CHAPTER 5

Principles of Counterdeception

Chapters 1 through 4 provided a general introduction to deception by describing its increasing role in the global security environment, the various models and theories that have been developed in order to describe and understand it, the various biases that contribute to its seemingly almost certain success, and the variety of technical and nontechnical methods that support the conduct of deception operations. We also proposed that there are four fundamental principles that form the foundation for the different models and methods of strategic deception. Now, we turn our attention to the topic of counterdeception and attempt to answer several questions. What is counterdeception? What guidance can be found in the literature for countering deception? Is there a corresponding set of fundamental principles of counterdeception that can guide analysts and decision-makers? What can be done to overcome the various biases that we saw contribute to deception's success? What technical and nontechnical means can be employed to counter strategic and tactical deception operations? And, perhaps the most intriguing question of all: Is Barton Whaley right? Is deception almost always successful as the historical evidence implies? This chapter addresses the first three of these questions. After defining what we mean by counterdeception, we will examine the variety of models, concepts, and approaches found in the literature related to counterdeception in the national security context. We will then examine the common themes that emerge from this work, and derive a set of basic principles of counterdeception.

5.1 What Is Counterdeception?

The U.S. Department of Defense [1] defines counterdeception as: "Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations." This is an operationally oriented definition that emphasizes mitigating deception's effects (like surprise) and exploiting knowledge of the adversary's deception. Our focus will be primarily on the intelligence function part of that definition, but the concept of counterdeception goes beyond just "identifying foreign deception operations." We believe that the purpose of counterdeception is to find the answers to two fundamental and highly interdependent questions. First, counterdeception must make it possible for analysts and decision-makers to penetrate through the deception to discern the adversary's real capabilities and intentions, in other words, to answer the question: What is real? Simultaneously, analysts and decision-makers must determine what the adversary is trying to make them believe in order to consider the second question: What does the adversary want you to do? The answers to these two questions are absolutely essential to the success of one's own strategies, policies, and operations.

The intelligence aspects of counterdeception are aimed at detecting, characterizing, and penetrating foreign deception operations. It is important to keep in mind that there is no sharp demarcation line between normal intelligence activities and counterdeception intelligence activities. This is because no such line exists between the adversary's normal security activities and his calculated deception operations. Although large, sophisticated deception operations (like Plan FORTITUDE in World War II) are rare, as we saw in Chapter 2 deception itself is a phenomenon that everyone experiences in one form or another on a daily basis. This presents intelligence analysts and decision-makers with a paradox: *Deception is simultaneously both common and rare*. As a result, analysts face a continuum of deception ranging from basic security activities aimed at the deliberate concealment of facts, to sources who engage in deceit and misrepresentation for personal reasons (e.g., a human asset who fabricates information in order to remain on an intelligence organization's payroll), to deliberate ad hoc official deceit, and finally, to deliberate well-planned, well-coordinated deception operations. This is why counterdeception in the national security context is more than just detecting deception. Just what kind of deception are we trying to detect? How do we distinguish between deliberate deception and the types of misperceptions that Jervis describes? As Rossa points out [2]: "Faced with an array of information on a subject, the analyst who is to put the pieces of the puzzle together must first determine which pieces to use and which to discard or reshape on the basis of whether it was obtained despite foreign denial operations, as a result of foreign deception operations, or in the absence of either." This leads us to conclude that counterdeception is characterized by three dimensions of action: *awareness*, *detection and exposure*, and *discovery and penetration*.

Awareness primes the observer to register cues in the environment that signify either a threat or an opportunity. Anyone who has ever taken a personal security training course knows that awareness is considered the first line of defense; being aware what is happening around you often allows you avoid trouble before it even happens. Awareness is also analogous to the activation step in the Johnson et al. fraud detection model. The auditor is aware of certain cues that, if detected, lead to further questioning of the financial statement. A simple example of awareness in the intelligence context is when an analyst recognizes that a situation presents the adversary both the opportunity and motive to employ deception.

The *detection and exposure* dimension involves intelligence collection and analysis activities that are aimed at determining what the adversary is trying to make you believe and, as a result, what he wants you to do [3]. In essence, the objective is to accurately reconstruct the deceiver's deception story from the data and information available. The *discovery and penetration* dimension, on the other hand, focuses on revealing what is real. In this case intelligence collection and analysis assets are used to sort out the relevant from the irrelevant and the real from the false in order to determine what are the adversary's real capabilities and intent [4]. These two dimensions are not independent. They are highly coupled and interdependent and both employ similar processes and methods to reveal that which is concealed, separate deliberate distortions from unintentional misperceptions, and disentangle the real from the false in order to determine what really to believe.

5.2 The Search for Ways to Counter Deception

In Chapter 2 we saw that much of the literature related to military and strategic deception concentrates on the historical description and analysis of deception operations and their associated methods. The 1970s saw the beginnings of a theoretical phase of deception analysis where several authors used basic principles from psychology, systems engineering, communications theory, and other fields to begin the development of conceptual models of the process of deception itself. In this literature, the subject of counterdeception is, if addressed at all, treated almost as an afterthought. An author might devote a few paragraphs or perhaps a section of a chapter or paper to the topic. As Harris [5] observed in 1973, "There is hardly an adequate theory of deception, much less a theory of counterdeception." Events in the late 1990s (e.g., the 1998 Indian nuclear test and especially Iraq's efforts to hide its WMD program) generated significantly more interest in counterdeception; however, the literature on topic is still relatively sparse. This section mirrors the approach taken in Chapter 2 and summarizes the various counterdeception conceptual models, theories, and approaches that can be found in the literature. Like Chapter 2, they are presented in rough chronological order so that the reader can see how the thinking about counterdeception has changed over the years.

5.2.1 Early Pioneers [6]: "Is there, then, no way by which the target of stratagem can untangle the web of deceit?"

In 1942, R. V. Jones wrote [7]: "No imitation can be perfect without being the real thing [7]." The implication of this observation is that imitations should differ from the real thing in one or more ways, that is, observations made of the imitation should be inconsistent with those of the real object or event, thus leading to Jones to the conclusion that [8], "If there is inconsistency between the impressions derived from the several channels, the potential deceivee would do well to suspect a deception." Jones goes on to offer advice on what the target can do in this situation. First, he recommends [8] a "critical reappraisal of the intelligence picture" that "should include examining afresh the evidence coming in through each channel in turn, and particularly those channels giving conflicting evidence." In addition, there are other actions that analysts can take based on two principles that Jones offers for unmasking deception [9], "(1) in any channel of intelligence through which you may be deceive, arrange to work down to a greater level of sophistication than your opponent expected you to adopt, and (2) bring all other possible channels of intelligence to bear on the problem, to see whether the evidence that they can provide is consistent with the evidence in the channel through which you suspect you are being deceived." The first principle involves going beyond the obvious conclusions offered by an observation and subjecting the data to further scrutiny in search of clues that might reveal inconsistencies. Examining the Doppler characteristics of radio navigation signal is an example of this "deepening" examination of an information channel. If the source of the deceptive signal is ahead of an aircraft while the source of the authentic signal is behind it, the frequency of the real signal should be slightly lower than that of the deceptive one, thus, in principle, unmasking the deception [10]. An example of the second principle might be to double-check the observations of the radio navigation signal with other channels of information such as inertial guidance systems or dead reckoning methods using magnetic compass and clock. Once again, the detection of inconsistencies is cause for suspecting deception.

Jones also offers two maxims that are also quite relevant to counterdeception. The first [11] is "Crow's Law: Do not believe what you want to believe until you know what you ought to know." As we saw earlier, knowing what you ought to know will undoubtedly involve reappraising any evidence that is inconsistent with what you want to believe. The second is Occam's Razor: Hypotheses are not to be multiplied without necessity. Given missing, ambiguous, and contradictory information, analysts should seek the simplest hypotheses that will account for the information on hand. Jones points out that this will not necessarily produce the correct explanation, but that it provides the best basis to start from. Only rarely, he says, has Occam's Razor failed him. This is sound advice in the face of our human ability to make too much out of too little, as Jones [12] subsequently points out with "Crabtree's Bludgeon: No set of mutually inconsistent observations can exist for which some human intellect cannot conceive a coherent explanation, however complicated."

Barton Whaley briefly addressed the question of counterdeception in his famous 1969 book. In the chapter where he describes his theory of stratagem, he also proposes a decision-making model analogous to the one he describes for stratagem itself (see Section 2.2.2). Whereas a stratagem decision-making model is used to create a set of signals that the target observes and fits to a plausible alternative, a counterdeception decision-making model should be designed [13] "to analyze the signals of stratagem rather than the one designed to synthesize their false signals." Whaley offers two examples only one of which we will discuss here. While intelligence analysts consistently strive to expose an adversary's attempts at camouflage, Whaley observes that he could find no example of where the deceiver's attempts at camouflage were reported [13] "for their own sake." Whaley concludes that [13], "having done their work to identify camouflage, the analyst uses his findings only to correct the regular situation reports, order-of-battle maps, or traffic analysis studies. He does not use these findings to analyze the patterns of camouflage or 'noise' to see if they could imply a positive deception plan or campaign." In other words, the existence of camouflage becomes a signal of deception and such signals can be analyzed in order to detect patterns that might suggest the alternative objective of the adversary.

Harris, who, according to Whaley, coined the term *counterdeception* in 1968 [14], proposes that countering deception involves three related concepts [5]:

- The *detection* of an adversary's deceptions;
- The adoption of *countermeasures* that reduce the likelihood and adverse consequences of those deceptions;
- The *coordination* of both of these into a counterdeception system.

Harris concentrates primarily on the first two concepts and leaves it to the reader to "read between the lines" in order to identify the organizational implications of creating a system to coordinate the two activities. Therefore, we will concentrate on the three techniques that Harris describes for detecting the existence of deception operations and for uncovering the facts. These are: *reconstructive inference*, *incongruity testing*, and *vulnerability assessment* (see Figure 5.1). The first, reconstructive inference, involves attending to the patterns of misleading and deceptive signals that are transmitted by the deceiver. These spurious signals, or *sprignals*, appear to be directly analogous to the "signals of stratagem" that Whaley suggested looking for and therefore reconstructive inference—analyzing patterns of sprignals and their relationships—should make it possible to identify the "stratagemic plans" of an adversary. The analysis of sprignals also makes it possible to identify those channels that that are most likely to be used to disseminate disinformation at critical times. It may also be possible to correlate masses of sprignals with different deception styles. Of course, separating sprignals from real signals and noise is no easier than separating signals for noise and Harris suggests concentrating on separating sprignals from signals while recognizing the fact that some noise will wind up contaminating both categories. Sprignals are also likely to be sensitive to both time and context. Making things even more difficult, patterns of sprignals may provide clues that are only relevant to past encounters but not necessarily future ones. In addition, even if sprignals analysis yields insights into an adversary's initial plan, that analysis might not be relevant in a fluid situation (e.g., situations where a commander changes his plans and the deception plan winds up becoming the real plan).

The second technique is incongruity testing, which Harris defines as the matching and testing of alternative patterns for internal and interpattern consistency. He does not offer much detail regarding the methods for such testing, but simply states that [15]: "at least theoretically" incongruities could be discovered "given sufficient data and hypothesis testing." Reading through Harris's section, one comes to the

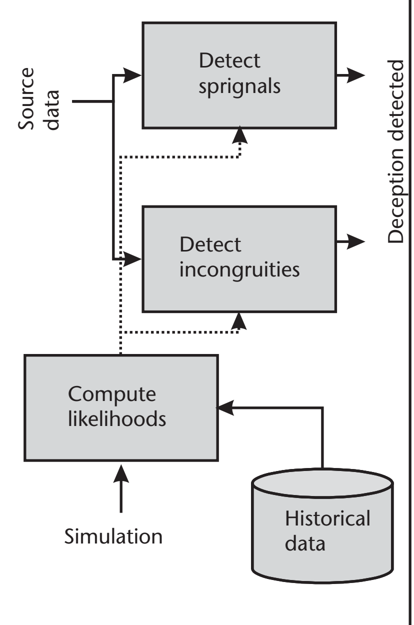
Method	Function	Operation
Reconstructive inference	Detection of spurious signals (sprignals) that indicate the presence of deception.	 Source data Detect sprignals Deception detected Detect incongruities Compute likelihoods Simulation Historical data
Incongruity testing	Alternative pattern matching and testing for internal and interpattern consistency.	
Vulnerability assessment	Predict the likelihood of deception as a function of modes and conditions, based on simulation, historical data, and gain to the deceiver.	

Figure 5.1 Harris's deception detection techniques.

conclusion that it involves the generation of alternative hypotheses that represent "alternative perceptual patterns" of the signal and sprignal data.

Harris notes that incongruity testing faces two main limitations: *disjointed incongruities* and *false incongruities*. Disjointed incongruities [16] "involve inconsistencies that have become, in the perceptions of the viewer if not in fact, separated or mismatched." The incongruities are not recognized because the different sets of inconsistent patterns are never paired. Jokes, hoaxes, and deceptions all rely on disjointed incongruities. Jokes are funny because the question sets up an incongruity and the punch line reveals the hidden resolution to the incongruity—a surprising alternate interpretation [17]. Deceptions work if the incongruities between the real and false situations are not resolved. Harris calls these *clandestinely* disjointed incongruities. The challenge to incongruity testers is that deception planners do their best to prevent their target from detecting the incongruities. Another form of disjointed incongruity that has counterdeception implications are *mutually* disjointed incongruities. In this case, observer A perceives situation A and observer B perceives situation B. It may be the case that situations A and B are representations of the same situation, but unfortunately this situation is not the true situation, C.

The other limitation to incongruity testing is the need to deal with false incongruities. Harris defines false incongruities as [16]: "The pairing of two or more apparently inconsistent patterns that represent a consistent underlying reality." These complicate the task of incongruity testing by adding clutter to the process. They can result from different perspectives of the underlying pattern or as the result of our ability to detect order in random patterns.

Some of these apparent but unreal incongruities are a matter of different perspectives; some are a consequence of the random distribution of noise in perceptual systems. In either case, they must be identified.

The third technique, vulnerability assessment, uses statistical approaches to predict future vulnerabilities to deception. Bayes' theorem, multivariate statistical analysis, game theory, and other modeling and simulation methods can all be used to explore the likelihood of encountering deception in different situations and under various conditions. Likewise, these methods can be used to assess the risks and costs of making Type I (failure to detect the deception) or Type II (false positive) errors. In addition, Harris suggest that rigorous studies of the deception styles and practices of prospective adversaries can help assess both one's own potential vulnerabilities as well as provide potential indicators of deception through the reconstruction of sprignal patterns.

In 1976, Robert Jervis concluded his book, *Perception and Misperception in International Politics*, with a chapter on minimizing misperception [18]. Although his focus was on misperception, not deception, his suggestions for minimizing misperception are equally applicable to situations where deliberate deception is involved. Jervis suggests four broad themes for compensating for perceptual errors:

- Making assumptions and predictions explicit;
- The use of devil's advocates;
- Making sure that identities and missions do not become linked with specific theories and images;
- Awareness of common misperceptions.

When considering deception, the first theme might be restated as making assumptions, preconceptions, and beliefs explicit. Jervis writes [19]:

> The failure to examine the plausibility of crucial beliefs, especially those relating to ends and means, is evident when the environment changes in a way that should, but does not, lead to changes in beliefs and policies. For example, one reason why the United States was taken by surprise at Pearl Harbor was that the initial analysis of Japan's alternatives had led to the reasonable conclusion that Japan would not attack American territory. But as the situation changed, American decision makers realized that Japan might strike at the Philippines. Since such an attack meant war with the United States, Americans should have noted that one of the major reasons why the Japanese would not attack Pearl Harbor was now removed and should have looked at the dangers again.

Jervis states that making beliefs and assumptions explicit requires not only understanding the elements that make up those beliefs and assumptions but also an examination of what evidence would confirm or disconfirm them. He suggests that [20], "If they are aware of what they expect, or rather what their images and beliefs should lead them to expect, actors will be more apt to heed unsettling incidents." Such awareness also extends to thinking about what events are excluded by the actor's assumptions and beliefs with the hope that he would be more likely to notice and react to those events if they occur as well as heighten his sensitivity to discrepant information.

Jervis [21] uses the concept of devil's advocates to emphasize the need for encouraging the "formulation and application of alternative images" noting that it is often politically and psychologically difficult for any one person to consider multiple alternatives. Jervis also has an interesting perspective on cognitive bias in this regard [22]: "Rather than seeking 'unbiased' treatments of the data, decision-makers should seek to structure conflicting cognitive biases into the decision making process to help themselves maintain their intellectual freedom." In other words, instead of trying to eliminate cognitive biases altogether, decision-makers should take advantage of them in order to produce differing perspectives of a given situation. In that same vein, Jervis continues [22], "To make it more likely that they will consider alternative explanations of specific bits of data and think more carefully about the beliefs and images that underlie their policies, they should employ devil's—or rather devils'—advocates." Jervis admits that a devil's advocate is unlikely to produce the correct image; however, incorporating devil's advocacy into the process has two major benefits. First, it exposes decision-makers to alternative explanations of events, thereby forcing them to exercise judgment as opposed to seeing one view as the only possible alternative. Second, devil's advocacy helps to expose the assumptions and beliefs discussed earlier.

Jervis offers less detail regarding the last two themes. The third theme addresses the potential dangers that arise when the mission and identity of individuals and organizations becomes too closely tied to specific theories and images of other actors. He cites as an example the U.S. Air Force's post–World War II resistance to guided missiles [23]: "The members of the organization had come to see its distinctive mission not as carrying out strategic bombardment, but as carrying out strategic bombardment by means of manned bombers." The deception implications should be obvious. If mission and identity are too closely tied to specific beliefs, a deceiver can manipulate those beliefs knowing that it is likely that information about other alternatives will be made to fit those beliefs or will not even be considered. Finally, Jervis [24] concludes his chapter on minimizing misperception with a general call "for decision makers to take account of the ways in which the processes of perception lead to common errors." The hope is that if decision-makers are aware of these biases and errors, they will be more likely to take measures to decrease misperception by avoiding or compensating for common perceptual errors, decrease their overconfidence in prevailing beliefs, become more sensitive to alternative perspectives, and perhaps reduce the amount discrepant information required to make them reconsider those beliefs.

5.2.2 The Theoretical Work of the 1980s

As we saw in Chapter 2, the 1980s saw the publication of a number of journal articles and books marking the start of a more theoretical approach to the study of deception. In 1980, the CIA's Mathtech Deception Research Program published a report, *Deception Maxims: Fact and Folklore*, which described the 10 deception maxims summarized previously in Figure 2.7. That report also addressed the counterdeception implications for three of those maxims in a single paragraph at the end of their report. Maxim 1 states that it is easier for the target to maintain preexisting beliefs even in the face of evidence that contradicts those beliefs implying that it is important to examine one's own beliefs for exploitable weaknesses in order to be less susceptible to deception. Maxim 4, Jones' Lemma, suggests that the deceiver should try to control as many of the channels available to the target as possible. The counterdeception implication is that the target should not rely on only one or two channels of information but should employ redundant sensors to increase the likelihood that incongruities can be detected. Finally, Maxim 6 counsels the deceiver that there are situations where deception assets should be husbanded until they can be put to more fruitful use. The implication of this maxim then is for the target to consider the stakes involved in any situation when evaluating the adversary's options: higher stakes may warrant the adversary using those husbanded deception assets.

Shortly thereafter, Richards Heuer published his landmark article, "Strategic Deception and Counterdeception: A Cognitive Process Approach." Although his article dealt primarily with the cognitive biases relevant to the problem of deception, Heuer also addresses the subject of counterdeception by reviewing three "commonly advocated approaches" and suggesting two more approaches of his own. The first three approaches are:

- Improved intelligence collection;
- Increased alertness to deception;
- Weighting of tactical indicators.

With regard to improved intelligence collection, Heuer notes [25] that advances in technical collection systems have improved the intelligence community's overall capabilities but that such systems "have contributed little toward improving estimates of intentions, strategy, or political dynamics." While improvements in intelligence collection are desirable, Heuer offers his belief [25] that such improvements are unlikely to significantly reduce one's vulnerability to deception and goes on to state, "Any systematic counterdeception program must focus primarily on problems of analysis, only secondarily on collection." Ideally, increased alertness to deception would stimulate a more thorough review of the information available and Heuer concedes that this is possibly the case if the possibility of deception has not already been considered. In such a case, Heuer [26] notes that "simply focusing on this possibility may be sufficient to identify overlooked information or prompt a change in analytical perspective." Nevertheless, he is generally pessimistic about the ability of alertness alone to detect deception and makes the case that such alertness is more likely to detect deception where it does not exist, lead analysts to be overly skeptical of all the information on hand, and when deception is present, cause analysts to dismiss the wrong evidence. The weighting of tactical indicators approach is based on Abraham Ben-Zvi's [27] study of surprise military attacks. Ben-Zvi found that tactical indicators of an impending attack were often discounted because they did not agree with the preconceptions and strategic assumptions held by analysts and commanders. Although Heuer agrees that analysts and decision-makers should be more open to changing their minds in the fact of discrepant information, giving more weight to such indicators will increase the false alarm rate and it is often difficult or impossible to know whether in any given situation it is better to heed the indicators or hold on to the established view.

Heuer's own suggestions fall into two categories: cognitive aids to analysis and organizational measures. The first category consists of alternative hypotheses and breaking mental sets. What has become to be known as Alternative Competing Hypotheses (ACH) is in response to the fact that research shows that people do a poor job of generating a sufficiently full set of hypotheses when analyzing a situation. As Heuer notes [28], "If the correct hypothesis is not even formulated for consideration, there is clearly little chance of making an accurate judgment." This failure to generate sufficient hypotheses is aggravated by other biases such as confirmation bias. Evidence tends to be evaluated in terms of how well it supports a hypothesis and the fact that such evidence may be consistent with other alternative hypotheses is often overlooked. For Heuer [28], "The systematic identification, examination, and testing of alternative hypotheses is one of the keys to the successful uncovering of deception." We will examine ACH in more detail in later chapters. Heuer [29] also proposes that "methods for breaking mental sets are particularly relevant for counterdeception analysis." He suggests methods such as the devil's advocate, interdisciplinary brainstorming, and "other techniques that facilitate the identification and systematic analysis of alternative perspective" [29]. The organizational measures that Heuer proposes focus primarily on the creation of a counterdeception staff as a form of "deception insurance." Heuer bases this suggestion on research showing that one of the most difficult cognitive tasks that a person can be called upon to perform is to reorganize information that they are already familiar with in order to view it from a totally different perspective. The more complex the information and the longer that one has held certain beliefs about what the information means, the more difficult this task becomes. Heuer suggests that a dedicated counterdeception staff is necessary to address complex questions concerning deception that cannot be handled by an individual analyst using cognitive aids.

In 1982 two books were published that addressed deception and surprise: *Strategic Military Deception,* edited by Daniel and Herbig, and *Military Deception and Strategic Surprise,* edited by Gooch and Perlmutter. In *Strategic Military Deception,* Daniel and Herbig [30] describe two groups of factors that influence the likelihood of deception. The first group is related to the different situations that confront a would-be deceiver, while the second group reflects certain characteristics of the deceiver. Although Daniel and Herbig do not mention that these factors could be used for counterdeception, we suggest that these factors represent potentially useful cues for analysts and decision-makers to be aware of. The situational factors include:

- *High-stakes situations.* Such situations encourage an adversary to use every capability at his disposal to ensure success or avoid defeat.
- *Lack of confidence in a situation's outcome due to military weakness.* Deception is a useful way of compensating for an adversary's superior strength.
- *Lower the costs of even an optimistic situation.* In addition to using deception in order to avoid human and material losses, an adversary may employ deception in order to avoid the political and economic costs of being viewed as an aggressor.
- *Uncertain situations.* A deceiver may use deception in order to keep his options open and to test his adversary's reactions to different actions.

The second group consists of factors related to the deceiver's previous conditioning or personal predilection and includes:

- *Cultural norms.* Cultural factor may affect when and how deception is used.
- *Political leaders that play a strong, central role in military decisions.* Deception may be more common in situations where this is the case, particularly in dictatorships and authoritarian regimes.
- *Bureaucratic and psychological pressure.* This factor is based on two traits common to many bureaucracies. The first trait is that organizations trained for particular tasks will seek to perform them. The second trait is related to the availability heuristic—people tend to think in terms of what is available to them. The first trait implies that an adversary that maintains the capability to plan, organize, and execute deception operations is more likely to use deception than one that is not. The second trait suggests that, even if not incorporated formally as doctrine, an adversary that has some familiarity with deception is more likely to use it than one that is not.
- *Personal predilection.* Leaders and commanders who appreciate deception and have relied on in the past are likely to do so again.

Paul Moose's chapter in *Strategic Military Deception* [31] presents an elementary systems model that envisions a dynamic relationship between two adversaries (Green and Purple) and their environment. This produces an "event stream" that is the result of each side's actions in response to the other as well as the environment. Moose's concept of counterdeception [31] involves a plan where the target (Purple) "hypothesizes two measurably different near-term event streams, depending on whether a deception is present or not" and initiates activities that precipitate some action on the deceiver's (Green) part in one of these streams which may reveal the deceiver's real intentions. The target then uses his own feedback channels to observe how the deceiver reacts to the target's reaction. Of course, the risks of waiting while the counterdeception plan unfolds versus acting on one of the hypothesized event streams must be considered. Moose also provides some general prescriptions regarding counterdeception. He states that [31], "The most effective way to prevent deception is to be continually aware of one's vulnerabilities as a target." He also notes that one should be skeptical about signals that encourage procrastination or inactivity and that the "leaky" nature of the adversary's internal communications (i.e., unintentional signals that might reveal the adversary's true intentions) should be exploited.

Also in *Strategic Military Deception* is a chapter by Theodore Sarbin, a narrative psychologist [32]. He proposes a theory of counterdeception that assumes that [33] "human beings think, perceive, and imagine according to a narrative structure." As we saw in Section 3.2.2.2, he suggests that the authors of strategy emplot narratives and observes that [33], "The task of the counterdeception analyst of strategy is like the task of the literary critic or the dramatic critic—to fathom the intentions of the author, to 'understand,' to decipher the meaning of the creative work." Given that deception typically represents a unique case where the context is a critical determinant of the actors' behavior, the target of deception cannot rely on statistical approaches or case studies (*sagacity*) to predict the deceiver's real intentions due to the lack of meaningful base rates. Therefore, the counterdeception analyst must rely on *acumen*—the empathic skill to take on the role of another. This ability is related to the person's ability to *decenter*—the ability to switch from one's own egocentric perspective and see things from another's perspective—and Sarbin suggests that [34], "From literary and autobiographical sources, one can infer that the person who is successful in taking the role of another is able to construct a scenario, a story, and place himself in relation to the other features of the story, physical features such as geography and climate, social features, such as role relationships with multiple role players." Such abilities help the person gifted with acumen succeed in consistently predicting the actions of others and are "the stock in trade of someone who can penetrate the masks or expose the lie of the adversary" [34].

Acumen is therefore an important skill for intelligence and counterdeception analysts to possess and Sarbin offers the hypothesis that analysts possessing the skill of acumen are more likely to identify the form of the narrative contained in the strategic plans of an adversary. He also poses two interesting questions in this regard. Are certain kinds of plots related to kinds of ethnic origins or national heritages? Can acumen be taught and learned? Sarbin asserts that literary historians are able to successfully identify the different forms of emplotment they encounter but admits that they have the benefit of hindsight. On the other hand, analysts face the problem of having to construct a plot from antecedent events and try to predict the outcome making their task tremendously more difficult. The difference is that [35], "Unlike the historian who emplots a narrative about events that have occurred in the past, the analyst of strategy must emplot concurrent events, events that are not frozen but fluid." With regard to teaching and learning acumen, Sarbin suggests that there may be ways to recognize "optimal cognitive strategies" for identifying the events associated with a specific plot structure [36], that is, "When is an 'event' an event?"

In the mid-1980s three closely related books by British authors (see the Haswell, Dewar, and Latimer portion of Section 2.2.3) appeared, but only one specifically addressed the topic of counterdeception. In *The Art of Deception in Warfare,* Dewar devotes a chapter to counterdeception [37], in which he summarizes Whaley's concepts of deception and uses them to make a number of points. These can be categorized into two broad areas:

- Macroscopic knowledge of the adversary;
- Microscopic analysis aimed at discovering inconsistencies.

Dewar notes [38], "A detailed knowledge of the enemy is as important in countering deception as it is in achieving it." This knowledge must extend to [39] "a macroscopic appreciation of the enemy's fears, aims, prejudices, and habits" and analysts "must also be able to see things from the enemy's point of view, think as the enemy thinks, list the options open to him and decide what is most probable" [40]. At one point Dewar goes as far as stating [41], "Thus the main, almost the only, weapon of the deception analyst is to put himself in the mind of the deceiver." This knowledge includes recognizing that the adversary's deception plans are themselves seldom flawless thus creating the opportunity for the "microscopic" search for the flaws in the pattern of the deceiver's deception plan. Here Dewar seems to be advocating a kind of analytical preparedness [42], "Defence against deception therefore requires a sustained questioning of evidence, a search for its corroboration and a review of previous deductions as fresh evidence is produced. In particular, it is helpful to look for small and obscure clues which are missing and which would prove or disprove the authenticity of the existing evidence." For Dewar, the golden rule of counterdeception is to avoid jumping to conclusions. He warns that deceivers thrive on the pressure that analysts labor under to provide timely assessments and predictions and urges analysts to resist the temptation to jump to conclusions whenever possible.

Dewar acknowledges the difficulty of looking at a situation from different perspectives noting that "increased alertness" to the potential for deception is largely ineffective, but suggests that a devil's advocate is one way that the data can be subjected to competitive analysis. Dewar summarizes his approach to counterdeception by reminding analysts that "first impressions are difficult to change and different starting points lead to different conclusions" and concludes [43]: "That is why competitive analysis should be undertaken whenever possible. Or to put it more simply, two heads are better than one."

The end of the 1980s saw the publication of Michael Handel's *War, Strategy, and Intelligence.* This book includes work that appeared as journal articles or as chapters in other books (e.g., Gooch and Perlmutter) and several of these address the topic of counterdeception both directly and indirectly. Handel is strongly pessimistic with regard to the possibility of preventing or forestalling surprise attack and this pessimism is reflected in his general skepticism regarding counterdeception. Nevertheless, he offers six possible deception countermeasures, noting that [44], "Some can be suggested, although their effectiveness cannot be guaranteed." The first suggestion, *avoid overreliance on one source of information*, emphasizes that potentially valuable information collected in one channel should be independently verified by sources in other channels. As we saw in Chapter 3, German over reliance on one channel of information (their network of agents in Britain—all controlled by the Allies) was a major factor in the success of Allied deception efforts. The next four suggestions address what can perhaps be the most important channel of information available to the deceiver—the double agent. His suggestions reflect several lessons that can be drawn from Germany's experience as the target of the Allies' Double Cross operations in support of the Fortitude deception. These include:

- *Never rely exclusively on nonmaterial evidence*. Handel quotes Clausewitz's remark that [44], "Words being cheap, are the most common means of creating false impressions." In other words, written or verbal information that an agent provides about physical entities must be checked and verified by other sources (e.g., an agent report about the location of a missile battery should be verified by imagery or signals intelligence). This suggestion also applies to information obtained through communications intercepts.
- *Never rely on agents who have not been seen or directly interviewed*. Much of the success of the FORTITIDE SOUTH deception is credited to the double agent GARBO and much of GARBO's success as a double agent was due to his ability to convince the Germans that he controlled a network of subagents. Unfortunately for the Abwehr and the German high command, this entire network was fictitious. All of GARBO's subagents, including his deputy, were notional. Handel [44] notes that this suggestion carries even more weight if the information that is received from possibly notional agents "dovetails nicely with one's own preferences or needs, or when it fits without contradictions into the reports of other possibly notional agents."
- *Check and double-check discrepancies in agent reporting*. Handel suggests that there are two situations where extra caution should be exercised when relying on agent reporting. First, there is the situation in which an agent's reports initially appear to be correct but then turn out to be wrong on an important issue and yet somehow the agent always seems have a good explanation for each discrepancy. The second situation calls for even more caution. Here Handel even suggests a special investigation of any agent who supplies high quality information of the greatest importance [44, 45], but "*only when it is too late to be of any use*—even if it arrives before the action it warns against has taken place."
- *Controllers of agents should also be encouraged to heed more closely the opinions of lower-level intelligence analysts*. Since the target of most strategic deception operations are top-level decision-makers, commanders, and intelligence managers, Handel suggests that deception has a better chance of being detected by lower level (not necessarily lower expertise or experience) analysts since they are less likely to be biased by any specific strategy, wishful thinking, or political interests. Handel cites examples from World War I, World War II,

> and the 1973 Yom Kippur War noting that many of the "negative or unpleasant conclusions" reached by lower level analyst were often ignored [46].

Handel's sixth suggestion makes it clear that it is necessary to know the adversary's limitations as well as his capabilities. This suggestion has its roots in mirror imaging and ethnocentric biases. The failure to analyze information about an adversary's capabilities and intentions must be done in accordance with the *adversary's* political and military needs—not one's own. Projecting one's own preferences, fears, and doctrine onto the adversary only increases the likelihood that one will be deceived or surprised.

Handel provides other direct references to the problems associated with counterdeception using a puzzle metaphor. For example [47], "Under certain circumstances, the more perfectly an intelligence puzzle fits together, the greater the danger of a possible deception ploy. This is particularly true when information—the solution to an important and complex intelligence puzzle—is received in the absence of much noise or contradictory evidence, and when the resulting conclusions conform neatly to one's hopes and expectations." Other "precautions" for avoiding deception are related to anticipating surprise attack and include asking [48]: "what are the most likely directions from which an adversary might attack, even if the available evidence contradicts these contingencies."

Handel's writings on strategic surprise and intelligence also indirectly address important counterdeception issues. For example, Handel discusses the roles that preconceptions, ethnocentrism, and misperception play in the problem of strategic surprise, and he attributes perceptual errors [49] to "projecting one's own culture, ideological beliefs, military doctrine, and expectations on the adversary (i.e., seeing him as a mirror image of oneself) or of wishful thinking…." To counter these ethnocentric biases, Handel makes the general suggestion of "know thine enemy," that is, develop a thorough and in-depth knowledge of an adversary's language, culture, politics, and values, as well as devoting more time and resources to knowing "thyself."

In addition, Handel discusses two mechanisms that are related to the subject of improving the objectivity and variety of input into the intelligence process. These mechanisms are also relevant to the challenge of countering deception. The first is *multiple advocacy*. The idea behind this concept is that multiple, independent intelligence agencies do a better job of providing decision-makers with a wider spectrum of views than does a single, centralized intelligence organization. The pros and cons of multiple advocacy are beyond the scope of this chapter; however, the contribution that it makes to counterdeception is to counteract a number of factors that tend to make the deceiver's job easier (e.g., the tendency to jump to conclusions and groupthink). The second mechanism is the *devil's advocate*. The purpose of a devil's advocate is to help ensure that dissenting, possibly unpopular, opinions are heard and evaluated. Again, the pros and cons of devil's advocacy are outside the scope of this chapter, but it is interesting to imagine what the results might have been in May 1940 if the French had an effective devil's advocate to warn them of the possibility of a German offensive through the Ardennes.

The end of the 1980s also saw the end of the Cold War, and as we noted in Chapter 2, deception research entered a hiatus period that was to last until the revelations of Operation Desert Storm and other events like the Indian nuclear test in 1998 made it clear that the need for understanding deception and improving ways to counter it had not disappeared. Interest in deception surfaced once again and has resulted in new practical and theoretical work by both some familiar early researchers and some new faces.

5.2.3 Current Directions

On the practical side, there is the 1997 CIA release of a set of analytic tradecraft notes that are a standard counterdeception reference for analysts both inside and outside of the CIA [50, 51]. *Note 10, Tradecraft and Counterintelligence* begins with an admonition to analysts "to show increased respect for the deceiver's ability to manipulate perception and judgments" and then describes two sets of warning signs that signal the possible existence of a deception operation. The first set goes by the acronym MOM, which stands for *means*, *opportunity*, and *motive,* and addresses the likelihood that a potential adversary is deliberately trying to distort the analyst's perceptions. *Means* addresses the adversary's experience and capabilities with regard to planning and executing sophisticated deception operations, while *opportunity* is related to the sources (channels) of intelligence available to the analyst. If the adversary is known to have knowledge of a source (e.g., a technical collection system), then he may likely have the opportunity to conceal information from that source or to deliberately distort the information the source collects. Finally, does the adversary have a *motive* to use deception? If all three warning signs are present, the analyst is wise to suspect that an adversary may resort to deception in order to achieve his goals.

The second set of warning signs focus on anomalies that analysts should be on the look out for regarding what they know, how they know it, and what they don't know. These warning signs include *suspicious gaps* in collection, *contradictions* to carefully researched patterns, and *suspicious confirmations*. Gaps in collection can be considered suspicious when information received through one channel is not supported by other channels especially when such confirmation would be considered normal. If new information contradicts well-supported trends and patterns, analysts need to critically examine such new information if it signals "inexplicable change" in the adversary's priorities, behaviors, and practices. Information received from one or more sources that seem to conveniently reinforce the rationale for or against one's own strategy or policy might also be considered suspicious. In such cases, the fact that multiple sources seem to corroborate one another may not necessarily mean the information is authentic.

Finally, Note 10 offers analytical tradecraft tips for dealing with the risk of deception when making intelligence assessments on complex issues. In the case of "regular" issues (those where there is no specific reason to suspect deception), the analyst is advised to employ a two-step process as insurance against the risk of deception. The first step is to organize information important to his conclusions and then critically examine it using the six warning signs mentioned previously. The second step calls for the analyst to play the role of devil's advocate and develop a hypothetical argument that deception is in fact taking place. In the case of "suspect and sensitive" issues, the note recommends undertaking an even more in-depth evaluation of the information at hand and annotating any resulting reports with a text box or annex that conveys to the reader that the possibility of deception has been considered seriously, appropriate analytic testing to determine the likelihood of deception has been done, and any reasonable doubts about the resulting analysis are noted.

The scientific community's interest in deception, which had been primarily focused on lying and deceit, also began to attract attention in national security circles in the 1990s. For example, Johnson et al. [52] have investigated the processes used by accounting auditors to detect the fraudulent manipulation of information in financial statements. They use Whaley's model of deception (i.e., masking, repackaging, dazzling, mimicking, inventing, and decoying) as the basis for the tactics that a deceiver can use to manipulate the target's processes of searching, processing, and interpreting information. They then propose a process for detecting deception that consists of three components:

- First the deception target identifies inconsistencies between his observations and his expectations for the observations.
- The target then determines that those inconsistencies are functional to the goals of the deceiver.
- Finally, the deception target identifies the potential actions of the deceiver that can be associated with one or more deception tactics and assesses the deceiver's ability to create the observed inconsistencies.

They then develop a *competence model* based on this process for detecting financial statement fraud. This model (see Figure 5.2) consists of four steps:

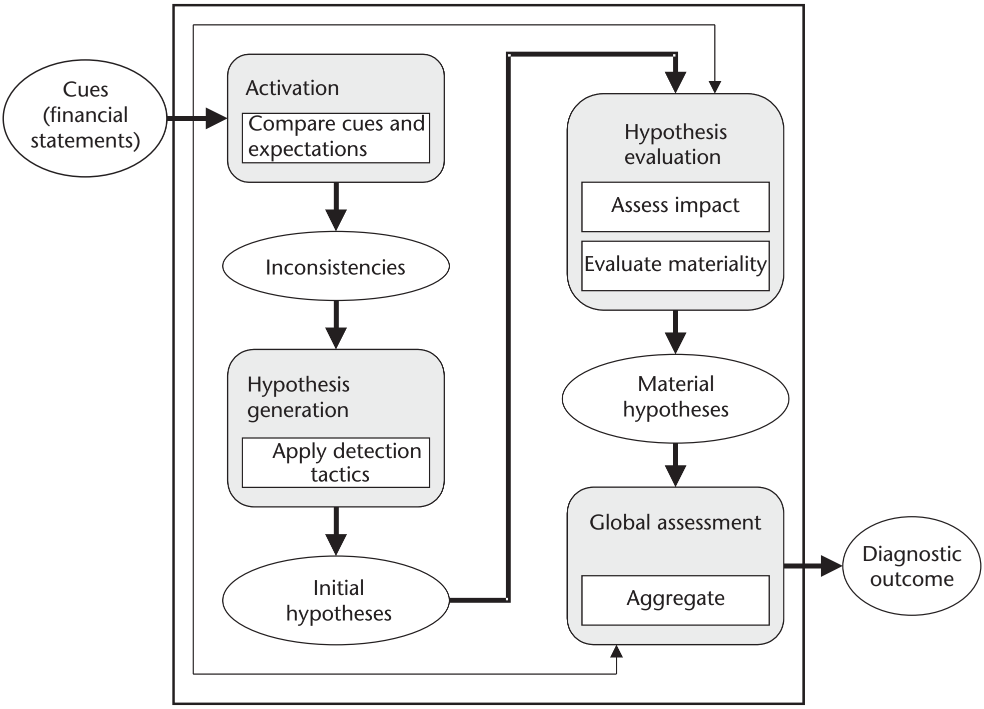


Figure 5.2 Fraud detection method. (*From:* [52]. © 2001 Cognitive Science Society. Reprinted with permission.)

activation, hypothesis generation, *hypothesis evaluation*, and *global assessment*. The activation step produces the expectations for the values of the various cues that might be found when an auditor examines a financial statement (e.g., an inventory balance value). These expectations are then compared to the actual observed values. Observed values that exceed expectations by some amount are then labeled as inconsistencies. The next step is to generate a set of hypotheses that explain the inconsistencies. In the auditing process examined by Johnson and his team, there are three possible hypotheses: accounting errors, insufficient disclosure, and, of course, deception. In this model, the deception hypothesis is generated when the inconsistencies satisfy the additional conditions of the detection process described earlier (i.e., functionality and feasibility).

In step three, the hypotheses are evaluated on the basis of their *materiality*. Materiality is an accounting term that is defined as [53] "…the magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement." The error and disclosure hypotheses are evaluated primarily on the magnitude of the difference between the expected and observed values of the financial statement cue. The basis for evaluating materiality for the deception hypothesis though depends on the deception tactic that is suspected to have been used (e.g., if the repackaging deception tactic is suspected, then the items that have been deliberately miscategorized should be recategorized using a worst-case scenario assumption). The global assessment step "aggregates and evaluates confirmed hypotheses" to produce the final rating of the company's financial statement—*unqualified* (the statement is "clean"), *unqualified+* (the auditor adds a paragraph noting a lack of consistency or some other concerns or uncertainty), or *misleading*. Finally, the model was implemented as a computer program that uses various data from financial statements to produce the final rating. The program successfully issued the correct global assessment rating for each of six cases it was given.

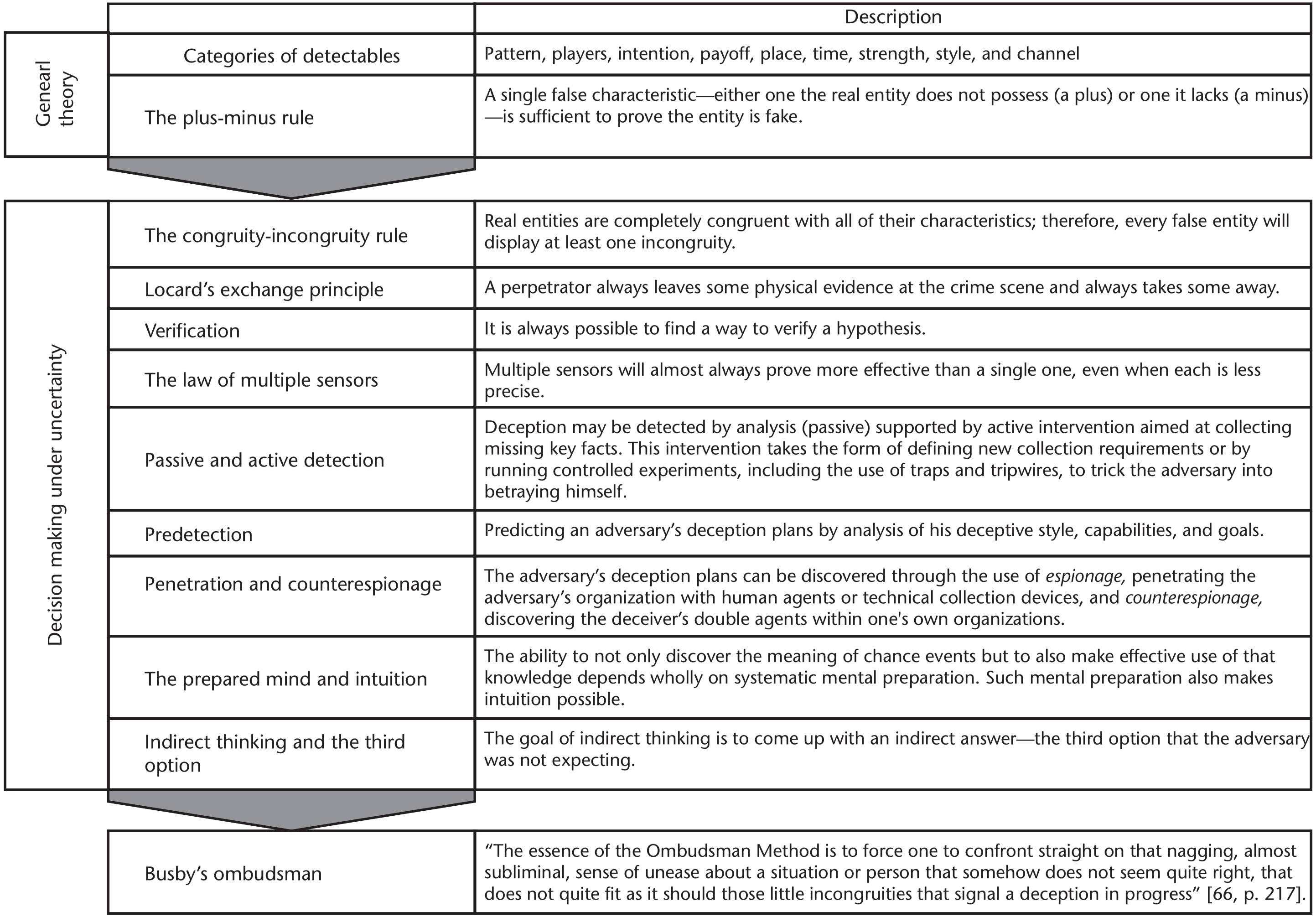
Even while counterdeception was attracting the interest of new researchers like Johnson and his associates, some familiar names were still active in field. It should probably not be a surprise that, over 30 years later, Barton Whaley was still active, contributing two chapters (one with magician Jeff Busby) to a book, *Strategic Denial and Deception: The Twenty-First Century Challenge* [54]. In the chapter coauthored with Busby, Whaley focuses entirely on counterdeception. Whereas many authors in the field of strategic deception are quite pessimistic about the prospects of successful counterdeception, Whaley (the principal author) offers a surprisingly optimistic perspective on the topic [55]: "I am optimistic that deceptions can be detected regardless of the field in which they occur. In theory, deception can always be detected, and in practice often detected, sometimes even easily." He proposes a general theory of counterdeception based on a wide range of sources, including results from case studies of different types of professionals who regularly deal with deception (e.g., intelligence analysts, police detectives, forensic scientists, art experts, and magicians). Whaley found that all the professionals who were highly successful at detecting deception used a common set of methods and that those same methods were never or only infrequently used by those who did poorly. In addition, he found these methods to be largely intellectual rather than technological in nature. Technology in the form of sensors that extend our natural senses and information technology that extends our ability to recall and manipulate information is important; however, deception detection remains a subtle, human intellectual process, as we will see when we examine the different elements of his theory.

This theory of counterdeception starts with two general components (see Figure 5.3): a taxonomy of "detectables" and the *Plus-Minus Rule*. Five of the nine categories of detectables (intention, time, place, strength, and style) have their origins as modes of surprise in Whaley's original work on stratagem [56]. The remaining four (pattern, players, payoff, and channel) make their appearance in Bell and Whaley's *Cheating and Deception* [57] in 1991. Together they represent the set of things that the deceiver will either conceal or reveal and they provide the counterdeception analyst with a checklist for the kinds of questions that must be considered when trying to determine the existence and form of a deception operation. The Plus-Minus Rule, on the other hand, is the cornerstone of their theory. This rule is based on the fact (noted by R. V. Jones in 1942) that [58], "No imitation can be perfect without being the real thing." Therefore, even though the imitation may share many of the characteristics of the original, it *must* lack at least one characteristic marking the original and it will often have at least one characteristic that the original does not possess. According to Whaley [59], "If either a plus (added) or a minus (missing) characteristic is detected, the imitation stands revealed. Note that a most important corollary of this rule is that the detective need not discover all the discrepancies or incongruities, a single false characteristic, whether plus (added) or (minus) is quite enough to prove the fakery."

Whaley is quick to note, however, that the Plus-Minus Rule demands total certainty about the added or missing characteristic and that while this is always possible, it is seldom likely in the real world. With this in mind, the next components of their counterdeception theory can be thought of as applied theory suitable to decision making under uncertainty. The first element, the *Congruity-Incongruity Rule,* flows from the Plus-Minus Rule and appears to be based on the results of Whaley's case studies of deception detection professionals. He found that these professionals clustered into two groups: *congruity testers* (e.g., scientists, internists, and historians) and *incongruity testers* (e.g., police detectives, interrogators, trial lawyers, and forensic pathologists). In the Congruity-Incongruity Rule, the emphasis is obviously all on incongruities [60]: "Every deception operation necessarily leaves at least two clues: incongruities about what is hidden; and incongruities about what is displayed in its stead" and "because neither simulation nor dissimulation can ever be done flawlessly, however, their detection also is always possible. In other words, discrepancies (incongruent clues) inevitably suggest alternative patterns (hypotheses) that themselves are incongruent (discrepant, anomalous, paradoxical) at some point with reality." In other words, detecting incongruities is the key to detecting deception.

The next several elements of the Busby and Whaley theory represent a portfolio of methods applicable to detecting deception:

- *Locard's Exchange Principle*. Although normally associated with *physical* evidence, Whaley suggests it can also be applied to deception by adding "psychological perceptions" to the principle. Unfortunately, he does not offer any insights into how these perceptions are to be added.



		Description
Genearl theory	Categories of detectables	Pattern, players, intention, payoff, place, time, strength, style, and channel
	The plus-minus rule	A single false characteristic—either one the real entity does not possess (a plus) or one it lacks (a minus)—is sufficient to prove the entity is fake.
Decision making under uncertainty	The congruity-incongruity rule	Real entities are completely congruent with all of their characteristics; therefore, every false entity will display at least one incongruity.
	Locard's exchange principle	A perpetrator always leaves some physical evidence at the crime scene and always takes some away.
	Verification	It is always possible to find a way to verify a hypothesis.
	The law of multiple sensors	Multiple sensors will almost always prove more effective than a single one, even when each is less precise.
	Passive and active detection	Deception may be detected by analysis (passive) supported by active intervention aimed at collecting missing key facts. This intervention takes the form of defining new collection requirements or by running controlled experiments, including the use of traps and tripwires, to trick the adversary into betraying himself.
	Predetection	Predicting an adversary's deception plans by analysis of his deceptive style, capabilities, and goals.
	Penetration and counterespionage	The adversary's deception plans can be discovered through the use of *espionage,* penetrating the adversary's organization with human agents or technical collection devices, and *counterespionage,* discovering the deceiver's double agents within one's own organizations.
	The prepared mind and intuition	The ability to not only discover the meaning of chance events but to also make effective use of that knowledge depends wholly on systematic mental preparation. Such mental preparation also makes intuition possible.
	Indirect thinking and the third option	The goal of indirect thinking is to come up with an indirect answer—the third option that the adversary was not expecting.
	Busby's ombudsman	"The essence of the Ombudsman Method is to force one to confront straight on that nagging, almost subliminal, sense of unease about a situation or person that somehow does not seem quite right, that does not quite fit as it should those little incongruities that signal a deception in progress" [66, p. 217].

Figure 5.3 The Busby-Whaley theory of counterdeception.

- *Verification*. Once the Congruity-Incongruity Rule, Locard's Exchange Principle, or some other method provides evidence of deception, Whaley suggests that it is "always" possible to find a means of verifying the deception hypothesis. Of course, the costs of doing so may be prohibitively high, but it could be done.
- *The Law of Multiple Sensors*. This law is based on the insights of R. V. Jones who noted that [60], "The ease of detecting counterfeits is much greater when different channels of examination are used simultaneously." Whaley notes that multiple sensors are almost always more effective than a single one and are also less vulnerable to countermeasures.
- *Passive and active detection*. To Whaley [61], passive detection is synonymous with the "straightforward analysis" of evidence and "always leads to inconclusive results unless all the key facts are available." Therefore, active detection must be used to collect the missing facts. Active detection involves levying new collection requirements on the various INTs (e.g., HUMINT, IMINT, and SIGINT) or by running "controlled experiments" to provoke the adversary into creating new evidence that might reveal the deception.
- *Predetection*. J. C. Masterman of World War II Double Cross fame was also the author of two detective novels. In the second of these, *The Case of the Four Friends: A Diversion in Pre-Detection*, the detective in the story, Ernest Brendel, is persuaded [62], "…to tell the tale of how he 'pre-constructed' a crime, rather than reconstructing it in the detective's normal fashion. As he says, 'To work out the crime before it is committed, to foresee how it will be arranged, and then to prevent it! That's a triumph indeed, and is worth more than all the convictions in the world.'" Whaley makes the connection that predetection is a method whereby an adversary's deception plans can be discerned and defeated by analysis of the adversary's deception style, capabilities, and goals.
- *Penetration and counterespionage*. Espionage is a powerful form of active detection that can be used to penetrate the adversary's intelligence, military, and command organizations. A well-placed asset in the right place is all that may be needed to reveal the adversary's deception plans. Counterintelligence (CI) and counterespionage (CE), on the other hand, seek to identify and neutralize the adversary's intelligence collection efforts, especially agents who have penetrated one's own organizations. CI and CE activities can cut off important paths through which the adversary obtains information about the target's preconceptions and beliefs as well as the feedback needed to know how his deception operations are doing. In addition, CI and CE operations can reveal the existence of double agents being used as a channel for feeding the adversary's disinformation to the target.
- *The prepared mind and intuition*. The prepared mind refers to a famous quotation by Louis Pasteur: "Dans les champs de l'observation le hasard ne favorise que les esprits prepares." Pasteur made this comment at a lecture given at the University of Lille in December 1854. Translated into English, it means "In the fields of observation, chance favors only the prepared mind," or more succinctly, "chance favors the prepared mind." The essence of Pasteur's

remark is that the ability to recognize the significance of chance events and make effective use of that knowledge depends wholly on systematic mental preparation. On the other hand, intuition is [63] "our capacity for direct knowledge, for immediate insight without observation or reason." It is the police detective's hunch, Irwin Rommel's *fingerspitzengefühl*, or the scientist's sudden awareness of the solution to a difficult problem while taking a shower. It is not unreasonable to think that accurate intuition is also a result of the same systematic mental preparation associated with the prepared mind.

- *Indirect thinking and the third option.* Whaley uses the term *indirect thinking* in honor of B. H. Liddell Hart's theory of the *indirect approach* to strategy [64]. The essence of this theory is to avoid direct confrontations with the enemy but instead upset his equilibrium—keeping him uncertain about the situation and your intentions—and confront him with what he does not expect and is therefore not prepared for. Such an approach often yields a third option—one that the adversary was not expecting. The German advance through the Ardennes in 1940 is an excellent example of the indirect approach and the third option. The French expected a German attack against either the Maginot Line or through Belgium. Instead, the Germans came up with a third option—the attack through the Ardennes and the Battle of France was over in just 44 days. Whaley is suggesting that the purpose of indirect thinking is to come up with an "indirect answer"—that third option—and that this ability to envision options available to an adversary that would be otherwise hidden or ignored is an essential method of counterdeception.

The final component of Whaley's overall theory of counterdeception is a specific method—the Jeff Busby *Ombudsman Method*. This method was developed by Busby in 1978 as a means of teaching casino employees to detect cheating without teaching them how to cheat at the games themselves. Whaley does not describe any of the details of the Busby Method; however, it is apparent that it is based on looking for discrepancies, irrelevancies, and misdirection [65] as well as some indirect thinking. He does state that [66], "The essence of the Ombudsman Method is to force one to confront straight on that nagging, almost subliminal, sense of unease about a situation or person that somehow does not seem quite right, that does not quite fit as it should those little incongruities that can signal a deception in progress." Whaley suggests that the method "seems the most promising of several suggested approaches" for use in training analysts about deception as well as in the analysis of both current and historical cases of deception.

In another chapter of Godson and Wirtz's book, Paul Rossa identifies several key issues germane to counterdeception [67]. The first of these affirms the second principle of deception we proposed in Chapter 2: *denial*. Rossa notes that [68], "Uncovering secrets also is key to exposing deceptions. Consequently, counteracting foreign denial efforts is critical to countering foreign denial and deception." Even identifying the deceiver's denial operations helps the counterdeception effort by helping to task collection resources where they are most likely to do the most good. An adversary's efforts to conceal information about a subject can also suggest the possibility that deception operations associated with the subject may also exist, thereby by affecting how all information on that subject is interpreted.

Other issues are related to recognizing the existence of a deception operation. Rossa points out that determining what information the analyst decides to use, discard, or “reshape” is hard enough, but it is even more difficult when deception is involved. Rossa makes the point that recognizing the existence of a deception operation depends heavily on the metadata (data about data) that is available. Examples of metadata include the way in which the data was acquired and the circumstances surrounding the acquisition. The metadata, along with the content of the information, may provide some hints regarding the presence or absence of a deception operation. Unfortunately, these hints are all too often ambiguous or contradictory.

Another important part of recognizing deception is paying close attention to information about a potential or suspected deceiver. What are his motives? Would the use of deception increase the likelihood of achieving his objectives? Has the adversary demonstrated a strong predisposition to the use of deception in the past? Does he possess the knowledge and capabilities to mount an effective deception operation?

Finally, Rossa addresses the issues of reducing one’s own “susceptibilities” to deception. One of the most important factors affecting the deception target’s susceptibility to deception is the extent of the adversary’s knowledge about the target’s strategies and methods of collecting intelligence, his analytic methodologies, and how the resulting intelligence is used to form judgments and make decisions. Such knowledge can come from a variety of sources, including the adversary’s espionage operations or the unauthorized disclosure of secret information [69]. Reducing that susceptibility depends on counterintelligence and counterespionage operations as well as the development of information gathering and processing methods that are unknown to potential deceivers or that are difficult to manipulate. Nevertheless, such efforts do not entirely eliminate the risk of deception. Deception can still succeed even when the deceiver’s information about the target is incomplete and secret intelligence collection and analysis methods may still be affected by deception operations. Better analytic methods and tools can also contribute to reducing susceptibility to deception. Rossa suggests that [70]: “The intelligence community would profit by development of conceptual frameworks, indicators, and analytic techniques that hold promise for recognizing and countering foreign D&D as it occurs.” He calls for qualitative and quantitative analysis of historical cases of deception and the need for D&D analysis to continue to evolve in order to keep pace with the issues and technologies associated with the post–Cold War world.

Scott Gerwehr and Russell Glenn represent a new generation of national security analysts whose focus is on strategic deception. In their report *Unweaving the Web*, Gerwehr and Glenn also address counterdeception and hypothesize that [71], “the most effective approaches to penetrating deception entail (1) combining more than one category of counterdeception and (2) applying the right category of counterdeception.” They then identify five categories of counterdeception, three of which focus on defeating deception by emphasizing the collection and processing of data. The first three categories are:

- The type or amount of data collected (e.g., using radar or hyperspectral sensors to defeat camouflage paints and netting).

- The methods for collecting data (i.e., the methods by which the sensors are employed). For example, changes to collection plans or search plans may disrupt an adversary's attempts to conceal his movements.
- The analysis of the data collected (for example, can alternative scenarios be developed using the same data?)

The fourth category focuses on unmasking deception through the use of one's own deceptions. For example, a feint or demonstration might force concealed units to maneuver or engage. The final category consists of strategies for rendering the adversary's deceptions moot. This is often the U.S. military's approach to counterdeception. For example, if an adversary has deployed numerous decoys among its real units (e.g., tanks or surface-to-air missile), the U.S. ability to employ overwhelming firepower makes it possible to target all potential targets without bothering to tell them apart.

Effective counterdeception therefore depends not only on applying the right category of counterdeception methods but also on applying methods from more than one category. Gerwehr and Glenn suggest that much more research needs to be done to resolve the issues raised by questions such as:

- What counterdeception methods should be matched to particular types of deception?
- Which of those methods are the most effective against individual deception techniques or are effective against the broadest range of deception techniques?
- What are the situational factors that affect their use?
- Which methods require the most time or manpower to use effectively?
- Which methods complement or interfere with each other?
- Do any of the methods work against one type of deception technique but in turn increase the vulnerability to another?

Even more recent work has been done by Stech and Elsässer who extend Johnson et al.'s model to develop a counterdeception "business process" [72]. The process links previous work done by Whaley, Jones, and Heuer to the Johnson model (see Figure 5.4) and Stech and Elsässer then use this process to in an effort to improve the effectiveness of Heuer's alternative competing hypothesis (ACH) method as a counterdeception tool. The first step of the process addresses the detection of anomalies using techniques based on Whaley's congruity-incongruity rule. One challenge for analysts though is that the detection of anomalies (incongruities) is not necessarily evidence of detection of deliberate deception. They may result from sensor malfunctions, unintentional distortion or corruption of data or information during transmission, or analytical error. In fact, deception is often successful because the deception target explains away such anomalies and failing to correctly attribute them to deception. That is where the next step in the process comes in. There must be some way of linking anomalies to deception, and Stech and Elsässer propose that R. V. Jones's concepts of deception masking provides such means—analyzing the anomalies through multiple information channels. The third and fourth steps use ACH to assess the likelihood that the observed anomalies are

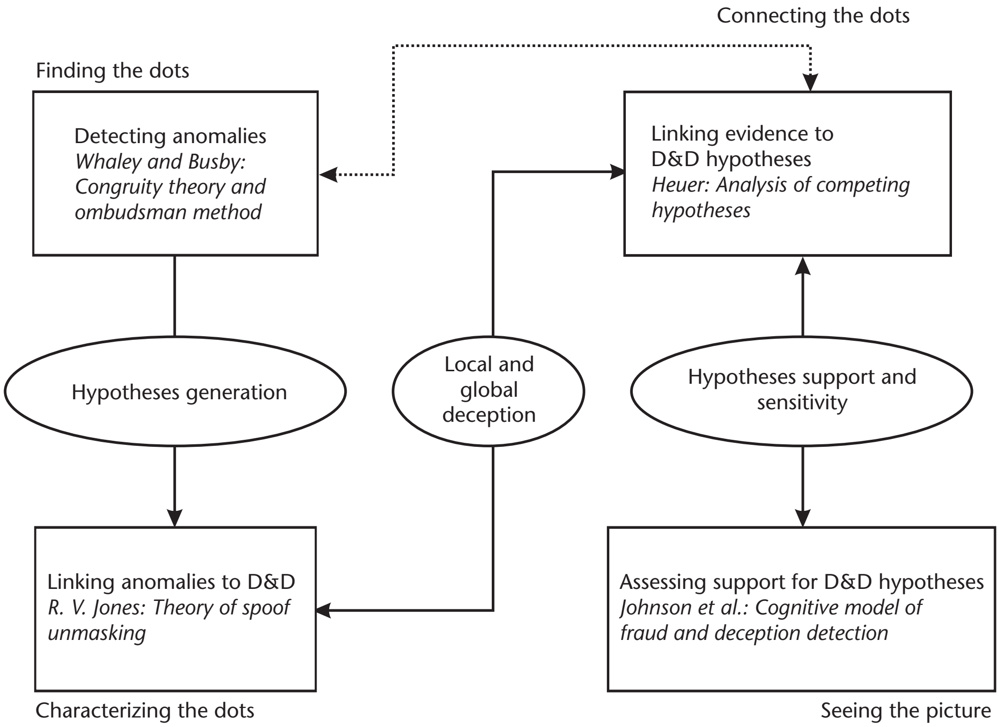

Connecting the dots
Finding the dots
Detecting anomalies
Whaley and Busby: Congruity theory and ombudsman method
Linking evidence to D&D hypotheses
Heuer: Analysis of competing hypotheses
Hypotheses generation
Local and global deception
Hypotheses support and sensitivity
Linking anomalies to D&D
R. V. Jones: Theory of spoof unmasking
Assessing support for D&D hypotheses
Johnson et al.: Cognitive model of fraud and deception detection
Characterizing the dots
Seeing the picture

Figure 5.4 The Stech-Elässer counterdeception business process. (*Source:* [72].)

associated with a probable deceptive course of action (COA) and to evaluate the level of support for each identified hypothesis.

Stech and Elsässer have also developed what they call *alternative competing hypotheses for counterdeception* (ACH-CD). Their most significant adaptations to Heuer's original eight-step outline for the analysis of competing hypotheses are [73]:

- Adding the "other" or "unknown" hypothesis to step 1 (i.e., "Identify the possible hypotheses to be considered"). This modification supports further Bayesian analysis of the alternative hypotheses.
- Making sure that step 2, "Make a list of significant evidence and arguments for and against each hypothesis," considers not only the case where evidence supports a hypothesis, $p(E|H_i)$, but also the likelihood that observing that same evidence if the hypothesis is not true, $p(E|\neg H_i)$.
- Specifically considering deception-related COAs in steps 4 ("Refine the matrix") and 5 ("Draw tentative conclusions about the relative likelihood of each hypothesis").
- Adding the concept of conducting operational "experiments" to step 8 ("Identify milestones for future observation that may indicate events are taking a different course than expected") in order to provide additional intelligence that would reveal evidence of deliberate deception.

The first two adaptations support Stech and Elsässer's work on developing Bayesian belief networks to model the alternative COAs, perform sensitivity analysis in order to analyze the diagnosticity of the evidence (part of Step 3 in ACH), and to suggest possible key indicators to look for that would reveal the adversary's intentions.

5.3 Searching for Common Themes

In Chapter 2 we saw that there was considerable agreement on a range of topics in the deception research community, which we then organized into six general themes (Figure 2.15). We then examined these themes in the context of a generalized deception cycle (Figure 2.13) and Waltz's three-level hierarchy of information. In this chapter, we propose to take a similar approach and organize the various counterdeception concepts, approaches, models, and methods presented in the previous sections into general themes using a framework based on the counterdeception definitions presented in Section 5.1. These counterdeception themes are then compared to the deception themes of Chapter 2 and used to synthesize a set of fundamental principles of counterdeception.

5.3.1 A Holistic Approach to Counterdeception

In Section 5.1, we saw that counterdeception consists of both intelligence and operational functions. These can be broken down as follows:

- *Intelligence functions*. Awareness of deception cues, detection and exposure of deception operations, and discovery and penetration the adversary's real capabilities and intentions;
- *Operational functions*. Negate or mitigate deception's effect and exploit the adversary's own deception plan.

These five functional dimensions form a simple, yet useful framework for thinking about counterdeception; however, keep in mind that these dimensions are not mutually exclusive. They are, in fact, highly interdependent and form more of a continuum of functions than a set of independent activities. This suggests that counterdeception requires a more holistic approach than is suggested by the traditional intelligence cycle. As we will see, the themes that emerge from the counterdeception literature reinforce this idea.

Our examination of the research suggests that there are nine themes representing processes and methods that would ideally work together synergistically to identify and defeat the adversary's attempts at deception. Figure 5.5 shows these themes arranged within the framework of the five intelligence and operations functions. Like the functional dimensions of our counterdeception framework, these themes are themselves interdependent and reflect a holistic approach to counterdeception.

The first theme, *human reasoning capabilities*, is probably the most important since it binds the other themes together. All of the authors we have reviewed, whether in Chapter 2 or this chapter, have either explicitly or implicitly recognized

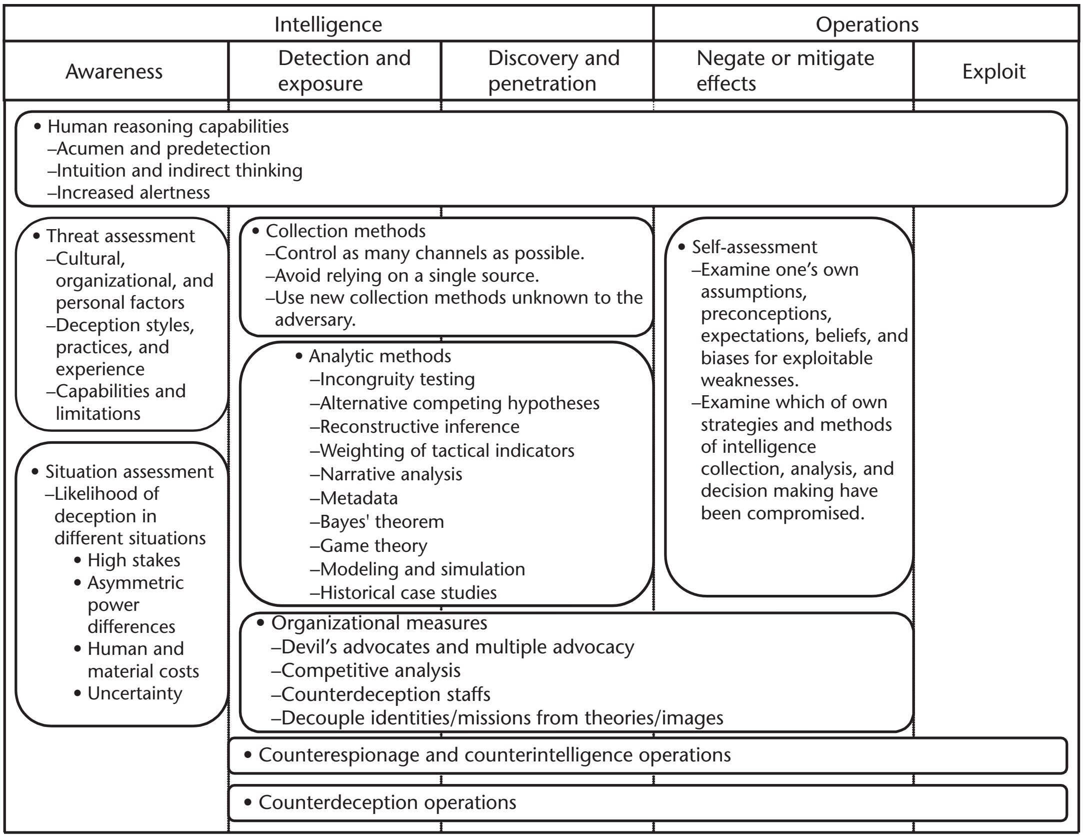

Intelligence
Operations
Awareness
Detection and exposure
Discovery and penetration
Negate or mitigate effects
Exploit
• Human reasoning capabilities
–Acumen and predetection
–Intuition and indirect thinking
–Increased alertness
• Threat assessment
–Cultural, organizational, and personal factors
–Deception styles, practices, and experience
–Capabilities and limitations
• Situation assessment
–Likelihood of deception in different situations
• High stakes
• Asymmetric power differences
• Human and material costs
• Uncertainty
• Collection methods
–Control as many channels as possible.
–Avoid relying on a single source.
–Use new collection methods unknown to the adversary.
• Analytic methods
–Incongruity testing
–Alternative competing hypotheses
–Reconstructive inference
–Weighting of tactical indicators
–Narrative analysis
–Metadata
–Bayes' theorem
–Game theory
–Modeling and simulation
–Historical case studies
• Self-assessment
–Examine one's own assumptions, preconceptions, expectations, beliefs, and biases for exploitable weaknesses.
–Examine which of own strategies and methods of intelligence collection, analysis, and decision making have been compromised.
• Organizational measures
–Devil's advocates and multiple advocacy
–Competitive analysis
–Counterdeception staffs
–Decouple identities/missions from theories/images
• Counterespionage and counterintelligence operations
• Counterdeception operations

Figure 5.5 Counterdeception themes in the deception literature.

that the success or failure of deception occurs in the minds of the analysts, commanders, and decision-makers who are its targets. Heuer is often quoted in this regard [74]: "Deception is, above all, a cognitive phenomenon; it occurs in our minds." Likewise, it is clear that many of these same researchers believe counterdeception is primarily a cognitive phenomenon as well. As Whaley concludes after examining 47 categories of real-life professionals who deal with deception [75], "Successful detection procedures were found to be largely or entirely intellectual rather than technological in nature." All of the counterdeception concepts dealing with human reasoning emphasize the role that broad, subtle powers of awareness, discernment, and discovery play in distinguishing between what is real and what is deceptively constructed by the adversary. This is why this theme covers all five dimensions of our framework in Figure 5.5.

This emphasis on concepts such as acumen and intuition has interesting implications for how one goes about implementing these ideas in real organizations. For example, Johnson et al. found that none of the 24 auditors in their study successfully identified the presence of fraud in all of the four cases they were given and, in fact, 20 auditors failed to detect fraud in at least three out of the four cases. In addition, two auditors failed to detect any fraud in any of the four cases and seven auditors failed to give an unqualified opinion on the clean cases they were presented. Obviously, not only is detecting deception difficult, but auditors also differ significantly in their fraud detection capabilities. In addition, if there is considerable variation in the counterdeception performance of highly skilled auditors examining relatively well-structured data in the form of financial statements, what must the situation be like for the analysts in the intelligence and military community who have to deal with information that is far more unstructured and ambiguous? How then can concepts like acumen and intuition be operationalized in those settings and applied to the problem of counterdeception? We will look into what approaches might provide some answers to this difficult question in the next chapter.

The next three themes working together also have the potential to make human reasoning capabilities more effective when it comes to counterdeception. These themes are themselves characterized by yet another theme (i.e., the concept of an assessment process). These three themes, *self-assessment*, *threat assessment*, and *situation assessment*, focus on what Handel referred to as “knowing thine enemy” and “knowing thyself.” Of course, Handel was not the first to draw this conclusion. The ever-quotable Sun Tzu observed [76], “Therefore I say: ‘Know your enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant of the enemy and of yourself, you are certain in every battle to be in peril.’” What was true over 2,000 years ago is amazingly still true today. Perhaps that was why the FORTITIDE deception was successful; Hitler was ignorant of both his enemy *and* himself.

The need for *self-assessment*, to know thyself, is a response to the empirical evidence that deception is almost always successful especially when the deception operation exploits the target’s own preconceptions and expectations (M-1 type deceptions). Given this obvious vulnerability, several authors advocate conducting such assessments as an important means of negating or mitigating deception’s effects and their work suggest that this should be a two-pronged process. First and foremost is the need to make both analysts and decision-makers aware of their own assumptions, preconceptions, beliefs, and biases. This type of awareness is not quite the same kind of vigilance implied in the awareness dimension of our framework, which involves an awareness of the presence or absence of external environmental cues. Rather it is inwardly focused and stresses consciousness of one’s own self. As Jervis notes [77]:

> People often not only have a limited understanding of the workings of other’s arguments, they also do not know the structure of their own belief systems—what values are most important, how some beliefs are derived from others, and what evidence would contradict their views. Particularly dangerous is the tendency to take the most important questions for granted. Analysis of policies that failed indicates that many crucial errors occur not because decision-makers arrive at the wrong answers, but because they ask the wrong questions. This often involves taking too many things for granted and failing to scrutinize basic assumptions.

Such knowledge is essential to mitigating and negating the adversary’s attempts at deception since deception relies so heavily on just such ignorance. The hope is that the self-assessment process will make analysts and decision-makers more alert to information and situations that appear to be too good to be true as well as making them less likely to casually dismiss information that conflicts with their expectations or beliefs. As Handel points out [78], "Under certain circumstances, *the more perfectly an intelligence puzzle fits together, the greater the danger of a possible deception ploy*. This is particularly true when information—the solution to an important and complex intelligence puzzle—is received in the absence of much noise and contradictory evidence, and when the resulting conclusions conform neatly to one's hopes and expectations."

The second prong of the self-assessment theme stresses the need to know which of your own strategies and methods of intelligence collection, analysis, and decision-making have been compromised. The importance of this vulnerability cannot be stressed enough since deception is in one sense a battle for control of information channels. Deception practitioners and researchers urge both the deceiver and target to try to control as many channels as possible. The deceiver seeks to compromise channels that the target considers to be credible and reliable without the target's knowledge. In a similar manner, the target seeks to develop channels unknown to the deceiver. The knowledge that the existence of a secret channel has been compromised or that an adversary has discovered a channel considered to be particularly valuable by the target is absolutely critical to the detection and discovery dimensions of counterdeception.

Since knowing thyself is likely to only produce a 50–50 chance of success according to the venerable Sun Tzu, if you want to be victorious in the next 100 battles, you need to know your enemy as well. The *threat assessment* and *situation assessment* themes focus on the various factors that influence an adversary's decision to use deception. In a counterdeception context, the factors suggested by Daniel and Herbig provide an excellent starting point for any threat assessment and should be supplemented with information about the adversary's capabilities and experience with running deception operations For example, is deception part of the adversary's doctrine? Does he typically rely on specific styles of deception? Have previous attempts at deception resulted in success or failure? The *situation assessment* theme recognizes that the use of deception is likely to be highly situation dependent. Normal situations will most likely only call for normal deception measures (i.e., denial in the form of security measures). For example, sophisticated deception operations are not normally associated with conventional weapons development programs such as routine improvements to armored vehicles. On the other hand, other situations (high stakes or asymmetric differences in power or capability between the adversary and the target) may make it more likely that an adversary will employ more sophisticated deception measures. One needs only to watch the evening news to see any number of stories (nuclear proliferation for instance) that are examples of potential high-stakes situations where deception is likely to play a role. These two assessment processes fit naturally under the awareness dimension of our framework since the resulting knowledge helps to prime analysts to recognize and register both the obvious and subtle cues (e.g., the MOM warning signs in the CIA tradecraft note) that help them to detect deception operations.

Our next two themes, *collection methods* and *analytic methods*, form the methodological foundation for both detecting and exposing deception and discovering and penetrating the real story behind the deception. Collection methods drive what the target observes and subsequently perceives. From the days of R. V. Jones to the present, the number-one prescription for countering deception has been to try to control as many channels (sources) of information as possible with the corollary to this rule being that one should avoid relying on a single source of information wherever possible. This is especially true when the stakes are high. Since human sources and technical collection systems provide the data and information needed to both detect and penetrate a deception, it is also highly advisable to exploit channels that are unknown to the adversary, either by using new methods unknown to him or known methods that have been compromised without his knowledge (e.g., the Allies' ability to exploit the German Enigma code).

Human history includes thousands of years of trying to understand the events and phenomena we observe in the world around us. As a result, philosophers and scientists have developed methods of thinking (from the Socratic method of natural philosophy to the scientific method of the scientific revolution) as well as innumerable specific techniques (logic, mathematics, algorithms, and other tools) that have transformed our world. It is no surprise therefore that *analytic methods* should be a major theme that emerges from the counterdeception literature. Counterdeception relies on intelligence analysis and intelligence analysis relies first and foremost on the capabilities of human analysts. They in turn rely on analytic methods and techniques to help them make sense of the data and information pouring in from multiple sources. Two methods stand out in the literature when it comes to counterdeception. First, incongruity testing is a fundamental method that supports the detection and exposure function within our framework. Likewise, Heuer [76] emphasizes the importance of generating and evaluating alternative hypotheses (essentially an adaptation of the scientific method) "as a tool to aid judgment on important issues requiring careful weighing of alternative explanations or conclusions." Here the emphasis is less on detecting deception and more on selecting the adversary's actual course of action from other potential COAs where deception is likely a factor. The results of incongruity testing and hypotheses evaluation will more than likely raise further questions. The answers will require additional information to resolve real from false incongruities, eliminate information gaps (missing evidence), and find information that can disprove hypotheses. These information needs can be satisfied by tasking collectors and integrating their inputs with information from counterintelligence and counterdeception operations. Other methods and analytic techniques support not only the detection and discovery dimensions but also the processes associated with other themes (e.g., the use of the Bayes' theorem, game theory, and other modeling and simulation methods to support situation assessment activities). Finally, the information uncovered about the adversary's deception operations drives the planning and execution of counterdeception operations aimed at exploiting the adversary's own plans. Given the importance of these themes, we will delve further into the details of counterdeception analytic and collection methods in Chapter 7.

Although deception occurs in the human mind, we have also seen that there are organizational processes and biases that can make the deceiver's job either easier or harder. Factors such as the size of the target's decision-making groups, their goals and mindset, resources and resource allocations, the size and numbers of intelligence and military organizations, and the nature of their bureaucratic political processes all affect how information is acquired, filtered, shared, and interpreted. For example, as we saw in Chapter 3, Hitler's leadership style and the nature of the

German command structure made the Allies' job of deception notably easier than it might have been under other circumstances. The *organizational measures* theme gathers together a set of ideas that counterdeception researchers believe, theoretically anyway, should make the deceiver's job harder. The primary focus of the subjects within this theme is on ways that an organization can overcome organizational mindsets and remain open to the possibility of what Whaley called the "third way." Devil's advocacy and multiple advocacy are both simply means of putting alternative interpretations of a situation in front of decision-makers. None of these interpretations may actually reflect the true situation, but such processes help to ensure that the situation is at least seen from different perspectives and any questions about assumptions and evidence are properly raised and addressed. Jervis probably does the best job of making this point when he writes [22]:

> Of course the correct image will not necessarily emerge from this adversary process. But—and this is important enough—the decision-maker can be given a wider range of choice in two related ways. First, because he is exposed to conflicting interpretations of events and shown how alternative images make the world appear differently, he will have to exercise explicit judgment to select his explanations and images rather than immediately seeing one view as the only possible one. Second, debates will help bring out the implicit assumptions discussed above. An individual rarely has the ability or the incentive to expose the structure of his beliefs, and interaction with someone who holds a different position is usually the best, if not the only, way for those he is advising, and indeed for the person himself, to see where his arguments are most vulnerable. It is unlikely that any participant will be converted. But those who listen to the arguments are in a good position to learn what perspectives they are rejecting, what evidence they should examine more closely, and what assumptions need further thought. As a result, fewer important questions will be overlooked because everyone agrees on the answer.

Our two final themes represent proactive means of counterdeception that play important roles across both the intelligence and operational dimensions of our framework. The potential target of deception does not have to be, and in fact should not be, a passive participant in the process. Instead of simply accepting the data and information (both real and false) received through his information channels, the target can conduct his own espionage and technical collection operations aimed at gathering intelligence about the adversary—his plans, capabilities, and real intentions. Counterespionage and counterintelligence operations focus on denying the adversary the information he needs to plan and execute his deception operations and, most importantly, uncovering his double agents in order to negate their value or even turn them against the deceiver. In cases where deception is suspected, counterdeception operations can be used to probe the environment in order to provoke the adversary to some action that will confirm the deception or, better yet, reveal his true plans. Likewise, if intelligence confirms the existence of a deception operation, the target can conduct his own counterdeception operations to deceive the adversary that his deception working while simultaneously undertaking operations to exploit the adversary's plans.

5.3.2 Counterdeception Themes and the Deception Cycle

In Chapter 2 we proposed that a model of a general deception cycle could be used to understand the basic workings of deception. Figure 5.6 shows the impact the nine counterdeception themes can have on the different steps in the cycle. At the far right-hand side of the figure we see that, as always, *human reasoning capabilities* play a decisive role in how observations of the environment are transformed into knowledge and how that knowledge is transformed into decisions and actions. Human acumen, sagacity, and intuition determine the most likely explanation (the reconstructed story) that accounts for the observed data as well as what to make of it and what to do about it. Also on the right-hand side of Figure 5.7 are three of the themes that help leverage those human capabilities. The main impact of the analytical methodologies theme is on helping analysts to reconstruct the deception story and, more importantly, recognize that it is a deception. The self-assessment theme influences the target's perceptions of the story. It enables analysts and decision-makers to ask questions like: Does the reconstructed story fit a little too well with expectations? Finally, the impact of the organizational measures theme is on the target's understanding (and timeliness) of the situation as well as on the resulting decisions and actions that need to be made.

On the left-hand side of Figure 5.7 are the threat and situation assessment themes—the "know thine enemy" themes. The impact of these themes is to try to get one step ahead of a potential adversary by identifying his possible motives for deception as well as the situations where those motives are likely come into play.

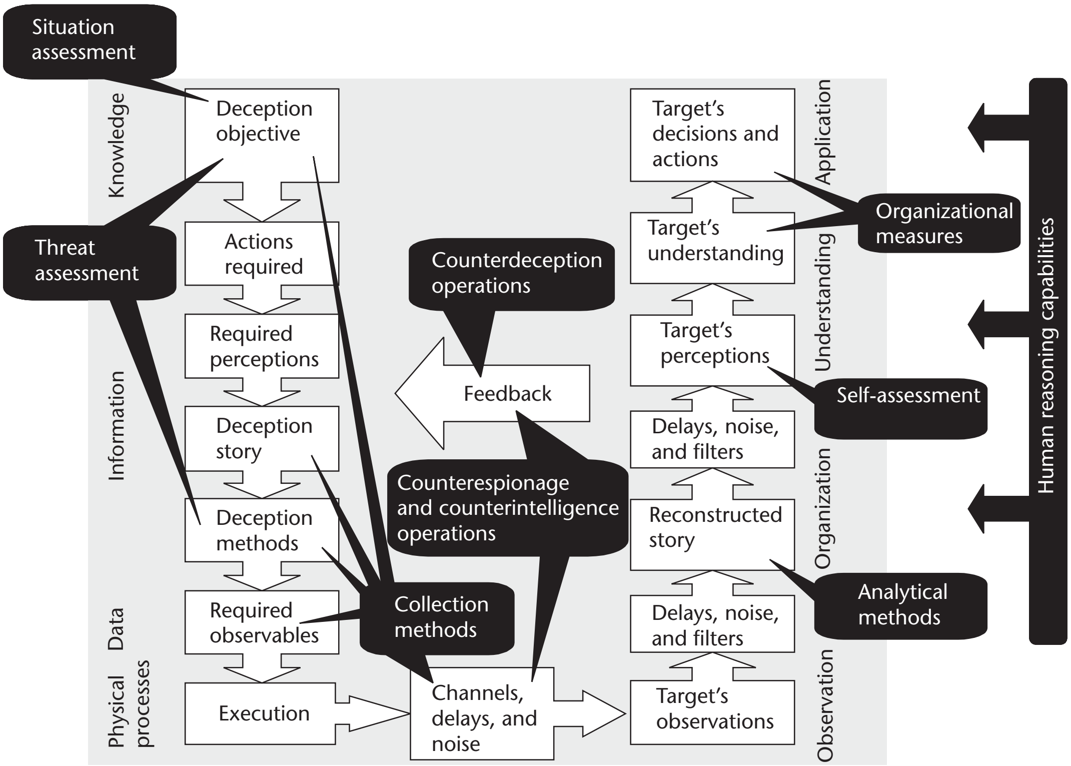


Figure 5.6 Counterdeception themes in the general deception cycle context.

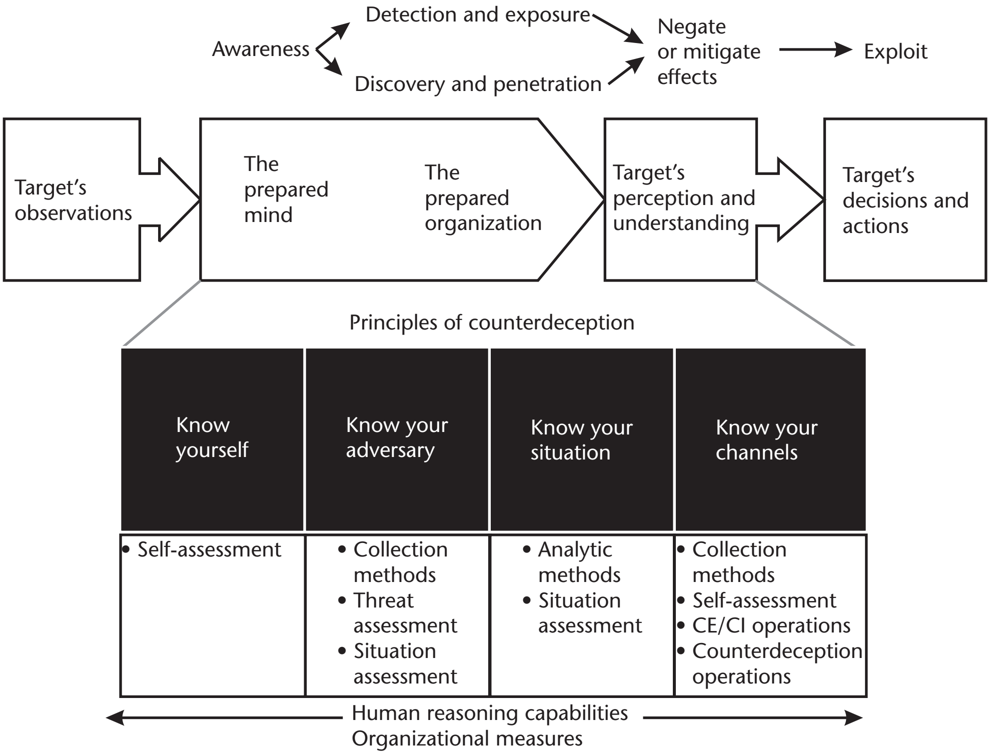


Figure 5.7 Principles of counterdeception within the context of the counterdeception framework.

These motives drive the adversary's deception objectives and the subsequent actions the adversary wants the target to take. In addition, the threat assessment helps to identify likely deception methods the potential adversary is likely to be capable of employing to achieve his objectives.

In the middle of Figure 5.6, we see that the impact of counterdeception and counterespionage/counterintelligence operations falls primarily on the feedback that the deceiver receives from the target. Depending on the feedback that he receives (see Figure 2.10), the deceiver must make a choice whether to maintain, escalate, or stop the deception. By discovering and manipulating those feedback channels, the target has the potential to force the adversary to show his hand. Discovering those feedback channels is where CE and CI operations come into the picture. Leaks can either be closed off or used to manipulate the deceiver's perception of how the deception operation is proceeding. The same goes for the deceiver's human and technical collection sources (spies, bugs, compromised secure communications systems, and so forth). Counterdeception operations can be used to manipulate other channels of information the deceiver relies on such as overhead reconnaissance or diplomatic assets. CE and CI operations also impact the channels of information available to the target. As we said before, this involves exposing those channels that are being used as part of the deception operation but also involves helping to protect the channels that the deceiver is unaware of.

At first glance, the collection methods theme appears to have considerable potential for counterdeception. As we have seen, controlling as many channels of information as possible is a key counterdeception maxim. Not only is this necessary from an analytical sense, but controlling as many channels as possible may also restrict range of deception methods available to the deceiver and drive his cost of deception up by increasing the number of observables that are required to produce a realistic deception scenario. A broad range of robust collection methods across all the INTs increases the likelihood that the target may be able to penetrate the deceiver's security measures and discover the existence of the deception operation (say, through a human asset or a COMINT intercept), the details of the plan (the deception story), and the deceiver's objectives themselves. Nevertheless, it is important to recall one more time Heuer's cautionary words [79]: "The kinds of additional information one might realistically expect to obtain through enhanced collection capabilities, however, are unlikely to reduce vulnerability to deception significantly. Any systematic counterdeception program must focus primarily on problems of analysis, only secondarily on collection."

Before moving on it is important to once again stress that our interpretation of the counterdeception literature leads us to the conclusion that it represents a holistic process. Harris [5] decries "seat-of-the-pants counterdeception efforts" as "uncoordinated, perhaps sporadic efforts to detect and outwit foreign deception operations and calls for "the coordination of *detection* and *countermeasures* programs in a *counterdeception system*." Systems are holistic; their properties cannot be explained simply by examining the properties of their components. Nothing in the counterdeception literature contradicts Harris's recognition that counterdeception has this same characteristic. Although our nine themes do not yet constitute a formal counterdeception system, it should be clear that they can only be effective when used in a highly coordinated, mutually supportive manner. With that in mind, let's move on and introduce our proposed principles of counterdeception.

5.4 Proposed Principles of Counterdeception

Centuries of conflict have seen strategic and tactical deception [80] transformed from "an idiosyncratic fad of exceptionally imaginative leaders" to a fairly well understood component of strategic and tactical doctrine. Our review of the literature leads us to conclude that no similar process or doctrine of counterdeception has as yet evolved. The adversary's deception planners, armed with a wide array of deception methods honed by hundreds of years of practical experience, do not face a corresponding counterdeception organization armed with a similarly wide range of practical counterdeception tools. Instead, we see that the contest between deceiver and target pits deception methods against basic human reasoning capabilities and the formal and informal processes, procedures, policies, and structures of the organizational they operate in. In essence, all that really stands in the way of the deceiver is what Pasteur called "the prepared mind" and, extending that concept, the prepared organization.

The concepts of the prepared mind and the prepared organization correspond well with the intelligence functions within the counterdeception framework introduced in Section 5.3. Pasteur's original comments were made to emphasize that only the prepared mind is receptive to the significance of anomalies or surprising results when making scientific observations. The prepared mind and "chance" combine to produce serendipitous scientific discoveries and insights. In a counterdeception context, the prepared mind is receptive to both positive and negative cues (i.e., something is different, surprising, or missing) and is then able to bring to bear a number of counterdeception methods—collection, analytical, or operational—on the problems of simultaneously detecting and penetrating the deception. The prepared organization is able to collect and organize insights and discoveries generated by individuals and teams and integrate it into the target's (political leaders and military commanders) common perception and understanding of the environment and situation in a way that negates or mitigates the effects of the intended deception. It is the prepared mind and organization, supported by a range of collection methods, analytical methods and techniques, and operational capabilities that makes the target less susceptible to deception. This basic idea is summarized in Figure 5.7, which shows how four basic counterdeception principles support the prepared mind and organization to make the target's perceptions and understanding less susceptible to the effects of deception. With that as our context, let's look at our four proposed principles.

5.4.1 Know Yourself

Sun Tzu makes it clear that, at a minimum, you must know yourself if you wish to have any reasonable hope of success in battle. The same is true in the battle of mirrors, masks, lies, and secrets [81] that characterizes the contest between deceiver and target. In Chapter 2 we saw that deception is particularly successful when it exploits the target's expectations and preconceptions, or paraphrasing Whaley, the best stratagem is one where the course of action suggested by the deception is more plausible in terms of the target's prior experience and knowledge then other COAs. Later in Chapter 3 we saw this phenomenon summed up by the simple phrase *seeing what we expect to see*. Such observations are the basis for the self-assessment theme that emerges from the counterdeception literature and lead us to our first fundamental principle of counterdeception: *know yourself*. Putting it another way, if you know you are going to see what you expect to see, you better know what those expectations are and how they came about.

Although it was made in a different context, U.S. Secretary of Defense Donald Rumsfeld's comment about known knowns, known unknowns, and unknown unknowns [82] represents an important feature of the know yourself principle. Counterdeception requires that you not only evaluate what you know and don't know (recall Crowe's Law), but that you must also consciously consider how that knowledge came about. Is what you think you know (or believe) based on fact, or is it really just an assumption or a preconception? Is what you think you know biased by expectations or ethnocentric biases? And although Rumsfeld was accused of gobbledygook [83] in many circles for the "But there are also unknown unknowns—the ones we don't know we don't know" comment [83], the consideration of the unknown unknowns critically depends on the know yourself principle because this is where expectations and biases are most likely to blind the target to potential courses of action available to the deceiver (the third option).

If Sun Tzu was right, then knowing yourself gives you at least a fighting chance at detecting deception. It also helps to bear in mind that Whaley also said [84]: "If the victim does not suspect the possibility that deception is operating, he will inevitably be gulled." Knowing yourself plays a critical role in awareness, that sense of vigilance that triggers some suspicion that something is quite not right or conversely that things are going just a bit too perfectly. Such self-awareness and self-reflection is the first step towards avoiding being "gulled."

5.4.2 Know Your Adversary

"Know your enemy." Once again our ancient Chinese stratagemist Sun Tzu points the way to another fundamental principle of counterdeception. The second principle of deception is *know your adversary*. We use the term adversary here in order to make the point that the threat of deception is not limited strictly to military enemies. The potential for deception exists in any situation—military, diplomatic, or economic—where one side can gain competitive advantage through its use. The know your adversary principle is the foundation of the two Ms in CIA Tradecraft Note No. 10—means and motive. Handel's deception typology (see Figure 2.5) provides a good framework for understanding the importance of this principle. According to Handel, all deception is directed at manipulating two categories of information: *capabilities* and *intentions*. Using the military context as an example, an adversary attempts to:

- Conceal his real capabilities in order to cause the target to underestimate the deceiver's real strength.
- Exaggerate his real capabilities in order to appear stronger than he really is.
- Conceal his plans and readiness for some action (e.g., an attack).
- Exaggerate his readiness (e.g., to deter attack).

From the counterdeception perspective, the know your adversary principle reminds analysts and decision-makers to consider the *means* the adversary has at his disposal (doctrine, training, personnel, experience, and technology) for concealing or exaggerating his capabilities if it is in his best interests to do so. Likewise, the principle focuses attention on the adversary's *motives* for concealing or exaggerating his capabilities and/or intent. These motives could range from achieving surprise, bluffing, deterrence, seeking prestige or influence, blackmail, or seeking concessions from the target. Daniel and Herbig's second set of factors related to the likelihood of deception are pertinent here. In addition, motives may change depending on the situation, so there is also a dynamic component to this principle. A country that is considerably stronger than a neighbor does not need to resort to deception in order to threaten or otherwise influence its victim. On the other hand, that same country when put into another situation involving a considerably stronger nation than itself might resort to deception in order to deter or bluff the stronger adversary.

We have taken Sun Tzu's "know your enemy" principle and interpreted it in a broader counterdeception context we label "know your adversary." Nevertheless, we have to take care not to fall into a potentially dangerous mindset involving the use of the words *enemy* and *adversary* by remembering that although large sophisticated deception operations are rare, deception itself is common. Everyone is a potential deceiver as Handel points out in one of his paradoxes discussed in Chapter 2 [85]: "*The more one has a reputation for honesty—the easier it is to lie convincingly*." Even more concisely: *Honest people/states can deceive the best*." This is why the concept of the prepared mind and the use of a holistic approach to counterdeception is so important; whether dealing with enemies (in a military sense), potential enemies, real and potential adversaries, or "honest people/states," the prepared mind and organization must be able to draw on a wide and deep pool of information about the other party. More importantly, in-depth knowledge of the adversary 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 main, perhaps only, effective weapon.

5.4.3 Know Your Situation

Our third principle, *know your situation*, focuses on the necessity for continually evaluating the environment for the cues indicating deception will have to be a considered as a major factor when formulating strategies, considering options, making decisions, or taking action. Earlier in this chapter we suggested that analysts are confronted by a continuum of deceptive activity, and most of it, like the normal security activities of an adversary (denial), can be considered normal and likely to occur no matter what the situation is. In addition, as numerous authors have pointed out, the use of large-scale, sophisticated deception operations is usually rare. This can be attributed to the fact that, with the exception of totalitarian regimes that usually have few scruples about the use of deception, most adversaries are unlikely to go to the effort to plan and execute extensive deception operations on a regular basis. As Handel points out [86], "To begin with, those who frequently make use of stratagem rapidly lose their credibility; what they may get away with one, two, or three times in succession they cannot hope to succeed with indefinitely." In addition, Maxim 6 in Figure 2.7 states [87]: "There are circumstances where deception assets should be husbanded despite the costs of maintenance and risk of waste, awaiting a more fruitful use." This maxim implies that each situation forces the adversary to perform a cost benefit tradeoff—should high value deception assets be used to take advantage of an opportunity even though their use will compromise them and render them valueless, or should they be saved in expectation of higher gains in some future situation?

The idea that the likelihood of deception is related to situational factors seems intuitively obvious. CIA Tradecraft Note 10 makes the distinction between "regular" and "suspect and sensitive" issues and it would be surprising if the distinction between the two did not include some sort of situational context aspect. There are also the obvious situational factors that we enumerated earlier such as high stakes situations and those involving asymmetric power relationships between the participants. Another important situational factor is change. Although some situational factors can be considered to be static (e.g., it is unlikely that the United States will be in the position of a second rank state caught between two large power blocs as some countries were during the Cold War), change is a constant factor in the calculus of international relations [88]. Changes in leadership, motives, political goals, military doctrine, or technological capabilities could all conceivably have an impact on the likelihood of deception. An absolutely essential aspect of knowing your situation is to recognize when such changes affect your assumptions, expectations, preconceptions, and beliefs in a fundamental way as we saw in Chapter 2, the United States' failure to recognize that Japanese naval doctrine had changed helped set the stage for the success of Japanese deception operations leading to the attack on Pearl Harbor.

Another situational factor that is important to consider is risk. In any situation, but especially those involving high stakes, it is important to remember that the high-risk, high-gain strategy is always an option available to the adversary [89]. Assessing the risks of a situation brings all three of the principles introduced so far into the picture. It relies heavily on the know your adversary principle, since estimating risk requires detailed knowledge of the adversary's culture, the frame of mind of the leadership, and what the adversary believes he knows about the target [89]. It also depends on the know yourself principle in order to mitigate the ethnocentric biases that produce mirror imaging—high-risk options are regarding as having a low likelihood of occurring because "that's what we would do in that situation." When it comes to risk, knowing your situation means memorizing Handel's second paradox [90]: "The greater the risk, the less likely it seems, and the less risky it actually becomes. Thus, the greater the risk, the smaller it becomes."

There is one final situational factor to mention. In matters of national security, the international environment is capable of distorting the perception and understanding of a situation. The signals produced by the international environment affect the target in two ways. First, events in the international environment, especially those associated with conflict, occupy the target's attention and serve as form of misdirection—focusing the target's attention away from the situation he faces with the adversary. In Chapter 2 we gave the example of how events in Europe tended to divert American attention away from Japanese intentions in the Pacific. On the other hand, a generally quiet and peaceful international environment produces another form of misdirection by reducing the target's attention and suspicions regarding important situational cues. Handel points out that this was the case at the outbreak of the Yom Kippur War [91].

The knowing your situation principle stresses the importance of human reasoning capabilities when confronted with situations that potentially involve deception. Sarbin's concept of acumen is at its core, requiring the potential target of deception to be able to switch back and forth between his perspective of the situation as well as the adversary's. It also highlights the importance of indirect thinking. Counterdeception analysts must develop the ability to break loose of potentially blinding mindsets in order to see the situation in a completely different light. Nevertheless, as powerful as these skills are, especially when combined with our first two principles, there is one more important principle that all three rely on for their effectiveness.

5.4.4 Know Your Channels

Over 2,000 years after Sun Tzu, another pioneer of deception and counterdeception, R. V. Jones, reiterated repeatedly the importance of controlling multiple channels in unmasking deception. If a playing field or game board exists for deception and counterdeception, it must surely be the channels of information over which each party vies for control. Thus, R. V. Jones's wisdom forms the basis for our last principle: *know your channels*.

This principle recognizes that data and information are the raw material from which knowledge is formed and decisions made. Our first three principles all rely on data and information in one way or another. Data and information about the success or failure of his decisions and actions influences the target's preconceptions, expectations, and beliefs. Data and information collected about an adversary contributes to the target's knowledge of the adversary's military capabilities, leadership, politics, organizations, economics, and culture. Data and information are essential to the adversary and target's understanding of situations in which they find themselves involved. All this data and information is obtained from a variety of sources, human and technical, commonly referred to as channels. The data and information flowing from these channels in turn possesses characteristics of its own; it can be relevant or irrelevant, tangible or testimonial, direct or ancillary, solicited or unsolicited, fact or fiction, clear or ambiguous, confirming or contradictory, and most importantly, credible or noncredible. Since most of these channels represent secondhand, third-hand, or even greater sources of information (see the believing what we are told category of biases in Chapter 3), the likelihood that the data and information will be distorted increases even when deception is not a factor.

Gilovich reminds us that the old maxim to *consider the source* is one of the most important ways of avoiding erroneous beliefs in everyday life but he points out that this is something that everyone recognizes in theory but is often overlooked in practice [92]. Our fourth principle is, essentially, the conscientious application of this everyday maxim to the channels of information used by intelligence analysts and political leaders. If it is only recognized in theory but overlooked in practice, the outcomes are likely to be much worse than believing what appears in the *Weekly World Review*.

5.5 Summary

The purpose of this chapter has been to derive a set of fundamental principles of counterdeception that can be used as a framework for exploring both technical and nontechnical approaches to countering deception. As in Chapter 2, our strategy for achieving this purpose has been to provide the reader with an overview of the counterdeception literature as it relates to strategic deception and then identify any common themes that emerge from that review. We then examined the impact that the resulting themes have on the general deception cycle. The resulting nine themes were then further consolidated into four fundamental principles that emphasize a holistic analytical approach to counterdeception relying on the concepts of the prepared mind and the prepared organization. In the next two chapters we will use these principles to organize our examination of ways to make human beings and organizations less susceptible to deception. Chapter 6 examines the concepts of the prepared mind and organization in greater detail and takes a high-level look at nontechnical methods and approaches for mitigating deception's effects. Chapter 7 delves even deeper into the subject of counterdeception methodology, examining technical methods of deception detection and discovery and their implementation. We will then be in a better position to decide whether or not Barton Whaley's optimism regarding the detection of deception is warranted.

Endnotes

[1] Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 12 April 2001 as Amended Through 9 May 2005, p. 126, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

[2] Rossa, P., "The Denial and Deception Challenge to Intelligence," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 225.

[3] In this chapter, we are using the general dictionary definition of the word *detection*, that is, to discover something is to determine its existence or presence. Later in Chapter 7, a more precise, technical definition will be used when discussing technical methods for counterdeception.

[4] In this chapter, we are using the general dictionary definition of the word *discovery*, that is, discovery requires exploration or investigation in an effort to find out the facts or the truth about something. Later in Chapter 7, a more precise, technical definition will be used when discussing technical methods for counterdeception.

[5] Harris, W. R., *On Countering Strategic Deception*, R-1230-ARPA, November 1973, p. 33.

[6] Whaley, B., *Stratagem: Deception and Surprise in War*, Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, 1969, p. 146.

[7] Jones, R. V., *Reflections on Intelligence*, London, U.K.: Mandarin Paperbacks, 1990, p. 131.

[8] Ibid., p. 144.

[9] Ibid., p. 132.

[10] Ibid., p. 129.

[11] Ibid., p. 134.

[12] Ibid., p. 88.

[13] Whaley, B., *Stratagem: Deception and Surprise in War,* Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, 1969, p. 147.

[14] Whaley, B., and J. Busby, "Detecting Deception: Practice, Practitioners, and Theory," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 189.

[15] Harris, W. R., *On Countering Strategic Deception*, R-1230-ARPA, November 1973, p. 40.

[16] Ibid., p. 42.

[17] Ritchie, G., "Developing the Incongruity-Resolution Theory," *Proc. of AISB Symposium on Creative Language: Stories and Humour*, Edinburgh, U.K., 1999, pp. 78–85, http://citeseer.ist.psu.edu/ritchie99developing.html.

[18] Jervis, R., *Perception and Misperception in International Politics,* Princeton, NJ: Princeton University Press, 1976, pp. 409–424.

[19] Ibid., p. 412.

[20] Ibid., p. 413.

[21] Ibid., p. 415.

[22] Ibid., p. 416.

[23] Ibid., p. 422.

[24] Ibid., p. 423.

[25] Heuer, R. J., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly*, Vol. 25, No. 2, 1981, p. 318.

[26] Ibid., p. 320.

[27] Ben-Zvi, A., "Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks," *World Politics,* Vol. 28, No. 3, 1976, pp. 381–395.

[28] Heuer, R. J., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly*, Vol. 25, No. 2, 1981, p. 322.

[29] Ibid., p. 323.

[30] Daniel, D., and K. Herbig, "Propositions on Military Deception," in Daniel, D., and K. Herbig, (eds.), *Strategic Military Deception*, New York: Pergamon Press, 1981, pp. 12–14.

[31] Moose, P., "A Systems View of Deception," in Daniel, D., and K. Herbig, (eds.), *Strategic Military Deception*, New York: Pergamon Press, 1981, pp. 136–150.

[32] Narrativepsych.com describes narrative psychology as "a viewpoint or a stance within psychology which is interested in the 'storied nature of human conduct' (Sarbin, 1986)—how human beings deal with experience by constructing stories and listening to the stories of others. Psychologists studying narrative are challenged by the notion that human activity and experience are filled with 'meaning' and that stories, rather than logical arguments or lawful formulations, are the vehicle by which that meaning is communicated." See http://web.lemoyne.edu/~hevern/nr-basic.html.

[33] Sarbin, T., "Prolegomenon to a Theory of Counterdeception," in Daniel, D., and K. Herbig, (eds.), *Strategic Military Deception*, New York: Pergamon Press, 1981, p. 157.

[34] Ibid., p. 162.

[35] Ibid., p. 170.

[36] Ibid., p. 168.

[37] Dewar, M. *The Art of Deception in Warfare*, Devon, U.K.: David & Charles Publishers, 1989, pp. 194–203.

[38] Ibid., p. 194.

[39] Ibid., p. 200.

[40] Ibid., p. 195.

[41] Ibid., p. 198.

[42] Ibid., pp. 195–196.

[43] Ibid., p. 202.

[44] Handel, M., *War, Strategy, and Intelligence,* London, U.K.: Frank Cass & Co., Ltd., 1989, p. 396.

[45] Holt provides an excellent example from World War II where a double agent provided high quality, high importance information too late to be of use. While describing GARBO's role in the TORCH deception operation that protected the Allied landings in North Africa, Holt provides this anecdote: "Under date of October 29, GARBO reported that a convoy had sailed from the Clyde (this was true), and that 'an operation of great importance is imminent and I think I fulfill my duty by advising you of this danger.' Under date of November 1, he wrote that he had learned at the Ministry of Information that the Allies were about to land in French North Africa. Alas, through some unaccountable mishap in the post office these vital messages were delayed and only reached the Germans on November 7, just before the landings. Though the information was now useless, the Abwehr was overwhelmed by the skill of their star agent. 'Your last reports are all magnificent,' GARBO was told on November 26 'but we are sorry they arrived late.'" Holt, T., *The Deceivers: Allied Military Deception in the Second World War*, New York: Scribner, 2004, p. 271.

[46] Handel, M., *War, Strategy, and Intelligence,* London, U.K.: Frank Cass & Co., Ltd., 1989, p. 397.

[47] Ibid., p. 341.

[48] Ibid., p. 333.

[49] Ibid., p. 250.

[50] "CIA Opens Door on the Craft of Analysis," *Center for the Study of Intelligence Newsletter*, Winter–Spring 1997, No. 7, http://www.cia.gov/csi/bulletin/csi7.htm#toc9.

[51] "Note 10 Tradecraft and Counterintelligence," 1995, http://www.au.af.mil/au/awc/awcgate/cia/tradecraft_notes/note_10.htm.

[52] Johnson, P., et al., "Detecting Deception: Adversarial Problem Solving in a Low Base-Rate World," *Cognitive Science*, Vol. 25, 2001, pp. 355–392.

[53] Reyhl, D., "Peer Review Guide—Materiality," 2001, http://www.reyhl.com/peer_review/materiality.html#definition.

[54] Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, Chs. 3 and 7.

[55] Whaley, B., and J. Busby, "Detecting Deception: Practice, Practitioners, and Theory," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 182.

[56] Whaley, B., *Stratagem: Deception and Surprise in War,* Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, 1969, pp. 210–212.

[57] Bell, J. B., and B. Whaley, *Cheating and Deception*, New Brunswick, NJ: Transaction Publishers, 1991, pp. 328–331.

[58] Whaley, B., and J. Busby, "Detecting Deception: Practice, Practitioners, and Theory," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 197.

[59] Ibid., p. 192.

[60] Ibid., p. 191.

[61] Ibid., p. 200.

[62] Edwards, M., "J. C. Masterman," 1998, http://www.twbooks.co.uk/crimescene/jcmastermanme.html.

[63] Myers, D. G., *Intuition: Its Powers and Peril,* New Haven, CT: Yale University Press, 2002, p. 1.

[64] Whaley, B., and J. Busby, "Detecting Deception: Practice, Practitioners, and Theory," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 209.

[65] Ibid., pp. 213–214.

[66] Ibid., p. 217.

[67] Rossa, P., "The Denial and Deception Challenge to Intelligence," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, pp. 223–228.

[68] Ibid., p. 224.

[69] See Jim Bruce's chapter, "The Impact on Foreign Denial and Deception" in *Strategic Denial and Deception: The Twenty-First Century Challenge* for a more detailed treatment of the impact of unauthorized disclosures on U.S. intelligence capabilities as it elated to deception.

[70] Rossa, P., "The Denial and Deception Challenge to Intelligence," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 227.

[71] Gerwehr, S., and R. Glenn, *Unweaving the Web: Deception and Adaptation in Future Urban Operations*, Santa Monica, CA: RAND, 2002, p. xiv.

[72] Stech, F., and C. Elsässer, "Midway Revisited: Detecting Deception by Analysis of Competing Hypothesis," 2004, p. 3, http://www.mitre.org/work/tech_papers/tech_papers_04/stech_deception/, to appear in *Military Operations Research* in early 2007.

[73] Heuer, R. J., "Chapter 8, Analysis of Competing Hypotheses," *Psychology of Intelligence*, 1999, http://www.cia.gov/csi/books/19104/art11.html.

[74] Heuer, R. J., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly*, Vol. 25, No. 2, 1981, p. 321.

[75] Whaley, B., and J. Busby, "Detecting Deception: Practice, Practitioners, and Theory," in Godson, R., and J. Wirtz, (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge,* New Brunswick, NJ: Transaction Publishers, 2002, p. 187.

[76] Sun Tzu, *The Art of War*, trans. S. B. Griffith, New York: Oxford University Press, 1963, p. 84.

[77] Jervis, R., *Perception and Misperception in International Politics,* Princeton, NJ: Princeton University Press, 1976, pp. 410–411.

[78] Handel, M. I., *War, Strategy, and Intelligence,* London, U.K.: Frank Cass & Co., Ltd., 1989, p. 341.

[79] Heuer, R. J., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly*, Vol. 25, No. 2, 1981, p. 318.

[80] Whaley, B., *Stratagem: Deception and Surprise in War,* Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, 1969. p. 4.

[81] Sarbin, T., "Prolegomenon to a Theory of Counterdeception," in Daniel, D., and K. Herbig (eds.), *Strategic Military Deception*, New York: Pergamon Press, 1981, p. 163.

[82] United States Department of Defense News Transcript, February 12, 2002, 11:31 a.m. EST, http://www.defenselink.mil/transcripts/2002/t02122002_t212sdv2.html.

[83] Plain English Campaign, "The Foot in Mouth Award," 2005, http://www.plainenglish.co.uk/footinmouth.html.

[84] Whaley, B., *Stratagem: Deception and Surprise in War,* Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, 1969, p. 142.

[85] Handel, M. I., *War, Strategy, and Intelligence,* London: Frank Cass & Co., Ltd., 1989, p. 335.

[86] Ibid., p.334.

[87] Everest Consulting Associates and Mathtech, Inc., *Deception Maxims: Fact and Folklore*, Princeton, NJ, 1980, pp. 26–27.

[88] Jervis, R., *Perception and Misperception in International Politics,* Princeton, NJ: Princeton University Press, 1976, p. 19.

[89] Handel, M. I., *War, Strategy, and Intelligence,* London, U.K.: Frank Cass & Co. Ltd., 1989, p. 243.

[90] Handel, M., *Perception, Deception, and Surprise: The Case of the Yom Kippur War*. Jerusalem: The Hebrew University, 1976, p. 16.

[91] Ibid., pp. 16–17.

[92] Gilovich, T., *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life,* New York: The Free Press, 1991, p. 109.