Science and Technology* 27, no. 2 (December/January 2001): 10-15.

Parker, Charles F., and Eric K. Stern. "Blindsided? September 11 and the Origins of Strategic Surprise." *Political Psychology* 23, no. 3 (September 2002): 601-630.

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. New York, NY: Basic Books, 1984.

Pillar, Paul R. *Terrorism and U.S. Foreign Policy*. Washington: Brookings, 2001.

________. "Fighting International Terrorism: Beyond September 11th." *Defense Intelligence Journal* 11, no. 1 (Winter 2002): 17-26.

Poteat, Eugene. "The Use and Abuse of Intelligence: An Intelligence Provider's Perspective." *Diplomacy and Statecraft* 11, no. 2 (July 2000): 1-16.

Poteat, George H. "The Intelligence Gap: Hypotheses on the Process of Surprise." *International Studies Notes* 3, no. 3 (Fall 1976): 14-18.

Prados, John. *America Confronts Terrorism: Understanding the Danger and How to Think About It*. Chicago: Ivan R. Dee, 2002.

Ransom, Harry Howe. "Strategic Intelligence and Foreign Policy." *World Politics* 27, no. 1 (October 1974): 131-146.

"Reinventing War." *Foreign Policy*, Nov/Dec 2001, 30-47.

Report of the Accountability Review Board on the Embassy Bombings in Nairobi and Dar Es Salaam on August 7, 1998. ADM William J. Crowe (ret), Chairman, available at www.fas.org/irp/threat/arb/board_overview.html, 1999.

Roberts, Karlene H. "The Significance of Perrow's *Normal Accidents: Living with High-Risk Technologies*." *The Academy of Management Review* 14, no. 2 (April 1989): 285-289.

Rochlin, Gene I., Todd R. La Porte, and Karlene H. Roberts. "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea." *Naval War College Review* LI, no. 3 (Summer 1998): 97-113; originally published in Autumn 1987 issue.

Rousseau, Denise M. "Review of *the Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, by Scott D. Sagan." *Administrative Science Quarterly* 41, no. 1 (March 1996): 200-203.

Sagan, Scott D. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, NJ: Princeton University Press, 1993.

Shlaim, Avi. "Failures in National Intelligence Estimates: The Case of the Yom Kippur War." *World Politics* 28, no. 3 (April 1976): 348-380.

Shulsky, Abram N. "Elements of Strategic Denial and Deception." In *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz, 15-33. New Brunswick, NJ: Transaction Publishers, 2002.

Shulsky, Abram N., and Gary J. Schmitt. *Silent Warfare: Understanding the World of Intelligence, 3d Ed*. Washington, DC: Brassey's, 2002.

Snook, Scott A. *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*. Paperback ed. Princeton, NJ: Princeton University Press, 2002.

Steele, Robert David. *On Intelligence: Spies and Secrecy in an Open World*. Oakton, VA: OSS International Press, 2001.

________. "Crafting Intelligence in the Aftermath of Disaster." *International Journal of Intelligence and Counterintelligence* 15, no. 2 (Summer 2002): 161-178.

Stein, Janice Gross. "'Intelligence' and 'Stupidity' Reconsidered: Estimation and Decision in Israel, 1973." *Journal of Strategic Studies* 3, no. 2 (September 1980): 147-177.

________. "Military Deception, Strategic Surprise, and Conventional Deterrence: A Political Analysis of Egypt and Israel, 1971-73." *Journal of Strategic Studies* 5, no. 1 (March 1982): 94-121.

Taubman, Philip, and Joel Brinkley. "The U.S. Marine Tragedy: Causes and Responsibility." *New York Times*, December 11 1983, accessed via LexisNexis. Special report in eight separate articles.

Turner, Stansfield. "Intelligence for a New World Order." *Foreign Affairs* 70, no. 4 (Fall 1991): 150-166.

U.S. Congress, House. "Adequacy of U.S. Marine Corps Security in Beirut." Committee on Armed Services, Investigations Subcommittee. Washington: GPO, December 19, 1983.

________. *U.S. Intelligence Performance and the September 20, 1984, Beirut Bombing*. Permanent Select Committee on Intelligence, October 3, 1984. Washington: GPO, 1984.

________. "Review of Adequacy of Security Arrangements for Marines in Lebanon and Plans for Improving That Security." Committee on Armed Services, Investigations Subcommittee, November-December 1983. Washington: GPO, 1985.

U.S. Congress, Senate. *The Security of American Personnel in Lebanon*. Committee on Foreign Relations, Staff Report, October 1984. Washington: GPO, 1984.

________. *Saudi Arabia and Beirut: Lesson Learned on Intelligence Support and Counterterrorism Programs*. Select Committee on Intelligence, Hearings July 9, 1996. Washington: GPO, 1996.

U.S. Department of Defense. *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*. Washington: GPO, 1984.

Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, IL: University of Chicago Press, 1996.

Vertzberger, Yaacov. "India's Strategic Posture and the Border War Defeat of 1962: A Case Study in Miscalculation." *Journal of Strategic Studies* 5, no. 3 (September 1982): 370-392.

Vickers, Robert D., Jr. "The State of Warning Today." *Defense Intelligence Journal* 7, no. 2 (Fall 1998): 9-15.

Warner, Michael. "Wanted: A Definition of Intelligence." *Studies in Intelligence*, no date 2002, 15-22.

Wasserman, Benno. "The Failure of Intelligence Prediction." *Political Studies* 8, no. 2 (June 1960): 156-169.

Weick, Karl E., and Karlene H. Roberts. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks." *Administrative Science Quarterly* 38, no. 3 (September 1993): 357-381.

Whaley, Barton. *Codeword Barbarossa*. Cambridge, MA: The MIT Press, 1973.

________. "Toward a General Theory of Deception." *Journal of Strategic Studies* 5, no. 1 (March 1982): 178-192.

________. "Conditions Making for Success and Failure of Denial and Deception: Authoritarian and Transition Regimes." In *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz, 41-94. New Brunswick, NJ: Transaction Publishers, 2002.

Whaley, Barton, and Jeffrey Busby. "Detecting Deception: Practice, Practitioners, and Theory." In *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz, 181-221. New Brunswick, NJ: Transaction Publishers, 2002.

Wirtz, James J. *The Tet Offensive: Intelligence Failure in War*. Ithaca, NY: Cornell University Press, 1991.

________. "Deja Vu? Comparing Pearl Harbor and September 11." *Harvard International Review* (Fall 2002): 73-77.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.