Analyzing Intelligence
National Security Practitioners' Perspectives
Second Edition
Roger Z. George and James B. Bruce, Editors
Georgetown University Press
Washington, DC
2014

CHAPTER 12

Foreign Denial and Deception: Analytic Imperatives

JAMES B. BRUCE AND MICHAEL BENNETT

We must significantly reduce our vulnerability to intelligence surprises, mistakes, and omissions caused by the effects of denial and deception (D&D) on collection and analysis.

—President's Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction, March 2005

Foreign denial and deception (D&D) is a fact of life for every intelligence analyst who has ever worked a "hard target."[1] Such targets are objects of high intelligence interest and are considered to be hard because they defy a wide variety of ordinary collection methods and pose the most difficult analytic challenges. The standard collection activities such as human intelligence (HUMINT), signals intelligence (SIGINT), and imagery or geospatial intelligence (GEOINT) are typically less productive against such targets because the countermeasures these targets take against collection reduce, and sometimes confuse, the factual basis for analytic understanding. During the Cold War, the Soviet Union was the exemplary hard target. Today countries such as China, North Korea, and Iran, along with post-Soviet Russia offer the best examples, as well as such nonstate actors as international terrorist groups, including al-Qaeda and other networks that seek weapons of mass destruction (WMDs).

What Is Denial and Deception?

Highly relevant to national-level policymakers and to warfighters, D&D is defined as any undertaking (activity or program) by adversaries—state and nonstate actors alike—to influence or deceive policymaking and intelligence communities by reducing collection effectiveness, manipulating information, or otherwise attempting to manage perceptions of intelligence producers and consumers (for example, policymakers and warfighters). Those who practice D&D seek to shape the decisions and actions of policymakers by

manipulating their perceptions. Notably the perceptions of these intelligence consumers can be shaped by influencing the intelligence they receive. More specifically:

- *Denial* refers to activities and programs designed to eliminate, impair, degrade, or neutralize the effectiveness of intelligence collection within and across any or all collection disciplines, human and technical. The goal is to distort intelligence by depriving it of information it requires for a more complete and accurate understanding.
- *Deception* refers to *manipulation* of intelligence collection, analysis, or public opinion by introducing false, misleading, or even true but tailored information into intelligence channels with the intent of manipulating the perceptions of policymakers in order to influence their actions and decisions. The goal is to *influence* judgments made by intelligence producers and thus the consumers of their products.

Since intelligence collection and analysis can play a significant role in shaping policymaker perceptions, intelligence agencies are a key target for the deception planner.

Effective D&D has the potential to significantly degrade US intelligence capabilities by attacking vulnerabilities in collection and analysis. Such vulnerabilities tend to be costly to the targeted intelligence organization as can be seen in previous US intelligence failures. As shown in chapter 10, of the eight cases of failure examined there, deception was a factor in most, and denial was a factor in all. That denial is a factor in all these failures suggests that it is not only pervasive but also consequential. Though deception is far less common than denial—it is held in reserve for only the rare but perfect circumstances—its batting average is extraordinarily high, succeeding more than nine times of every ten it is used.[2]

An important historical example of D&D is illustrated in the surprise military attack that Japan conducted against the United States at Pearl Harbor in 1941. The Japanese denial measures successfully concealed the eleven-day transit of a massive naval task force that conducted the attack, killing 2,400 unsuspecting Americans and bringing the United States into World War II. Deception measures were so successful that even Japanese intentions to go to war with the United States were never comprehended by US intelligence, policy, and military officials (see box 12.1).

It is clear from historical cases as well as more recent ones that analysts who underestimate the power of D&D increase their vulnerabilities to its effects, while those who are equipped to understand and counter the techniques that D&D practitioners use will perform better against not only hard targets but also any targets no matter their complexity. Successfully countering D&D holds the key to avoiding tactical and strategic surprise.

Denial: Foundations for Poor Intelligence

Denial of intelligence collection is a significant impediment to successful analysis. As shown in chapter 10, that denial effectively neutralized collection in major US intelligence failures is one thing. But analysts' failure to understand and correct for successful

BOX 12.1 Japanese Denial and Deception in the Pearl Harbor Attack

Denial: Intelligence was denied through effective operational security:

- Radio communication among ships in the task force were forbidden beginning on November 10.
- Naval call signs were changed twice between November 1 and December 1 prior to the attacks, slowing any US translations of radio intercepts.
- The northern rendezvous point off Etorofu Island was chosen because it was unlikely to be observed, even by Japanese citizens.
- The military concealed the purchase and attainment of clothing, equipment, and supplies for the rendezvous point and for the northern journey toward Pearl Harbor.
- Dumping of garbage or waste into the water from ships in the task force was forbidden to reduce the likelihood of detection.
- Only top Japanese naval planning officers were aware of the Pearl Harbor plan; military Cabinet secretaries were informed only late in the game, and some Cabinet members were never informed prior to the attack.
- Members of the ships' crews were kept unaware of their destination until after their departure.
- Pilots and crews training for the attack knew nothing of the ultimate purpose of their training.

Deception: Expectations of attack were reduced through manipulating information and perceptions:

- Japan sought to create the illusion that the task force was still in training at Kyushu. The main force in the Inland Sea created massive, deceptive communications to manufacture this ploy. This deception was reinforced by allowing a large number of shore leaves in Tokyo and Yokohama for naval men.
- Japanese military commanders in other theaters such as in Indochina were given false plans for military campaigns other than those actually being planned.
- The Japanese navy issued a war plan on November 5 with full and accurate details of planned attacks on the Philippines and Southeast Asia but omitted any reference to the Pearl Harbor mission whose orders had been communicated verbally.
- The Foreign Office announced that one of its largest ocean liners would sail on December 2 to California and Panama to evacuate Japanese citizens, giving the impression that Japan would not commence hostilities while its liner was at sea.
- The Japanese government and press continued to play up the Japanese–American negotiations prior to the attack.

Sources: Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Palo Alto, Calif.: Stanford University Press, 1962), 368–85, and Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College, Center for Strategic Intelligence Research, 2002), 121–22.

denial is quite another. In general, analysts need a much better understanding of the impact of intelligence denial on their analysis. Often they may not even be aware that needed information has not been collected, even though it may bear directly on the issue that they are analyzing. When denial measures succeed against the collection disciplines, human and technical, the result is that intelligence sought is intelligence denied. We are thus left with "missing information."

But even when we know that certain missing information is the result of effective denial, the *impact* of that denial on analytic processes and findings is often poorly understood. No one doubts that intelligence findings about any difficult issue (for example, in terrorism, WMDs, or warning situations) would be different if more and better information had been collected. But the potential impact on analysis of important information that is *not* collected can also distort results. Analytic judgments based on missing information are inherently uncertain; they may also be wrong. Had analysts better identified the impact of missing information on their analysis of Iraqi WMDs, a more reliable estimate might have been the result.

Targets of intelligence collection that wish to avert discovery or observation generally have two resources at their disposal: knowledge of their adversary's collection capabilities and use of countermeasures against the collection activities they aim to degrade, such as camouflage against imagery or other direct observation. There are good reasons that Iran chose to place its uranium enrichment efforts in underground facilities (UGFs) at Natanz and Qom—UGFs offer excellent means to negate overhead imagery. Good D&D practitioners have countermeasures that work against not only imagery but also human and signals collection efforts. Though much of denial activity is passive, such as practicing good operational security and just "staying below the radar," hard targets are notable for their sophisticated denial capabilities, which are not merely passive but also seek to actively neutralize intelligence collection methods. Their ability to do this entails an understanding of collection programs that cannot normally be attained at unclassified levels. Sophisticated denial capabilities successfully exploit classified information about collection sources and methods that has been compromised in some way or another, often through spies or through press leaks and other disclosures that may or may not have been authorized. The cumulative effects of many and frequently major disclosures enable D&D practitioners to actively deny US collection efforts.

Effective D&D programs thus require good knowledge of the collection that targets them—it is the bedrock of effective denial. Because all collection disciplines save for open sources are intended to work secretly or clandestinely, their effectiveness depends on how well their secrecy works. As intelligence is the collection of secret information by secret means, acquiring the target's secrets (such as plans for surprise attack) presumes that the most effective collection methods remain a secret.

Secrecy is the opposite of transparency. As an intelligence service's methods become more transparent, its loss of secrecy necessarily impairs its effectiveness. A priority objective of smart intelligence targets is acquiring information that compromises the secrecy of intelligence collection sources and methods. All hard targets conduct priority efforts

to learn how to defeat collection. This knowledge can be acquired through both authorized disclosures, such as intelligence sharing or diplomatic demarches, and unauthorized disclosures, such as media leaks that disclose classified information.[3] In particular, media leaks, according to the report of the WMD Commission, "have significantly impaired US intelligence capabilities against the hardest targets."[4] When secret collection capabilities are compromised, analysis is also impaired. Analysts are not only denied information later as a result—they also need to understand the impact of compromises at least as well as the D&D practitioners that defeat transparent collection and thereby degrade analysis.

In general, the effectiveness of denial techniques against collection is often better than it seems. As we come to appreciate the impact of key gaps in our information that result from effective denial, both collectors and analysts need a better understanding about unproductive or unsuccessful collection operations in all disciplines and why they are not productive. Overcoming key intelligence gaps produced by adversaries' denial activities will require much more effective counterdenial approaches if analysts are to succeed.

Principles of Deception

If denial is the foundation of D&D, then deception is the silver bullet that almost never misses. Dodging the bullet requires an understanding of how deception works. Based on a comprehensive review of the literature on deception, including a large number of historical cases, Michael Bennett and Edward Waltz have described four fundamental principles of deception:

- Truth. All deception works within the context of what is true.
- Denial. Denying the target access to select aspects of the truth is the prerequisite to all deception.
- Deceit. All deception requires and utilizes deceit.
- Misdirection. Deception depends on manipulating what the target registers.[5]

These principles can be used as a framework for understanding the deception process by examining the relationship between the deceiver and the target of the deception and why deception is almost always successful.

It might seem odd that *truth* should be a principle of deception. But if deception is to work at all, there must be a foundation of accepted perceptions and beliefs about the world that can be exploited. This first principle is based on the study of deception in nature (that is, with plants and animals) and the observation that most organisms expect an honest response when signaling another organism.[6] Such interactions make deception possible when honest signals produce an unexpected or even dishonest response. In D&D the selective use of the truth—supplying the target with authentic data—establishes the credibility of those channels of communication on which the target depends, such as particular collection disciplines and information collected by them.

Denial, on the other hand makes deception possible by creating the opportunities the deceiver needs to manipulate the target's perceptions. Denial conceals selected aspects of what is true, such as the deceiver's real intentions and capabilities, and denial used alone can have serious consequences even when intentional deception is not a factor. Thus, as the Pearl Harbor example illustrates, denial is also the foundation on which deception is carried out.

Together truth and denial set the stage for deception methods associated with *deceit*, the most obvious deception principle. Barton Whaley calls deceit in the form of disinformation the "most important single broad category of ruses."[7] Without deliberate deceit, the target is only the victim of misperceptions due to misinformation and/or self-deception, not deception. But when these first three principles are integrated, they allow the deceiver to present the deception target with what appears to be highly desirable, genuine data while reducing or eliminating the real signals that the target needs to form accurate perceptions of the situation. The end result is that the target must rely on data that has been deliberately fashioned so as to manipulate his perceptions to the deceiver's benefit.

With a few notable exceptions, the strategic deception literature generally does not recognize the fourth principle, *misdirection*, as a distinct concept, although numerous authors consider it to be the very foundation of magic.[8] In magic, misdirection diverts the audience's attention toward the magic effect and away from the method that produces it. The history of deception is filled with examples where the deceiver either deliberately redirects the target's attention or exploits environmental factors that have the same effect. For example, a feint is perceived as a *real* attack (the truth principle), not a false one; it is used to redirect the adversary's attention away from where the real attack will occur.

Used in concert, these four principles are exercised by the deceiver in a way to control what the target of the deception observes and, as a result, what the target registers and thus what the target perceives. When deception succeeds, it causes the target to act to the deceiver's advantage and to his own disadvantage.

Bias Traps and Analytic Vulnerabilities

The deception principles described above illustrate how deceivers exploit very basic human vulnerabilities at several levels. These vulnerabilities can be attributed to biases—systematic errors in perception, judgment, and reasoning—that fall into three major categories: cultural and personal biases, organizational biases, and cognitive biases.[9]

Cultural and personal biases are the result of interpreting and judging phenomena in terms of the preconceptions and beliefs that are formed by the individual's personal experiences. These are further influenced by the knowledge, beliefs, customs, morals, habits, and cognitive styles that the individual acquires as a member of his or her specific social environment—that is, culture. The preconceptions and beliefs that result can be extremely resistant to change, even in the face of large amounts of discrepant

information, and they can thus be exploited by deception planners. Such biases also affect the way analysts interpret events. Cultural biases can also influence how people go about solving problems and analyzing situations, and analytic flaws such as mirror imaging may be the result. Such personal traits as overconfidence (hubris) can facilitate being deceived. As Roy Godson and James J. Wirtz point out, the successful deceiver "must recognize the target's perceptual context to know what (false) pictures of the world will appear plausible."[10]

Organizational biases are similar to cultural biases and are generally associated with the limitations and weaknesses of large bureaucratic organizations. These biases are the result of the goals, mores, policies, and traditions that characterize the specific organization in which the individual works and often appear in the form of barriers to the flow of information within and between organizations. An even more insidious bias appears in the manner in which the very nature of the information about a specific topic changes as it winds up flowing through different channels. Such differences in information across linked organizations such as in the intelligence community are even more extreme when classified information is involved. Barriers to information flows and differences in perception due to the uneven distribution of compartmented information, as shown above, contributed heavily to the American failure to anticipate the Japanese attack on Pearl Harbor. Such barriers and differences in perception also played a role in the failure to anticipate the terrorist attacks on September 11, 2001.[11]

Two prominent organizational biases in intelligence agencies are the search for consensus and time pressures. As we have learned in discovering the rationale for alternative analysis, if consensus becomes a goal in and of itself, it may deprive decision makers of important information about potential weaknesses in the analytic judgments presented, as well as the existence and grounds of alternative views. A second bias, time pressure, is inherent in fast-paced analysis, particularly current intelligence. Analysts have always been under pressure to provide timely intelligence. But the post-9/11 threat environment and congressional pressure for a quick answer, as we saw with Iraqi WMDs, may exert added pressure on analysts to make judgments prematurely. Like the pressure for consensus, time pressures may also elevate the impact of cognitive biases that increase susceptibility to deception.

Cognitive heuristics represent a wide variety of adaptation mechanisms that help humans to accurately perceive and understand the world around them on a day-to-day basis. They usually help us by reducing the complexity of difficult problems (for example, assessing probabilities). These same processes, however, also make us vulnerable to optical illusions, magician's tricks, con artists, and, of special interest to us, military and political deception. It is impossible to survey the range of cognitive biases that are relevant to denial and deception here.[12] Fortunately, professor of psychology Thomas Gilovich provides an excellent framework for capturing the role these heuristics and biases play in deception. He summarizes much of the social and cognitive psychology research into what he calls *determinants of questionable and erroneous beliefs* and organizes them into categories, three of which are especially relevant to D&D:[13]

- Too much from too little—the tendency to form judgments from incomplete or unrepresentative information and to be overconfident about those judgments
- Seeing what we expect to see—the tendency for our expectations, preconceptions, and prior beliefs to influence the interpretation of new information in ways to support our present beliefs
- Believing what we are told—the tendency for a good story to seem credible and to bias one's beliefs

The powerful cognitive traps that Gilovich describes here were very much in evidence in the faulty national intelligence estimate that erroneously judged Iraq to have weapons of mass destruction in 2002, more than a decade after the WMD programs had actually been shut down. See box 12.2.

Together the four principles of deception and Gilovich's determinants of questionable beliefs provide a framework for understanding analysts' vulnerabilities as they apply to D&D. They show how a deceiver can exploit each of the deception principles to gain advantage. For example, from the deception planner's perspective, revealing some truth to the target provides several advantages. In the case of *too much from too little*, selective truth can convince a target of deception—for example, that something exists when it does not. The Allies took advantage of this in World War II when feeding information to the Germans in order to create the false order of battle for FUSAG and other elements of the Fortitude deception plan.[14] The *too much from too little* bias sets the analyst up to misinterpret limited information. Providing truthful information also allows the deceiver to exploit the *believing what we are told* determinant. By incorporating real events, people, organizations, equipment, and information into the deception story, the deceiver can increase the story's immediacy and plausibility, thus making it more believable. This also acts to increase the target's confidence in his sources of information, and it is that confidence in those channels that is critical to the success of deception. The deceiver will use those same channels later, such as a controlled source believed by the target to be reliable, to pass false information in order to build up the deception story (the principle of deceit).

BOX 12.2 Iraq WMDs: A Deception Paradox

Deception is characteristically complex. Iraq's D&D overreached, fooled the IC, and backfired.

Saddam Hussein had two target audiences for his deception plan: (1) the United Nations and the West, whom he wanted to assure that he was in full compliance with sanctions and that he had shut down his WMD programs, and (2) his enemies, internally the Kurds (previous targets of his chemical weapons attacks) and the Shiites, and externally Iran and Israel, against whom he wanted to posture as a powerful tyrant and leader in full possession of the robust WMD arsenal he had built before Desert Storm curtailed them in 1990.

The burden of his deception plan was to sustain the contradictory narratives to each audience for as long as possible—to the UN and the West, he had shut down his weapons programs, but to his enemies, he retained them. Both could not be true at once. What was the truth?

The 2002 national intelligence estimate on Iraq WMD acknowledged Iraq's major denial-and-deception efforts and correctly judged them as major impediments to assessing WMDs. But it wrongly concluded that these D&D countermeasures to US intelligence were concealing WMDs. And this erroneous judgment was well supported by Saddam's repeated refusals to provide the UN with documentation supporting his claims that he had destroyed the weapons. In truth these D&D efforts were concealing the *absence* of such weapons, as we later learned Saddam had actually shut down the full range of his CW, BW, and nuclear programs after Desert Storm.

This case illustrates a deception paradox: While analysts correctly understood the scope and impact of the Iraqi D&D program, they misunderstood its purposes. In assuming that D&D was intended to conceal WMDs and not their absence, faulty analysis here illustrates the seduction of the cognitive traps that Gilovich warns against:

- *Too much from too little:* Iraq's successful denial efforts deprived analysts of needed information to understand intentions, so analysts drew unwarranted conclusions about them from too little evidence. His intentions spanned a broader audience than one.
- *Seeing what we expect to see:* Analysts expected to see D&D, which they did, and to see it conceal a major WMD program, which it didn't. They did not expect D&D to conceal the fact that the weapons program had been shut down. In not seeing the weapons, and in concluding that D&D must be hiding them, they judged WMD as present, not absent.
- *Believing what we are told:* Although analysts are inherently skeptical and cannot really be "told" anything, they accepted the past "analytic line" uncritically—namely, that Iraq possessed WMDs before 1990 (which was true) and, lacking convincing evidence to the contrary, believed it must still be true in 2002 (which was false).

These are preventable errors. Good D&D analysis should make use of such structured analytic techniques as Analysis of Competing Hypotheses, Key Assumptions Check, and Structured Brainstorming. This tradecraft almost certainly would have revealed the snare of these cognitive biases and resulted in more accurate analytic judgments.

Sources: For elaboration, see Bruce, "Denial and Deception in the 21st Century," in *Defense Intelligence Journal* 15, no. 2 (2006): note 1, 18–22, and chapter 14, for tradecraft discussion. Michael I. Handel explains how both denial and deception support military intentions and capabilities in *War, Strategy, and Intelligence* (London: Frank Cass, 1989), 314–16 and figure 2.

Denial has its greatest impact through the *seeing what we expect to see* set of biases. Research studies and real-world events have repeatedly demonstrated that individuals consistently fail to appreciate the limits of the data and information available to them.[15] What is unknown, what is out of sight, is out of mind. Effective denial techniques mean that what little information is available, no matter how ambiguous, may be eagerly grasped and fit to existing expectations and preconceptions. Denial, therefore, is the key to making sure that nothing significant occurs to change the target's mind once the deception plan is put into motion.

Deceit is probably the first thing one thinks of with regard to the relationship between deception and *believing what we are told*. After all, it is deceit in the form of double agents, deception operations such as Mincemeat, security "leaks," and exotic camouflage techniques that give deception its historical importance.[16] Analysts and decision makers depend heavily on secondhand information, and this dependence makes them vulnerable to serious biases and errors, especially if those sources are providing false or inaccurate information. More important, deceit exploits the *seeing what we expect to see* bias when analysts readily accept disinformation and fit it to their existing expectations and preconceptions.

Misdirection can be of two general types: one physical, the other psychological.[17] In World War II, for example, the Allies always made sure to pass information to the Germans about the movement of both real and fictional units (that is, truth and deceit) to reinforce their expectations, as well as to distract their attention from the real buildup in southwestern England.

Principles of Counterdeception

To succeed against smart adversaries for whom denial and deception are key weapons in their security arsenals, intelligence analysts must master counter-D&D understanding, principles, and skills, learn to assess the impact of missing information on their analytic judgments, develop significant expertise in the collection disciplines, and adjust for unwarranted dependency on inadequate information. These imperatives find their practical justification in the experience of poor intelligence community performance against foreign D&D and their theoretical justification in sound counterdeception principles.

Bennett and Waltz's review of the deception literature produced not only fundamental deception principles but also yielded four *counter*deception principles, all of which point to the analyst's level of knowledge and understanding:

- Know yourself.
- Know your adversary.
- Know your situation.
- Know your channels.

Understanding and acting on these principles is prerequisite to an analytic posture to reduce vulnerability to D&D and mitigate its effects when it succeeds.

Drawing from the work of Heuer and the cognitive heuristics literature leads to the first fundamental principle of counterdeception: *Know yourself.* Put succinctly, this principle stresses that the analyst's first defense against D&D is a sound understanding of those cognitive vulnerabilities discussed above. Sun Tzu makes it clear that you must know yourself if you wish to have any reasonable hope of success in battle.[18] The same is true for the battle waged between deceiver and target. Whaley has demonstrated how deception can be particularly successful when it exploits the target's expectations and preconceptions (the *seeing what we expect to see* bias).

The *know your adversary* principle should be a constant reminder to analysts and decision makers to consider the means, motives, and culture of their adversary. The means that the adversary has at his or her disposal include doctrine, training, personnel, experience, and technology for concealing or exaggerating intentions, capabilities, and activities. Historically motives have generally included achieving surprise, bluffing, deterrence, seeking prestige or influence, blackmail, and seeking concessions from the target. Today specific D&D motives include concealing WMD capabilities and transactions and planning terrorist attacks. This principle also stresses the need to develop the depth of knowledge of the adversary that makes it possible to begin breaking down ethnocentric biases and come to see things from the adversary's perspective. As Dewar noted, being able to put yourself into the mind of the adversary may be the counterdeception analyst's most effective weapon.[19]

Analysts throughout the intelligence community require a much better understanding of adversarial D&D capabilities than they routinely exhibit. If they do not understand an adversary's D&D capabilities, they cannot be expected to understand how effective—or how hobbled—their nation's intelligence will be when working against that adversary. Analysts who are assigned a specific country or nonstate actor account should make it their first priority to learn all they can about the D&D capabilities that their assigned target can mount against the specific collection disciplines that produce intelligence on that target.

The third principle, *know your situation*, focuses on the necessity for continually evaluating the environment for cues that indicate that deception should be considered as the adversary is formulating strategies, considering options, making decisions, or taking action. An important thing to keep in mind is that analysts are confronted by a continuum of deceptive activity and that most of it, like an adversary's routine operational security measures (denial), is normal and likely to occur no matter what the situation is. Because large-scale, sophisticated deception operations are rare, situational factors may offer important clues to the possibility that the adversary is planning or employing more sophisticated deception operations. These situational factors include

- high-stakes situations;
- asymmetrical power relationships between the participants;

- changes in leadership, motives, political goals, military doctrine, or technological capabilities;
- situations involving potential surprise and risk as high-risk, high-gain strategy; and
- events in the international environment that threaten security or provide opportunity.

The fourth counterdeception principle, *know your channels*, is the conscientious application of this everyday maxim to the channels of information used by intelligence analysts and policymakers. For the analyst, it means above all else having a sound understanding of the collection disciplines—their capabilities and their limitations, and especially their vulnerabilities to denial and deception. *It is critical to understand the extent to which those collection capabilities are known and understood by intelligence targets and are thus vulnerable to being denied and deceived by them.* An in-depth understanding of collection channels and what the intelligence target knows about them is a vital requirement for effective analysis, particularly against hard targets.

Analysts, as illustrated in chapter 10, require a far better understanding of their *dependency on intelligence collection* than they often demonstrate. Briefly, when collection succeeds, it significantly improves the probability that analysis will also succeed. When collection fails—as it did against al-Qaeda before September 11, 2001, and against Iraqi WMDs before Operation Iraqi Freedom—it increases the probability that analysis will also fail. Analysts who do not fully understand the broad range of intelligence collection *capabilities* as well as collection *limitations*, or the enormous importance of their having this special expertise, significantly increase their vulnerabilities to D&D.[20]

Analysts also require a far better understanding of their *dependency on only one or a few key pieces of information*. Sometimes the whole analysis of a complex problem may crumble if a key piece of evidence is removed. If that key datum is unreliable, fabricated, or tenuous—and the analysts are not fully cognizant of its tenuousness or of its potentially exaggerated impact on the analysis—their analysis is likely to be wrong. Their certainty or confidence will also be misplaced. Errors in analysis can sometimes be traced to exaggerated dependence on poor evidence.[21] Because D&D is a major cause of missing evidence, it is also a potential source of poor or deceptive evidence.

Finally, as we know all too painfully from the pernicious effects of the source "Curveball" on the faulty judgments about Iraq's biological weapons capabilities in 2002, sources of intelligence information require better vetting than ever before. Curveball's impact on the erroneous biological weapons analysis in the 2002 WMD national intelligence estimate dramatically illustrates the dependency vulnerability discussed just above. The need to apply more rigorous scrutiny to both human *and* technical sourcing is a key requirement for better intelligence adaptability to D&D. Of course, no intelligence service ever takes information at face value from any source. But sophisticated D&D techniques can be subtle and insidious, and reliable intelligence requires even better *counter*-D&D techniques in the vetting of intelligence collection.[22]

Vulnerable Minds and Vulnerable Organizations

Even the most competent analysts and decision makers have found themselves deceived. To make matters worse, they may find themselves accused of incompetence by those blessed with 20/20 hindsight. To say that we are vulnerable to deception is by no means pejorative, because the concept of vulnerability helps to distinguish the important ways that humans and organizations are open to attack or damage by deception. Therefore, understanding our vulnerabilities to deception can act as a guide to actions we can take to mitigate those vulnerabilities.

Such understanding starts by considering the profiles of the vulnerable mind and the vulnerable organization.[23] The *vulnerable mind*—the one least prepared to counter D&D—sees reality unwittingly shaped by its own biases, preconceptions, and expectations. It understates or ignores the impact of ambiguous, contradictory, and missing information, and exaggerates the importance of the information it expects to see. It is unduly gullible or influenced by a good story. It tends to be overconfident in understanding complexity. And it lacks accurate, in-depth knowledge of its adversary, including especially the D&D capabilities that adversary may wield. These vulnerabilities result in flawed perceptions and judgments that cede advantage to the deceiver. This is a formula for successful D&D.

Similarly, the *vulnerable organization* overemphasizes consensus, consistency, and being decisive. It fails to exploit its full collaborative potential, performing with less than the sum of its parts. It has inadequate learning processes and fails to learn from past performance, including its failures, which it tends to repeat. And it is preoccupied with the present at the expense of the historical or strategic and future perspectives.

Countering Foreign Denial and Deception

With these vulnerabilities understood, we can now develop counterdeception analytic imperatives for transforming vulnerable minds and vulnerable organizations into prepared minds and prepared organizations.

The Prepared Mind

Our desired goal is to deliver better, more accurate judgments that will negate or at least mitigate the effects of denial and deception.

Bennett and Waltz propose two broad strategies for reducing the mind's vulnerability to D&D. The first is to *improve the information available*. Two approaches can accomplish this. One is to improve collection. Multiple intelligence sources and new collection methods increase the likelihood of uncovering flaws in an adversary's D&D attempts. Another is to develop better metadata to support the vetting of our information sources, such as the credibility of a human source.

The second strategy is to *improve analysis* itself. This entails mitigating cognitive biases, adopting the use of a systematic or structured analytic tradecraft, improving intuitive reasoning, and developing "acumen" skills.[24]

The *know yourself* principle emphasizes continuous awareness of the vulnerable mind's most exploitable weakness: its own preconceptions, expectations, and beliefs. One of these weaknesses is the failure of the vulnerable mind to generate adequate hypotheses. And the persisting failure to generate alternative hypotheses is insufficiently recognized in the intelligence community. This failure can be attributed to the use of a suboptimal heuristic of choosing the first explanation that seems to be the closest fit to the evidence at hand ("satisficing" and jumping to conclusions). A major contribution of alternative analysis is that it shows the value of multiple hypotheses.

Just as the failure to generate hypotheses increases vulnerability to deception, so also do confirmation bias and overconfidence. A particularly helpful approach to mitigating confirmation bias and overconfidence is to *restructure the analytic task*. This is aimed at challenging the mind-sets that induce confirmation bias and exaggerate confidence. Several methods of restructuring the analytic task can reduce analytic susceptibility to this kind of error. For example:

- Asking analysts to list reasons why their answers to questions might be wrong.
- Instructing analysts to consider the opposite interpretation of a judgment or forecast, or to engage in *any* second explanation task (for example, explaining a different version of the same outcome).
- Asking analysts to consider what evidence would be required to convince him or her that the interpretation is wrong or what evidence could cause the analyst to change his or her mind.[25]
- Asking analysts to assess any inconsistencies and discrepancies that have been explained away ("bending the map") might indicate that other possibilities are being ignored.[26]
- Having analysts define "tripwires," events that should not be occurring or levels that should not be exceeded if the favored hypothesis is correct. Finding that too many tripwires are tripped could be an indication that the favored hypothesis is wrong.[27]

The *know yourself* principle emphasizes recognizing the assumptions, preconceptions, and expectations that influence analyst beliefs, while the *know your situation* principle focuses on continually evaluating the environment for the cues that deception may be a factor in the situation under consideration. The use of structured analytic techniques (SATs), including Challenge Analysis, also provides another way of restructuring problems so that assumptions, preconceptions, and mental models—that is, factors shaping mind-sets—are not hidden, by making them more explicit so that they can be examined and tested. In particular such SATs include Analysis of Competing Hypotheses, Key Assumptions Check, Structured Brainstorming, Argument Mapping, and Signpost Analysis. Challenge Analysis techniques include Devil's Advocacy, "What If" Analysis,

and High-Impact/Low-Probability Analysis.[28] Using such tradecraft can highlight possible biases or situational cues.

A prepared mind will make a conscientious effort to see the problem or situation from the adversary's point of view. It will continually test and retest its judgments, update and evaluate all the evidence at hand, and remain alert to cues and anomalies in the environment that something has changed or is missing. It will not ignore its intuition when something does not quite feel right about a complex analytic situation. And it will diligently update and evaluate the credibility of information sources, stay alert to any channels that may have been compromised, and revisit the issue of source vetting and validation.

The Prepared Organization

To conclude, we want to emphasize four things that an intelligence organization can do to facilitate better counter-D&D analysis and to make itself less vulnerable to denial and deception:

- Prioritize an effective counter-D&D analytic capability and ensure that it is well resourced, incentivized, and protected.
- Enable analysts to better collaborate, access and share sensitive information, and exchange alternative and/or dissenting views.
- Create and encourage a robust analytic learning environment that emphasizes "lessons learned" and structured analytic techniques.
- Emphasize anomaly detection to help ensure that little surprises do not become big surprises.

The prepared organization will be well armed with robust counter-D&D analytic capabilities. Such capabilities can be gauged largely by the strength of the organization's counter-D&D analysis components (or even whether there *is* one), the quality and stature of the analysts who staff them, the skills of fellow D&D analysts in the hard-target components throughout the IC, and the measure of the training resources that directly support the counter-D&D mission. Though the IC has seen wide variation in these capabilities in previous decades, they have been perennially short of critical mass.[29]

A positive step toward creating an intelligence community of prepared organizations is the recent effort of the director of national intelligence to create a "culture of collaboration" that emphasizes greater intelligence sharing among analysts.[30] Greater counter-D&D collaboration must also encourage championing alternative views. A more collaborative and sharing environment must continually challenge and update analysts' expectations, mental models, and situational awareness.

Prepared organizations are also learning organizations. For countering D&D, two types of learning are especially required. First, there should be active learning programs that capture and share lessons learned to help analysts learn from past performance;

these activities should address both previous events and more current issues.[31] The prepared organization will also resist pressures of day-to-day distractions and devote time to learning from unexpected events, knowing that if it fails to do so, it will remain vulnerable to later unexpected events. Another important type of learning will provide analysts practice in situations involving D&D before they encounter it. Both types require more robust intelligence community training programs than are now in place.

Finally, reducing vulnerability to D&D surprises requires paying attention to anomalies, or what Barton Whaley calls "incongruities." Whaley's rule for this is that "when enough evidence is reconsidered in one brief time—in the forefront of the analyst's memory—incongruities, if present, tend to become obvious."[32] Where D&D is concerned, the intelligence community's goal is the same as that in the highly reliable organizations studied by Karl E. Weick and Kathleen M. Sutcliffe—that is, to deal with the small surprises before they become big ones.[33] Analysts should always recall what Cynthia Grabo has taught us about warning failures: "While not all anomalies lead to crises, all crises are made up of anomalies."[34]

Implications for the Future

Deception has been a part of life on this planet since its beginnings. It will surely continue to play a significant role in human competition and conflict in the years ahead. History has shown that the use of deception gives the deceiver a significant advantage over both naive and sophisticated targets.

Our adversaries recognize the immense economic, information, and military advantages that the United States enjoys. History has shown that deception offers the means of equalizing the kinds of asymmetrical power relationships in favor of the deceiver. The United States now faces a range of adversaries who view deception as a proven force multiplier and a dependable tool of statecraft through diplomacy, military strategy, and other instruments of power.

The explosion of information technology has important implications for both deception and counterdeception. The number of channels available for reaching deception targets is expanding. Increasingly ubiquitous mobile devices, social media, and internet technology, including malware, all multiply ways of reaching out and influencing target audiences or even individuals. Computer-generated imagery is reaching such a degree of sophistication that the phrase "pictures don't lie" may become a quaint anachronism. Advances in material science and electromagnetics point to the possibility of "smart skin" camouflage materials and of signature reduction and adaptation techniques that may make "cloaking" devices a reality.

In sum, foreign denial and deception pose major threats to successful intelligence analysis. The best counters to the D&D analytic threat begin with an understanding of the principles of deception (truth, denial, deceit, and misdirection) and require a keen awareness of bias traps and cognitive vulnerabilities to being deceived. By knowing yourself, your adversary, your situation, and your channels, you can greatly reduce your

susceptibility to D&D-induced faulty analysis. In particular the prepared mind and the prepared organization together present the best possible assurances of intelligence analysis uncorrupted by foreign denial and deception.

Notes

1. This chapter draws heavily from James B. Bruce, "Denial and Deception in the 21st Century: Adaptation Implications for Western Intelligence," *Defense Intelligence Journal* 15, no. 2 (2006): 13–27, and Michael Bennett and Edward Waltz, *Counterdeception Principles and Applications for National Security* (Boston: Artech House, 2007).
2. This is based on calculations made by Richards Heuer using two databases starting in 1914 compiled by Barton Whaley. One database ($N = 68$) ended in 1968, the other ($N = 93$) in 1972. Both showed a deception success correlation of slightly higher than .9. Donald C. F. Daniel, "Denial and Deception," in *Transforming U.S. Intelligence*, ed. Jennifer E. Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2005), 138.
3. Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction, *Report to the President of the United States, March 31, 2005* (Washington, DC: Government Printing Office, 2005) (hereafter, *WMD Commission Report*), 381.
4. Ibid. See also James B. Bruce, "How Leaks of Classified Intelligence Help U.S. Adversaries: Implications for Laws and Secrecy," in *Intelligence and the National Security Strategist*, ed. Roger Z. George and Robert D. Kline, 399–414 (Lanham, MD: Rowman & Littlefield, 2006).
5. Bennett and Waltz, *Counterdeception Principles and Applications*, 58–66.
6. R. W. Mitchell, "Epilogue," in *Deception Perspectives on Human and Nonhuman Deceit*, ed. R. W. Mitchell and N. S. Thompson (Albany: State University of New York Press, 1986), 358.
7. Barton Whaley, *Stratagem: Deception and Surprise in War* (Cambridge, MA: Center for International Affairs, Massachusetts Institute of Technology, 1969), 17.
8. See J. Lierpoll, Misdirection Resource Center, www.lierpoll.com/misdirection/misdirection.htm.
9. Bennett and Waltz, *Counterdeception Principles and Applications*, 71–88. Richards Heuer pioneered the early work on how cognitive bias increases vulnerabilities to deception. See Richards Heuer, *Psychology of Intelligence* (Washington, DC, Center for the Study of Intelligence, CIA, 1999), and chap. 8 by Jack Davis.
10. Roy Godson and James J. Wirtz, "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, 2002), 3.
11. *The 9/11 Commission Report*, authorized ed. (New York: Norton, 2003), 416–18.
12. For further reading on cognitive biases and deception, see Bennett and Waltz, *Counterdeception Principles and Applications*, chap. 3, and Richards J. Heuer, "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981). For more on cognitive heuristics and biases, see Daniel Kahneman, Paul Slovic, and Amos Tversky, *Judgment under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982).

13. T. Gilovich, *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life* (New York: Free Press, 1991).
14. "FUSAG" refers to Lt. Gen. George Patton's First US Army Group, the notional army unit in southern England preparing for the Allied invasion of Pas de Calais—in reality, the deception setting up the Germans for the invasion of Normandy. R. Hesketh, *Fortitude: The D-Day Deception Campaign* (New York: Overlook, 2000), 193.
15. Gilovich, *How We Know What Isn't So*, provides a good overview of such research.
16. During World War II, Operation Mincemeat successfully deceived the Germans that Greece and Sardinia were the Allies' next invasion target instead of the island of Sicily, the real target. See Ewen Montagu, *The Man Who Never Was* (New York: Oxford University Press, 1996).
17. P. Lamont, and R. Wiseman, *Magic in Theory* (Hatfield, UK: University of Hertfordshire Press, 1999), 36–52.
18. Sun Tzu, *The Art of War*, trans. S. B. Griffith (New York: Oxford University Press, 1963), 84. See also Jennifer E. Sims, "Understanding Ourselves," in *Transforming U.S. Intelligence*, ed. Sims and Gerber, 32–59.
19. M. Dewar, *The Art of Deception in Warfare* (Newton Abbot, UK: David & Charles, 1989), 194–203.
20. *WMD Commission Report*, 409–10.
21. Heuer, *Psychology of Intelligence Analysis*, 105–6. Also see the discussion of the Iraq WMD national intelligence estimate in chaps. 9 and 10.
22. See *WMD Commission Report*, 158–61, 367–72.
23. Bennett and Waltz, *Counterdeception Principles and Applications*, 186–93.
24. Ibid., 200.
25. Gary Klein, *The Power of Intuition* (New York: Currency Doubleday, 2004), 147–48.
26. Ibid.
27. Ibid.
28. See chap. 14 by Pherson and Heuer.
29. James Bruce, foreword to Bennett and Waltz, *Counterdeception Principles and Applications*, ix.
30. See chap. 17 by Fingar.
31. Stever Robbins, "Organizational Learning Is No Accident," *Working Knowledge for Business Leaders Newsletter*, Harvard Business School, 2005, http://hbswk.hbs.edu/item.jhtml?id=3483&t=srobbins.
32. Barton Whaley, "Meinertzhagen's Havesack Exposed: The Consequences for Counterdeception Analysis," unpublished manuscript, 2007.
33. Karl E. Weick and Kathleen M Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity* (San Francisco: Jossey-Bass, 2001).
34. Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College, Center for Strategic Intelligence Research, 2002), 31.