1

DECEPTION

The Basics

Oh what a tangled web we weave
When first we practise to deceive!

Marmion: A Tale of Flodden Field, Sir Walter Scott

This chapter introduces the basics of deception and the role of intelligence in both supporting and defeating deception. It sets the stage, with definitions and a set of basic principles, for the following chapters that explain how to conduct deception and to identify an opponent's use of it. But first, let's look at the case of a *perfect* deception—something that happens only in the movies, of course.

THE STING

The popular media have given us many great stories about well-conducted deceptions. The staged "sinking" of a Soviet ballistic missile submarine in *The Hunt for Red October* (1990) and the elaborate scam to steal $160 million from a casino owner in *Ocean's Eleven* (2001) come to mind. But few if any Hollywood movies can offer the beautifully executed deception operation set forth in the 1973 film *The Sting*.

The film is set in 1936, in the depths of the Great Depression. In it, a small-time con man Johnny Hooker (Robert Redford) has helped pull off a minor street scam with his friend Luther. Unfortunately for them, it turns out that the mark was a courier of crime boss Doyle Lonnegan (Robert Shaw) and Luther is quickly tracked and killed. Hooker must run for his life from Lonnegan's revenge. (Lonnegan does not know what Hooker looks like, which turns out to be a key part of the story.) Hooker gets advice that perhaps Luther's old friend, the legendary con

(*Continued*)

(Continued)

master Henry Gondorff (Paul Newman) can help him start anew, and tracks down Gondorff, who is hiding in Chicago from the FBI. Hooker subsequently persuades Gondorff to undertake an elaborate con operation, partially to honor Luther, targeting Lonnegan.

The scam begins when Gondorff, posing as a Chicago bookie, joins Lonnegan's high-stakes poker game on a train, and outsmarts and out-cheats Lonnegan to the tune of $15,000. In the process he earns Lonnegan's enmity by behaving boorishly, gloating over his winnings, and repeatedly mispronouncing Lonnegan's name. Hooker, posing as Gondorff's employee, visits Lonnegan's berth, supposedly to collect the winnings. He instead convinces Lonnegan that he wants to betray boorish Gondorff and take over the bookie operation with the help of a partner who works in the Chicago Western Union office. The scheme involves giving the wire results of horse races to Lonnegan, who then bets on the winning horses *before* the results arrive at Gondorff's betting parlor. After winning a race in this fashion, Lonnegan decides to bet $500,000 (about $10 million at today's prices) on the next race to wipe out Gondorff's operation and exact revenge.

At the same time, an unexpected visitor arrives: a corrupt police officer named Snyder, who is searching for Hooker in Chicago after being victimized by a counterfeit money payoff. He is intercepted by undercover FBI agents led by Agent Polk and is ordered to help them arrest Gondorff with Hooker's aid. Snyder subsequently captures Hooker and brings him to Polk. Polk then pressures Hooker into betraying Gondorff.

The next day, at the designated time, Lonnegan receives the tip to "place it on Lucky Dan," and makes his $500,000 bet at Gondorff's parlor. The race description is another part of the scam—broadcast by an announcer in a back room of the parlor. As the race begins, the tipster arrives, and when told that Lonnegan had bet on Lucky Dan to win, explains that when he said "place it" he meant, literally, that Lucky Dan would "place." The panicked Lonnegan rushes to the teller window and demands his money back, but the teller says he is too late. At this moment, Agent Polk, Snyder, and a half-dozen FBI officers break into the parlor. Agent Polk tells Gondorff that he is under arrest and informs Hooker that he is free to go. In reaction to the apparent treachery, Gondorff shoots down Hooker; Agent Polk guns down Gondorff and tells Snyder to get Lonnegan out of there and away from the crime scene.

Once Lonnegan and Snyder are gone, Gondorff and Hooker get up, unhurt—their deception is complete. "Agent Polk" and his fellow "agents" are, of course, part of the con.

Aside from its entertainment value, the movie illustrates many features of a deception operation that are covered in this book:

- It has an objective, or desired outcome scenario for the perpetrators: relieving the target—Lonnegan—of $500,000 and escaping before he finds out that he has been duped.

- It presents a story—a false picture of reality—for Lonnegan to believe, in order to get him to make the $500,000 bet.
- It has several channels for presenting the story: the poker game set-up, Hooker's representations about replacing Gondorff, the fake betting parlor, a fake race announcer in the parlor back room, a staged meeting with the tipster at the Western Union office, the intrusion of "Agent Polk," and Gondorff's and Polk's shootings.
- It demonstrates the importance of a good understanding of the opponent. In this case, Lonnegan's greed is a factor, of course. But also important is his overwhelming need to "pay back" for insults or injuries suffered, in this case from a loss in a poker game to a man he despised. And, a contributing factor to the deception's success is Lonnegan's desire for respectability that causes him to depart the scene of a shooting, leaving behind his money.
- It sets up Lonnegan for the desired decision or action steps by presenting him with the opportunity to "pay back" Gondorff for humiliating him in the poker game.
- It shows a fine sense of timing that is often critical in the execution of a deception—the Western Union tipster arriving at the right moment to send Lonnegan into a panic, and "Agent Polk's" immediate arrival to force the end game before Lonnegan could recover his wits.

The movie also illustrates some other points. Most deceptions require good showmanship, and Hollywood understands how to put on a good show—a talent that the US government occasionally calls on, as we'll see in a later case study. In every deception, curveballs will present themselves. Success demands constant observing, orienting, and reacting as events unfold. The sudden appearance of the corrupt local cop, Snyder, looking for Hooker had to be dealt with. The deception plan was changed to include him as a target. It also creates an outcome that most often is the ideal—the "mark" or opponent, Lonnegan, never realized that he had been deceived (nor did Snyder). On some occasions, though, you prefer for an opponent to know he's been deceived because of the subsequent bad decisions that he makes.

Deception itself is a word that has been used in a great many contexts, from deliberate acts within wars between nations to the deliberate acts in personal relationships as exemplified in *The Sting*. In this sense deception is a process. As it is used in this book, it also refers to a deliberate and rational process executed by an actor, in order to benefit that actor within a subjective context. The spectrum of contexts in this book is focused on actions promoting governmental rather than private interests. That includes, for example, the intelligence and operational planning processes of military, police, and/or civilian organizations.

Before expounding on the specific principles stemming from this definition, context, and framework for deception, it is worth spending a little time answering the question: Why should deception be useful to antagonists in a conflict situation?

WHY DECEPTION?

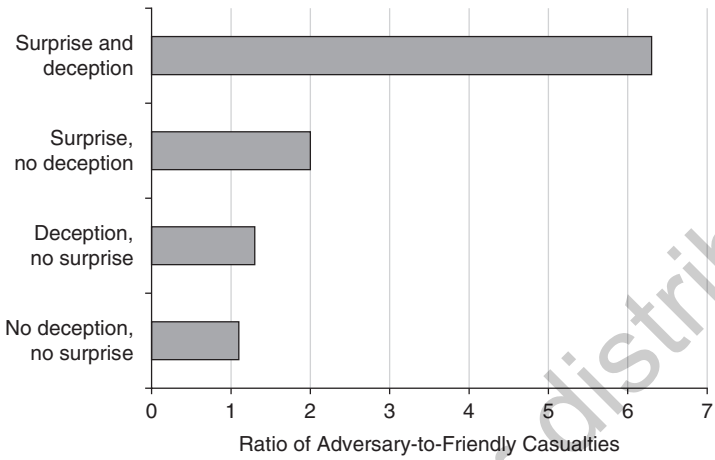
There is no better place to start than by explaining why deception is important, even essential, in the conduct of national and domestic security affairs. Countries with a substantial edge in the instruments of national power often perceive deception as something that benefits a weak power but is generally a less worthy effort for the powerful. Statistics—in military conflicts, at least—don't support that assumption, as we'll show in a moment.

One does not conduct deception for the sake of deception itself. It is always conducted as a part of a conflict or in a competitive context, intended to support some overarching plan or objectives of a participant. In a military and civilian intelligence context, the overarching plan or strategy is usually stated clearly. So in this context, the most direct answer is the following axiom: The more successful the deception in support of a plan, the greater the chance the plan will be successful. In dealing with war and security issues, measures of success are usually characterized by precious resources that include material and people. Though by no means exhaustive on the issue, one of the most accessible studies as to the effects of employing deception in operational- and strategic-level military planning is Barton Whaley's 1969 book *Stratagem, Deception and Surprise in War*.[1] By drawing on the comparative analysis of 122 historical cases, Whaley shows a clear relationship between deception, surprise, and the ratio of adversary to friendly casualty results from engagements. Figure 1-1 illustrates his results. The bottom axis is the ratio of adversary to friendly casualties—higher numbers are better. As one succeeds in either deception or surprise, casualty ratios become more favorable. The ratio improves dramatically when deception is used *and* surprise is achieved.

Favorable casualty ratios are important; however, winning in a conflict must take precedence, and that requires successful operations. In Figure 1-2, the comparative study results illustrate one clear principle: As the intensity of your adversary's surprise increases, so does your chance for a successful operation. (Low surprise equates to a 1 or 2 on a scale of 0 to 5, where 0 equals no surprise; high surprise equates to a 3, 4, or 5 on that scale.)

So one answer to "Why deception?" is embedded in the dynamics of the conflict itself. Successful deception increases the intensity of surprise; the higher the intensity of surprise, the higher the chance of operational success. And in terms of armed conflict, high intensity of surprise means higher enemy casualties and lower friendly casualties. On this final dynamic, if minimizing

FIGURE 1-1 ■ Effect of Deception and Surprise on Casualties



Source: Drawn by authors from statistics in Barton Whaley, *Stratagem, Deception and Surprise in War* [reprint of 1969 edition] (Norwood, MA: Artech House Publishing, 2007), 104, tables 5.19 and 5.20.

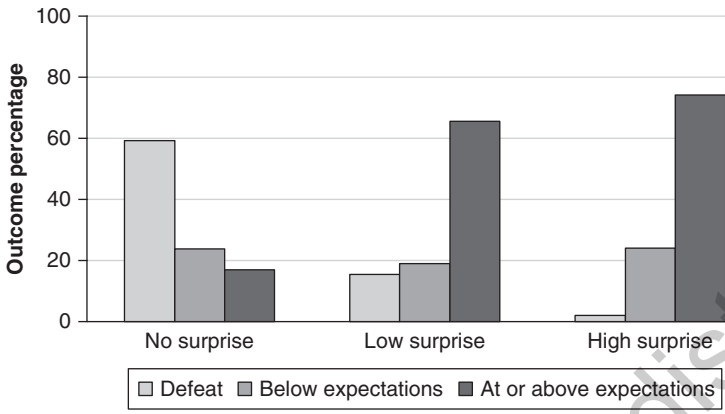
casualties and loss of material is important, then one should attempt to use deception to increase the intensity of surprise. In fact, many observers would argue that commanders responsible for the overarching plan owe as much to their troops.

Surprise clearly is an important factor in any conflict outcome, along with deception; and the two are almost always related, since surprise often is the result of deception. The two in combination are highly effective, as Figure 1-1 indicates. Intensity of surprise is also a significant factor, as Figure 1-2 shows. The percentage of defeat for the attacker in conflicts drops most dramatically as one goes from no surprise (60 percent defeats) to high surprise (2 percent defeats).

The scope of operations for militaries has widened significantly from twentieth-century state-centric interactions. Conflicts are generally more complex, with constellations of actors having diverse functions and organizational cultures becoming involved in transnational conflicts. The importance of fundamental deception skills with relation to intelligence and operational planning cannot be overstated. Deception, possibly more than ever, is an essential dynamic of conflict; therefore, how to conduct and detect it is an essential part of a twenty-first-century military's preparation of the battlespace.

Furthermore, deception has a substantial role to play in all conflicts, not just military ones. Governments must be able to apply deception activity in conflicts across the political, military, economic, social, infrastructure, and

FIGURE 1-2 ■ Effect of Intensity of Surprise on Conflict Outcome



Source: Drawn by authors from statistics in Barton Whaley, *Stratagem, Deception and Surprise in War* [reprint of 1969 edition] (Norwood, MA: Artech House Publishing, 2007), 115, merged tables 5.30 and 5.31.

information (PMESII) domains. Nonstate actors such as terrorists, criminal groups, and other militants directly engage governments through social and economic lines of operation. The insurgents in Afghanistan offer "shadow" governance. Hezbollah militancy in Lebanon has a strong social and economic engagement, as did Daesh (also known as ISIS, ISIL, or IS) in Syria, Libya, and Iraq. However, "shadow governance" in Afghanistan is also a cover for narcotics cartels. The social and economic engagement of Hezbollah conceals ideological activities that support a militant agenda and Iranian foreign policy. Daesh did the reverse, using a radical religious ideological screen to hide the fragile economic and social connections to the Sunni tribes that form their support base on the strategic level. On the operational level they disguise their intelligence organization as an organization of tribal engagement offices in major communities. They hide military command and control (C2) within the social domain of the population they control.

The statistics shown in Figure 1-1 and Figure 1-2 are generally available for the outcomes of military conflict. No similar statistics have been found that deal with the many deceptions in the political, economic, and social realms, in part because outcomes of "victory" or "defeat" are harder to establish in those arenas. But it is likely that similar ratios of success for both deception and surprise apply in all the fields of conflict covered in this book. Comparable statistics do not exist for the counterintelligence or psychological operations (PSYOPS) disciplines for good reason. The statistics are almost binary: Failure of the deception almost always means failure of the operation. The series of deceptions executed by Soviet and later Russian intelligence to protect two major US sources for almost twenty

years, Aldrich Ames and Robert Hanssen, are described in Chapter 6. Those two were able to operate long after they should have been caught because the deceptions were so successful. The World War II *Black Boomerang* PSYOPS described in Chapter 3 succeeded because its listeners continued to believe that they were hearing a German Wehrmacht radio broadcast.

With that introduction, the following section provides a deeper dive into the definitions of deception, counterdeception, counterintelligence, and PSYOPS as they are used in the remainder of the book.

DEFINITIONS

Deception

There are a number of definitions of deception in a variety of contexts, some of which overlap. The eminent author on deception, Barton Whaley, defines deception as

> Information (conveyed by statement, action, or object) intended to manipulate the behavior of others by inducing them to accept a false or distorted perception of reality—their physical, social, or political environment.[2]

Another prominent writer on the topic, J. Boyer Bell, defines deception very simply:

> Deception is the process of advantageously imposing the false on a target's perception of reality.[3]

Both definitions are accurate in the sense of defining an end result, in terms of the belief and/or behavior of others. Both also correctly describe deception as a process of deliberately inducing misperception in a target person or group of people. Deception is therefore not an accidental or unintended outcome.

Whaley explicitly takes the definition one step further, and it is an important step. His focus is on *manipulating behavior based on a false picture*. That's the widely accepted view: that belief is not enough; action (or refraining from an action that otherwise would be taken) is required for it to be deception.

However, Bell's definition explicitly recognizes that manipulating the behavior of others may not result in a good outcome, from the deceiver's perspective. In Whaley's definition, one could succeed with deception and have an unfavorable outcome, something that has happened many times in history, a few examples of which appear in this book. Bell's definition takes this into account by using the word *advantageously*; but in doing so, he excludes unfavorable outcomes. Whether it succeeds or fails, a deception is still a deception.

In this book, we simply add a word to Bell's formulation to encompass all of the cases discussed:

> Deception is a process intended to advantageously impose the false on a target's perception of reality.

This concise definition includes three basic concepts that we'll revisit frequently:

1. It emphasizes the idea that deception must have a *target.* In the next section, we'll introduce a structured approach to thinking about the targets. The section following that discusses the means, in the form of basic principles of deception.
2. It promotes the idea of using deception to gain an *advantage.* The key to deception planning is being able to envision a future situation that is more advantageous to the pursuit of the deceiver's objectives than if he or she did not conduct a deception. That future situation takes the form of a "desired" scenario to be achieved through deception, as later chapters will discuss.
3. It highlights the concept of imposing the *false* on the target's perception of reality. This false perception takes the form of a *story,* which will be discussed in Chapter 5.

Deception generally comes in two basic forms: misleading and ambiguity-increasing.

- *Misleading deceptions* reduce ambiguity by increasing the attractiveness of a wrong alternative.[4] These have the objective of getting an opponent to believe a false picture of the situation. Known in the literature as "M" type deception, it is designed to mislead an adversary toward a specific and preconceived direction.
- *Ambiguity-increasing deceptions*, by contrast, increase uncertainty or confusion so that the target is unsure as to what to believe. They are often referred to as "A" type deceptions. Such deceptions often seek to ensure that the level of ambiguity always remains high enough to protect the secret of the actual operation. Ambiguity-increasing deceptions seek to conceal critical elements of the truth to lead the opponent away from the truth, not necessarily to a specific alternative, but simply to increase the range of incorrect alternatives that the opponent must take into account.

Counterdeception

Much like the definition of deception, the term *counterdeception* is often differentiated by context and organizational mission. For example, the US Department of Defense definition follows:

> 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.[5]

This doctrinal distinction of counterdeception illustrates the prevailing view of a clear dividing line between intelligence (identifying and assessing deception) and the operational response employed to counter deception.

Intelligence organizations and many textbook authors on the subject use a definition similar to this one below, also isolating intelligence analysis from operations in countering deception:

> *Counterdeception* is an analytic process of identifying and assessing an opponent's deception operations. It usually is an intelligence function.[6]

This text is primarily focused on the intelligence component of counterdeception. In fact, Chapter 11, titled "Identifying Deception," is addressed to the intelligence team tasked with identification. This emphasis is a matter of priorities: One cannot deal with deception operationally until the deception has been identified and assessed.

But it is counterproductive and intellectually artificial to chop into parts what is, in reality, an interactive process involving both intelligence and operations. Therefore, counterdeception in this book refers to the collaborative practice of both identification and operational response to deception.

Counterintelligence

The US government defines counterintelligence as follows:

> Counterintelligence (CI) refers to information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities.[7]

The focus of this definition is on counterespionage. But counterintelligence today is more than counterespionage, and a broader perspective is needed in courses that focus on teaching the counterintelligence discipline. Most intelligence collection today relies on what the definition refers to as "other intelligence activities": open source (OSINT) and technical means—imagery intelligence (IMINT), signals intelligence (SIGINT), cyber intelligence (CYBER), and measurements and signatures intelligence (MASINT). Counterintelligence in general and deception in particular must consider all of these "INTs," or what we refer to in this book as *channels* of communication, adversarial collection, and adversarial analytical processes.

Operations

Operations is often thought of in a military context, and many of the examples in this book describe deception to support military operations. But law enforcement conducts operations to deter crime and capture criminals; and CI, as the previous definition indicates, includes "activities"—that is, operations. And nongovernmental organizations such as criminal and terrorist groups conduct operations. So the term is used in its most general sense throughout the book, in two ways: to describe an action taken, and to refer to an organization that executes political, informational, or economic as well as military actions.

Psychological Operations

Finally, before going further into the subject of deception, it's important to define psychological operations. The US military definition is as follows:

> *Psychological operations* (PSYOPS) are planned operations to convey selected information and indicators to audiences to influence their emotions, motives, and objective reasoning, and ultimately the behavior of governments, organizations, groups, and individuals.[8]

Note that this definition is somewhat broader than the definitions of deception conveyed at the beginning of this section, but it includes them all. The distinction between deception and psychological operations is often confusing to both outsiders and practitioners. One difference is the emphasis on results: PSYOPS stresses the resulting *perception* in the expectation that a desired behavior will follow. Deception emphasizes the opponent's *behavior* that produces a favorable outcome. Another difference is that PSYOPS includes conveying true information, sometimes without any falsehood. Deception, in contrast, requires conveying false information.

THE DECEPTION TARGET

All deceptions are aimed at a target. The principles, methodology, and examples in this book are concerned with three classes of targets: a decision maker, usually a military or national leader; an opposing intelligence service; or a defined group (other than an intelligence service). The target is different in each instance. But all three targets have things in common: Deception against them has a desired outcome scenario, and against all, one can make use of either misleading or ambiguity-increasing deception.

The Decision Maker

Most of the literature on deception is about targeting the decision maker for misleading deception, with good reason. In military operations where the most

deceptions are conducted, misleading the opposing commander usually results in success on the battlefield. Former deputy undersecretary of the US Army Thaddeus Holt has written the definitive account of Allied deception operations during World War II. In his book *The Deceivers* he enumerates the key commandments of misleading deception that were developed during that war. They fit well with the Whaley definition of deception:

- Your goal is not to make the opponent *think* something; it is to make the opponent *do* something.
- You want your opponent not only to do something—but do something specific.
- It is not always necessary to make the decision maker in your target network believe in the false state of affairs that you want to project; but it is enough to make him so concerned over its likelihood that he feels that he must provide for it.
- Non-action is a form of action; the decision to do nothing is still a decision.
- The decision maker(s) are the targets of deception, the intelligence services are the customers of deception.[9]

In Holt's portrayal, deception is a planned process, intentionally designed and executed to make the target of deception do, or not do, something specific. It is not intended to describe stand-alone disinformation or psychological operations, though both of these could definitely be supporting activities to a deception plan.

Sometimes it is enough to leave the opponent confused and uncertain. But a confused and uncertain opponent is likely to act unpredictably, and the deceiver cannot control the opponent's actions. The outcome may not be what was intended. Furthermore, an opponent can correct for confusion and uncertainty as the situation becomes clearer.

In targeting decision makers, misleading deception usually produces better results than ambiguity-increasing deception. The best outcomes usually happen when the opponent is certain—and wrong. And one should never underestimate the demoralizing effect of an opponent's discovering that he or she has been deceived when it is too late to recover.

The Intelligence Service

An opponent's intelligence service is usually thought of as a channel for deception. The last of Holt's commandments—that intelligence services are customers, not targets—sums up that idea. But an intelligence organization also can be the target. In counterintelligence, a frequent purpose of deception is to mislead an adversary's intelligence service about the deceivers' intelligence capabilities—what are known as "sources and methods."

So deception to support counterintelligence usually is intended to mislead. It is well known that if a deceiver can get an intelligence unit to reach a certain conclusion, it will stick with that conclusion until evidence to the contrary becomes overwhelming. The case studies about the Ames and Hanssen deceptions in Chapter 6 illustrate this. Ambiguity-increasing deceptions, by contrast, can have an opposite and generally undesired effect in counterintelligence; they can focus the opposing service on resolving the ambiguity. Of course, time is a relevant factor here. If it will take the opposing service a month to resolve the ambiguity, that may be all the time we need for the deception to be successful.

A Defined Group

Both misleading and ambiguity-increasing deceptions have important roles to play in the newer types of conflict encountered in international affairs. As these nontraditional conflicts continue to develop and as new channels open for sending a deception message to large groups, there is a need for long-term deception that is not tied to specific events or not intended to produce a specific decision. The outcome can be simply a favorable situation or state of affairs. Such deceptions typically target a defined group—an organization or even an entire population.

Deception usually targets a defined group to support psychological operations. In this role, it often overlaps with both misleading and ambiguity-increasing deception. It includes deception that does not result in a decision and action by an individual and does not fall into the realm of counterintelligence. What it shares with both of those is that it does produce an outcome.

We previously noted that an intelligence service will stick with a conclusion until the evidence against it becomes overwhelming. That's even more true for many defined groups that are targets of deception. Boston Globe Media Group science writer Sharon Begley has referred to this phenomenon as the "stickiness of misinformation." Begley notes that the more familiar we are with a claim or rumor, the more likely we are to believe it—even if the familiarity comes from attempts to debunk the claim or rumor.[10]

The view of the deception target as a defined group was developed in China nearly two millennia ago. It is recorded in a book called *Thirty-Six Stratagems* that originated in both oral and written Chinese history, with many different versions compiled by different authors over time. The book was rediscovered during World War II and popularized after the Communists came to power in China. Most of the thirty-six stratagems—which use colorful metaphors to convey the concepts—are about either deception or the use of deception as an enabler.

The perspective presented in the *Thirty-Six Stratagems* fits both non-Western views of deception and those of some nongovernmental organizations, especially terrorists and criminal groups. This perspective stresses the value of ambiguity-increasing deception, or deception in which the main objective might be none other than to create uncertainty or even chaos.

One subset of the stratagems is foreign to current Western thinking about the opponent as a deception target—though Niccolò Machiavelli would undoubtedly

recognize them, since he argued for the same stratagems in the sixteenth century. This subset emphasizes the use of deception against neutrals or even allies instead of opponents. Some examples follow:

- *Kill with a borrowed sword*. Attack an opponent using the strength of a third party. Use deception to persuade an ally to attack, for example.
- *Watch the fires burning across the river*. Avoid engaging in a multiforce conflict until all the others—opponents, neutrals, and allies—have exhausted themselves. Then enter the conflict with your forces intact. The form of deception implied by this stratagem is to use deceit to conceal your real intent from the others.
- *Borrow the road to conquer the State of Guo*. Borrow from an ally the means to attack a common enemy. After defeating the enemy, use those same means to attack the ally that lent them to you.[11]

The second set of stratagems (below) violates Holt's maxim for misleading deception against decision makers cited earlier: that the goal is to make the opponent *do* something. These mostly fall into the PSYOPS realm. The objective here is to use all means, including deception, to create chaos and to destabilize the opponent, thereby creating a favorable outcome scenario. There are several of these in the thirty-six stratagems, suggesting that they play an important role in Chinese thinking about conflict. Some examples follow:

- *Remove the firewood from under the pot*. This argues for an indirect approach, rather than directly confronting an opponent. Operations are aimed instead at the opponent's ability to wage a conflict.
- *Trouble the water to catch a fish*. Create confusion in the opponent's organization and use it to promote your objectives.
- *Feign madness but keep your balance*. Pretend to be a fool or a madman. Create confusion about your motives and intent. Encourage an opponent to underestimate your ability and make him overconfident.
- *Hit the grass to startle the snake*. Do something spectacular but apparently purposeless, strange, or unexpected to confuse the opponent or provoke a response that furthers your goals.
- *Replace the beams with rotten timbers*. Disrupt the opponent's organization or standard processes. The idea is to tear apart the opponent's cohesiveness.
- *Let the enemy's own spy sow discord in the enemy camp*. Undermine your enemy's ability to fight by secretly causing discord between her and her friends, allies, advisors, family, commanders, soldiers, and population. While she is preoccupied settling internal disputes, her ability to attack or defend is compromised.

Once the stage has been set using one or more of these stratagems, then it is time to apply the execution or follow-up stratagem:

- *Loot a burning house*. When an organization is racked with internal conflicts, disorganized, and confused; when the environment is plagued by outside elements such as crime and corruption; then the opponent will be weak and unable to prevail in conflict. Then you attack it without mercy and totally destroy it.[12]

An example of this approach is contained in a 2000 book called *Proteus*, sponsored by the US National Reconnaissance Office. The book has a hypothetical future scenario called "Militant Shangri-La."[13] In that scenario, an alliance of Asian and African nations executes a strategy supported by deception with the simple objective of keeping the United States and its allies on the edge of chaos—nothing more. Viewed from a Western perspective, the scenario posed an unclear threat.[14] Viewed from many Asian cultural perspectives, the strategy was both elegant and clear: Leave the opponent confused and uncertain, plagued with internal disagreements, unable to think or act effectively.

The deception approaches and objectives presented in the *Thirty-Six Stratagems* are worth noting as a different perspective for thinking about deception, for two reasons. First, it may be useful in some conflicts to make use of deception for no other purpose than to create uncertainty and confusion, even chaos. Second, it is important in countering deception to recognize that such deceptions may be used against your side.

The use of deception to destabilize has often been applied against criminal and terrorist groups and in international economic matters. The British have demonstrated some skill in this area, as the next case illustrates.

THE IRA EMBEZZLEMENT STING

In the early 1970s, the British were engaged in a bitter conflict with the Irish Republican Army (IRA) in Northern Ireland. The two sides conducted several deceptive operations against each other. One British operation was designed to aggravate an emerging split between older IRA leadership and a younger faction of leaders. The veteran leaders were willing to consider a cease-fire with the British; the younger faction opposed any cease-fire.

Called the Embezzlement Sting, the deception was carried out largely by a British unit called the Mobile Reconnaissance Force. It relied primarily on allegations made to the press by a British double agent named Louis Hammond, a Belfast Catholic who had joined the British Army's Royal Irish Rangers in 1970.

The Embezzlement Sting began when Hammond contacted two *Sunday Times* reporters claiming to be an IRA agent who had infiltrated the Mobile Reconnaissance Force on IRA orders. Hammond provided the reporters with what he identified as an internal IRA memorandum alleging that the IRA leadership was

embezzling funds. The bogus document was purportedly written by a senior IRA leader in Long Kesh Prison. It alleged that seven leaders of an IRA battalion had embezzled £150,000 of IRA funds. Hammond told the reporters that he had contacted them because the leaders of the battalion had betrayed the faith and he wanted to see them punished. To bolster his claim to be a double agent working against the British, he gave the journalists basic organizational information about the Mobile Reconnaissance Force—information that the British government later confirmed in a press conference.

Convinced that Hammond's story was genuine, the journalists published a series of articles in the *Sunday Times* describing IRA corruption. The first article was titled "IRA Provo Chiefs Milk £150,000 from Funds," and cited as its source a former intelligence officer of an IRA company.

Unfortunately for Hammond, the press article pointed directly to him. The IRA enforcement arm seized him and conducted an intense interrogation. Hammond confessed to working for the British and was then shot three times in the head and once in the stomach. The IRA gunmen then dropped Hammond's apparently dead body in a deserted alleyway. Hammond somehow survived, partially paralyzed and with the loss of one eye.[15]

The deception was facilitated by information provided through a separate channel. Whenever the IRA robbed a bank to fund its operations, the British made a press announcement claiming that an amount somewhat higher than the actual loss was taken. British television reporter Desmond Hamill wrote that frequently the effects of this deception could be seen immediately, "Very often the Army found that soon afterwards, sometimes even the next day, there would be a number of kneecappings. It was not good for IRA recruiting."[16]

Let's look at the basics of what makes a deception work.

BASIC PRINCIPLES

Four fundamental principles have been identified as essential to deception. They are truth, denial, deceit, and misdirection.[17] The first three principles allow the deceiver to present the target with desirable data while reducing or eliminating signals that the opponent needs to form accurate perceptions. The last principle leads the opponent to an attractive alternative that commands his or her attention—a plausible cover story. Let's look at each of them.

Truth

All deception works within the context of what is true. Truth establishes a foundation of perceptions and beliefs; these are then accepted by an opponent and can be exploited in deception. Often, supplying the opponent with real data establishes the credibility of future communications that the opponent then relies on.

Truth can be presented to an opponent or an ally without the intent to deceive. For example, an opponent might already misperceive reality, and truth is presented to correct that misperception. Such use of truth is especially relevant when an ally or opponent plans an undesired action based on misperception. In 1940 Josef Stalin refused to believe that Nazi Germany was preparing to invade the USSR. The British, aware of this, tried to provide the truth. Stalin, suspecting a British plot to draw the USSR into the conflict, dismissed the British effort as a deception. As described in the next section, Saddam Hussein missed an opportunity to correct the US-led coalition's misperception of reality prior to Desert Storm. The coalition believed that Iraq had weapons of mass destruction (WMD). Saddam knew better, but maintaining ambiguity about his weaponry helped him both internally and in dealings with neighboring states. In retrospect, the truth might have served him better.

In the Stalin example, truth was provided with no intent to deceive. But it is possible to correct an opponent's misperception as part of a deception plan. Historically it has been applied to establishing the credibility of double agents who can be used with greater effect later. For example, one of the most famous channels used by the United Kingdom during World War II was a double agent named Juan Pujol Garcia, known as *Garbo* to the MI5 and as *Arabel* to the German Abwehr. By the end of the war MI5 had provided Garbo with enough truth to relay to the Germans that he had managed to receive an Iron Cross from them. Truth in this case was used to ensure there was no German misperception about his credibility, so that when it came time to use him for D-Day and the supporting deception, Operation Quicksilver (described in Chapter 2), the Germans were conditioned to Garbo's reporting being credible.

Truth is often presented as part of *conditioning*: repeating a pattern of operations (signals, force movements, or similar activities). The idea is to deliberately condition the target to a pattern of friendly or reliably accurate behavior, with the objective of desensitizing opponents to indications of a planned action. One of the best examples of conditioning was applied by the Egyptians against the Israelis in 1973.

CONDITIONING: THE YOM KIPPUR WAR

In the third Arab-Israeli war of 1967, Egypt had lost the entire Sinai Peninsula to Israel. The Israelis had occupied the eastern bank of the Suez Canal and built defensive works that included a 60-foot-high sand wall along the canal. Egyptian president Anwar Sadat was determined to retake the Sinai, but he needed a way to overcome the Israeli defenses, and he desperately needed the advantage of surprise.

A key element in breaching the defenses was getting through the sand wall quickly. After trying conventional methods (explosives and bulldozers), Egyptian engineers found that a sand wall could be flattened quickly by a high-pressure stream of water. Egypt subsequently purchased several high-pressure water cannons from the United Kingdom and East Germany.

The Egyptians conducted an effective conditioning campaign to achieve surprise. They projected the image of an incompetent Egyptian military in the press. President Anwar Sadat openly criticized the performance of Soviet military advisors and of the military equipment that the Soviets were providing. The Soviets responded with press releases blaming Egypt's military for poorly maintaining the missile equipment. Israeli Defense Forces (IDF) regularly observed Egyptian soldiers fishing and walking along the banks of the Suez out of uniform. The Soviets leaked false reports to the foreign press that the Egyptian missile force was negligent in its maintenance of Soviet-supplied equipment.

The success of the attack ultimately depended on the intentional conditioning. Prior to the attack, Egyptian forces staged an extensive series of conditioning operations to desensitize Israeli intelligence. During the first nine months of 1973, the Egyptian army did the following:

- Conducted twenty separate mobilizations followed by demobilization, so that the pattern became routine.
- Practiced canal-crossing operations that were easily observed by the IDF. The Egyptians moved troops to the canal, built tank ramps, and created openings in the canal ramparts, followed each time by a subsequent withdrawal.
- Just prior to October 1973, moved successive brigades to the canal to train, then moved part of each unit back to its point of origin at night with headlights on, leaving the impression that the entire brigade had withdrawn.

At first, the Israelis responded to the conditioning efforts by putting their forces on alert. By October, they had accepted the Egyptian activities as routine rather than as an invasion threat. They were caught by surprise when, on October 6, the Egyptians crossed the canal, breached the Israeli defensive wall with their water cannons, and scored major offensive gains in the opening hours of the Yom Kippur War.

Denial

In many texts and training courses, deception is coupled with denial, and the two concepts are labeled denial and deception, or D&D. There are advantages to treating them separately. One can practice denial without conducting active deception. Denial often is used when no deception is intended; that is, the end objective is simply to deny knowledge. Intelligence collectors routinely must deal with this type of denial:

- Terrorist organizations and drug cartels routinely practice operational security to deny information about their activities to human intelligence (HUMINT) sources.

- Military test ranges schedule their activity to avoid imagery collection by satellites, aircraft, and unmanned aerial vehicles (UAVs).
- Diplomats and military commanders protect their important communications by encrypting them.
- Military units in the field conceal vehicles and artillery using camouflage.
- Governments developing chemical, biological, or nuclear weaponry conceal their operations by putting them in underground facilities.
- Aircraft and ship designers work to suppress the signatures of their platforms using stealth technologies.

This book does not deal with these types of denial, unless they are a part of deception. All deception involves some form of denial. One can deny without intent to deceive, but not the converse. You cannot practice deception without also practicing denial of some aspects of the truth that you want the opponent to be unaware of or disbelieve. Operational security (OPSEC) is just as important to a deception operation as it is to the real operation, if not more, depending on how much success is hinged on the deception plan.

In fact, all deception requires that you deny the opponent access to some parts of the truth. Denial conceals aspects of what is true, such as your real intentions and capabilities.

When used as a part of deception, denial is often part of *manipulation,* which requires mixing true and false information. You can, for example, use manipulation to create a perception of strength where you are in fact weak, or the opposite. The Iraqi government, under Saddam Hussein, did exactly that in a denial effort about WMD that extended over several decades.

IRAQI WMD PROGRAMS

During the 1980s, Iraq developed chemical weapons that they used against Iranian troops and civilians during the Iran-Iraq war, and against Iraqi Kurds after the war. The chemical weapons production plants were built with the assistance of several German firms, and German companies provided Iraq with over 1,000 tons of precursor chemicals that were subsequently used to produce mustard gas, tabun, and sarin.

In the same time frame, the Iraqis pursued a biological weapons program, drawing heavily on German expertise for facility construction and on the US Centers for Disease Control and Prevention for biological samples such as anthrax, botulism toxin, and West Nile virus. The Iraqis claimed that they needed the samples for medical research. By the time of the first Gulf War (1991; codenamed by

the United States as Operation Desert Storm), Iraq had weaponized (placed into munitions) thousands of liters of botulism toxin, anthrax, and aflatoxin.

Finally, Iraq pursued a nuclear weapons development program during the 1980s, relying on Italian assistance to develop several laboratories and the technologies needed for weapons production. No weapon had been produced by the time of Operation Desert Storm.

All three WMD programs relied heavily on denial—specifically, denying information about the purpose of acquiring plants, technology, materials, and know-how. In the aftermath of the first Gulf War, the Iraqis had to contend with UN-mandated inspection teams, but continued their programs at a reduced level. Their efforts were aimed at maintaining the capability to resume weapons development in the future, rather than to produce weapons—which the inspection teams would have detected.

To conceal the programs, the Iraqis relied on a detailed knowledge of the UN inspection teams' processes. Using that knowledge, they developed a plan to deceive the inspectors about their WMD efforts. The plan relied heavily on denial of imagery and specialized technical collection.[18] Specifically, they concealed WMD facilities inside existing buildings or placed them underground. Buildings designed for the same purpose were deliberately made to appear different from the exterior. They suppressed telltale emissions and hid power lines and water feeds to conceal the purpose of facilities. They moved WMD-related equipment at night.[19]

The Iraqi denial effort was unusual in that it was an attempt to project two diametrically opposite perceptions to two different targets. Against the UN, the United States, and its allies, the objective was to portray an image of weakness—the lack of WMD and WMD programs. Against Saddam Hussein's opponents in the Middle East—Iran and Israel in particular—the objective was to portray an image of strength: that Iraq possessed WMD and was prepared to use them.

Deceit

Successful deception normally requires the practice of deceit. Without deceit the target is only the victim of misperceptions due to denial, misinformation, and/or self-deception, which is not the same as deliberate deception.

Deceit, in turn, requires *fabrication*—presentation of the false as truth. One might disguise a chemical weapons plant as a pesticide producer, as Iraq did. One can disguise friendly forces as neutrals or even as members of the enemy's force,[20] a practice commonly known as a pseudo operation.

Pseudo operations (also known as "false flag" operations) are frequently employed to combat insurgencies. They make use of organized teams disguised as insurgents, employed to penetrate insurgent camps. Their mission may be to collect intelligence or to capture or kill insurgent leadership. The team members usually are drawn from existing paramilitary or military units, though they sometimes make use of captured insurgents who have been "turned."[21]

Pseudo operations teams have proved so successful over many decades that they are considered to be an essential component of any counterinsurgency campaign:

- One of the earliest reported pseudo operations was conducted in the Philippines from 1946 to 1955. This was the time of the Huk rebellion. Originally formed to fight the Japanese, the Huks subsequently began an insurrection against the Philippine government. In response, the Philippine Constabulary created a small unit called Force X. The basic idea was to make this specially trained force look and act like a Huk unit that could infiltrate into Huk territory, gather intelligence, and kill or capture Huk leaders. Force X members were dressed and equipped like Huks. They were trained to talk and act like Huks by four guerrillas who had been captured and "turned" to work for the government.[22]
- From 1948 to 1955, at about the same time as the Huk campaign, the British ran a pseudo operation against the Malayan Races Liberation Army, a predominately Chinese Communist insurgent group. The operation was so successful that counterinsurgency experts regard it as a model for such operations.
- From 1952 to 1960, the British fought a counterinsurgency campaign against a tribally based insurgent group called the Mau Mau in Kenya. The Special Branch used pseudo gangs to infiltrate and then kill or capture roving bands of terrorists. Initially, these pseudo gangs had been formed to gain intelligence but they subsequently evolved into combat groups. Led by European officers in black face makeup, they were able to get close enough to the enemy to kill or capture them. Such pseudo groups were composed of loyal Kikuyu, sometimes drawn from tribal police or regular constables, white officers, and "turned" Mau Mau. The latter were most important for lending credibility, since they knew the latest secret signs, finger snaps, and oaths that would convince the Mau Mau of their authenticity.
- Portugal ran a number of pseudo operations in its African colonies during the 1960s and 1970s. The units were organized in small bands of African troops, often including insurgents who had been captured and turned. Their primary role was to gather intelligence.
- During Rhodesia's war against insurgents (1964–1979), military authorities within the Rhodesian Security Forces realized the need for accurate and timely intelligence. A secret unit therefore was created in 1973 to acquire this intelligence. The unit was the Selous Scouts, comprising intelligence experts from the police and military, soldiers, and turned guerrillas. Eventually this small unit expanded to a formidable counterinsurgency force of close to 1,000. The Scout operations put heavy psychological pressure on insurgents; the insurgents

began to constantly fear deception, betrayal, and surprise attacks. Scouts would often stage elaborate scenarios in which black members of the unit would pretend to be guerrillas leading captured white soldiers into a guerrilla camp. At the last moment all weaponry would be returned to the apparent captives, allowing the Scouts to catch the entire camp by surprise.

- Since the 1990s, the Turkish government has relied on Special Teams, operated by the gendarmerie, and Special Action Teams, operated by the police, to counter a Kurdish Partiya Karkeren Kurdistan (PKK) insurgency. The teams were assigned to conduct high-risk "counterterrorist" actions against PKK cadres. In practice, the teams functioned as "death squads," identifying and killing PKK leaders.
- During the coalition operations in Afghanistan that started in 2001, special military task forces and police units were designed to collect human terrain intelligence in insurgent-held territories of Kandahar and Helmand. This included infiltrating hostile territories for shuras (meetings) with the locals to assess the extent of insurgent activity, as well as to generate a picture of the social networks of importance in the areas to contribute to the planning of future operations.
- In the fight against Daesh, Iraqis employed special force units to conduct long-range disruption operations against Daesh lines of communication, on some occasions using pseudo operations to infiltrate within striking range, or to draw the Daesh into striking range.

Pseudo operations teams have been successful for decades in collecting intelligence that could not otherwise be acquired. They have also had a record of success in offensive operations—disrupting insurgent leadership. The key to their success is disguise—that is, deceit.

In today's information age, pseudo operations have broadened to include the Internet and all its forms of communication. What began as simple deceit about identity in chat rooms and blogs has expanded with the rapid expansion of digital social networking possibilities. Social media such as Facebook, Twitter, and Instagram have become vibrant battlespaces for pseudo operations. Fake profiles, groups, and avatars operated relatively unhindered until several of the larger firms began applying policies that are more restrictive. However, social media today is an acknowledged battlespace domain that is inherently permissive for pseudo operations.

Misdirection

Misdirection requires manipulating the opponent's perceptions in a specific direction. You want to redirect the opponent away from the truth and toward a false perception. In operations, a feint—often called a *diversion*—is used to redirect

the adversary's attention away from where the real operation will occur. The idea is to draw the adversary away from an area or activity; to divert the target's attention from friendly assets; or to draw the target's attention to a particular time and place.

Misdirection incorporates the other three principles of deception. It includes truth, an essential part of all deception. Denial is necessary to protect information about the real situation. Deceit creates the false perception.

Misdirection depends on having a good understanding of an opponent's intelligence sources and processes. The Indian government used such knowledge in developing a strategic deception plan to cover its nuclear device test on May 11, 1998. On that date, the Indians conducted three underground nuclear tests at their Pokhran nuclear test site in the country's northwestern desert. The test came as a complete surprise to the US government. This operation has a number of features that illustrate superb use of the channels for providing deception, so it will be highlighted again in Chapter 6.

THE INDIAN NUCLEAR TEST

The nuclear test deception plan succeeded because the Indian government had an excellent understanding of the keys that US imagery analysts used to detect test preparations. The US government had succeeded in deterring an earlier plan by India to stage the tests. In December 1995, US reconnaissance satellites had observed test preparations at the Pokhran site, including the movement of vehicles and the deployment of testing equipment. The US ambassador to India showed the imagery to top Indian officials in a successful demarche[23] to persuade them not to test.[24]

Using the knowledge they gained from the demarche, the Indians were able to plan an elaborate deception campaign to conceal preparations for the 1998 tests. The campaign was many faceted, aimed at protecting the operation from HUMINT and IMINT.[25] The deception campaign had several elements, making it an excellent example of multi-INT deception. And it is a prime example of all four characteristics of a deception:

Truth. Their test location was known. Indians had to work within that truth, knowing that the United States was going to monitor that facility using imagery. Also, the deception was helped along by the US government's knowledge that India wanted to improve trade relations. US officials were therefore predisposed to believe that India would not provoke a crisis by testing a nuclear weapon.[26]

Denial. The effort was protected by extensive secrecy measures within the Indian government. Few knew of the plan; the decision to test was not disclosed even to senior cabinet ministers. Work was done at night, and heavy equipment was always returned to the same parking spot at dawn with no evidence that it had been moved. The shafts were dug under a netting of camouflage. When cables for sensors were laid, they were carefully covered with sand and native vegetation was replaced to conceal the digging.

Deceit. Piles of dug-out sand were shaped to mimic the natural wind-aligned and shaped dune forms in the desert area. All technical staff at the range wore

military fatigues, so that in satellite images they would appear as military personnel charged with maintenance of the test range. The Indian government issued a number of public statements just prior to the test, designed to reassure Washington that no nuclear test was contemplated. Indian diplomats also categorically told their US counterparts that "there would be no surprise testings." All scientists involved in the operation left in groups of two or three on the pretext of attending a seminar or a conference. Tickets were bought for some location other than Pokhran under false names, and after arriving at their destination the group would secretly leave for Pokhran. After finishing their part of the work, the group would go back, retracing their path. Then another group would leave for the range, employing similar means to do their part of the work on the bombs.

Misdirection. Just prior to the test, Indian leaders began an effort to focus US attention elsewhere. They were aware that the United States monitored ballistic missile tests at their Chandipur missile test range, more than a thousand miles from the Pokhran site. They consequently started preparations for what appeared to be a ballistic missile test at Chandipur. The Indians actually tested a Trishul surface-to-air missile (which was of relatively low intelligence interest to the United States), but they moved additional equipment into the test range so that the preparations appeared to be for a test of the Agni intermediate-range ballistic missile (which was of high intelligence interest).[27] As a result, US reconnaissance satellites reportedly were focused on the Chandipur site, with only minimal coverage of the nuclear test site at the time of the test.[28]

The following chapters of this book lay out the methodology for organizing a deception campaign. But first, it's worth taking a moment to understand the roles of operations and intelligence in conducting deception.

ROLES OF OPERATIONS AND INTELLIGENCE

Holt's commandments of deception described earlier were generated by lessons learned from World War II and were shaped by the organizational environment in which military deceptions were carried out by the Allies. It then should come as no surprise that those tenets are based on deceptions that required both an intelligence element and an operations element. The relationship between the two elements has often determined the success or failure of deception operations.

Deceptions are planned and carried out under the guidance of a decision maker to support a policy or military objective that can be strategic, operational, or tactical. In military terms, the decision maker is the commander; and his or her

organization for attaining the overall objective, referring back to our definition, is called *operations.*

All deception should be operations led and intelligence driven. It is a simple edict; but because of the contrasting organizational cultures of operations and intelligence, it has not always been employed effectively. However, the logic that operations should be driven by the best situational understanding possible is hard to deny, and is also the overarching principle behind deception operations. As stated earlier, deception operations are not carried out for the sake of deceiving. Rather, they are carried out in order to increase the chances of success for the real operation. With this in mind, the role of intelligence becomes no different from nondeception operations; intelligence must drive the deception operation by providing the best situational understanding possible.

Deceptions are usually planned by the operations component of an organization. And experience with conducting deceptions, dating back at least to World War II, have repeatedly demonstrated that the operations unit is best equipped to handle the deception mission. PSYOPS, in particular, is an operations function. Which leaves open the question: What then is the role of intelligence?

- Operations and policy bureaucracies—especially US bureaucracies—are sometimes criticized as being reluctant to incorporate deception in their planning. So an upfront role of intelligence is to provide opportunity analysis: identifying the potential for applying deception in planned operations.
- Once a decision is made to engage in deception, intelligence has several roles in ensuring that the deception succeeds. It must identify the types of deception that are most likely to succeed. It must identify likely reactions of the target for both successful and unsuccessful deception. It must select the channels for providing the deceptive information.
- In the context of driving deception operations, the intelligence element of the organization applies a *reflexive* methodology to understanding the adversary's process for obtaining and using intelligence—that is, in counterintelligence. It is reflexive in the sense that the intelligence arm observes and assesses *how the adversary observes and assesses,* and this information is used to create a situational understanding specifically for use with designing and executing supporting deception operations.

Also, in a few cases, the intelligence organization handles both the operations and intelligence roles. These cases include several types of covert actions and those missions in which the primary objective of the operation is intelligence collection.

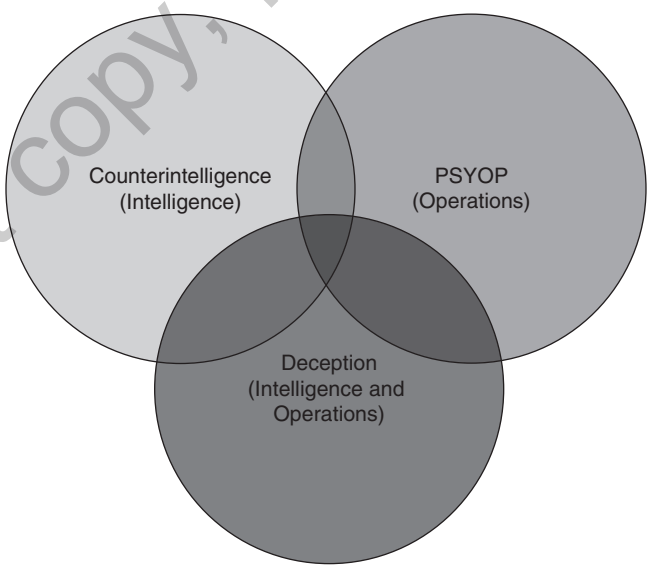
Finally, on the subject covered in Chapters 10 and 11—detecting and defeating deception—the answer is different. There, intelligence must take the lead. Deceptions inevitably are conducted against the sensory channels of an organization—primarily, but not exclusively, against intelligence channels. So the intelligence unit is the first line of defense in countering deception. Intelligence has the job of being aware of possible deception and ensuring that its customers are aware of it.

This focuses on two categories that both government and military leaders often don't consider: the opportunity to conduct deception against opponents, and the threat of deception operations conducted against them. It is an important capability as not only does it increase the chances of success for your operations, but it also decreases the chance of success of adversarial operations against your side.

Deception, counterintelligence, and psychological operations, as this chapter discusses, overlap each other. The traditional Venn diagram shown in Figure 1-3 illustrates that point. It also illustrates the point that operations and intelligence have specific roles to play in each area. Military organizations often have separate units responsible for deception and psychological operations, and there is a history of confusion and friction between the two.[29]

The next several chapters of this book lay out the methodology for organizing and managing deception and counterdeception. Chapters 2–9 cover how intelligence analysis should support deception operations, while Chapters 10 and 11 illustrate how intelligence analysis should drive counterdeception efforts.

FIGURE 1-3 ■ Venn Diagram of Overlapping Functions



NOTES

1. Barton Whaley, *Stratagem, Deception and Surprise in War* [reprint of 1969 edition] (Norwood, MA: Artech House Publishing, 2007), 104, tables 5.19 and 5.20.
2. Barton Whaley, "The Prevalence of Guile: Deception through Time and across Cultures and Disciplines," essay prepared for the Foreign Denial and Deception Committee, DNI, Washington, DC, February 2, 2007, https://cryptome.org/2014/08/prevalence-of-guile.pdf.
3. J. Bowyer Bell, "Toward a Theory of Deception," *International Journal of Intelligence and Counter-Intelligence* 16, no. 2 (2003): 244–79, doi:10.1080/08850600390198742.
4. D.C. Daniel and K. L. Herbig (Eds.), *Strategic Military Deception* (Elmsford, NY: Pergamon Press, 1982), 5, 6.
5. "Counterdeception," http://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=1334.
6. Frank Stech and Kristin Heckman, "Cyber Counterdeception: How to Detect Denial and Deception (D&D)," conference paper, MITRE Corporation, March 2014.
7. US Executive Order 12333, December 4, 1981. United States Intelligence Activities, Section 3.4(a). EO provisions found in 46 FR 59941, 3 CFR, 1981 Comp., p. 1.
8. Joint Publication (JP) 1-02, "Department of Defense Dictionary of Military and Associated Terms," November 8, 2010 (amended through February 15, 2016), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
9. Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Skyhorse Publishing, 2007), 54–61.
10. Sharon Begley, "The Stickiness of Misinformation," *Mindful*, October 5, 2015, https://www.mindful.org/the-stickiness-of-misinformation/.
11. Stefan H. Verstappen, *The Thirty-Six Strategies of Ancient China* (San Francisco: China Books & Periodicals, Inc., 1999).
12. Ibid.
13. Pamela H. Krause, *Proteus: Insights from 2020* (Washington, DC: The Copernicus Institute Press, 2000), D-i–D-xx.
14. Ibid., 83.
15. Mark L. Bowlin, "British Intelligence and the IRA: The Secret War in Northern Ireland, 1969–1988," US Naval Postgraduate School, September 1999, pp. 80–83, https://archive.org/stream/britishintellige00bowlpdf/britishintellige00bowl_djvu.txt.
16. Ibid.
17. Edward Waltz and Michael Bennett, *Counterdeception Principles and Applications for National Security* (Boston: Artech House, 2007).
18. Director of Central Intelligence George J. Tenet, speech at Georgetown University, February 5, 2004.
19. David Kay, "Denial and Deception: The Lessons of Iraq," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, ed. Roy Godson, Ernest R. May, and Gary Schmitt (Washington, DC: Brassey's, 1995), 120.
20. Scott Gerwehr and Russell W. Glenn, *The Art of Darkness: Deception and Urban Operations* (Santa Monica, CA: RAND, 1999), 21, http://www.rand.org/publications/MR/MR1132.
21. Lawrence E. Cline, "Pseudo Operations and Counterinsurgency: Lessons from Other Countries," US Army War College, June 2005, http://www.strategicstudiesinstitute.army.mil/pdffiles/pub607.pdf.

22. Ibid.
23. A demarche is a political or diplomatic step, such as a protest or diplomatic representation made to a foreign government.
24. Tim Weiner and James Risen, "Policy Makers, Diplomats, Intelligence Officers All Missed India's Intentions," *New York Times,* May 25, 1998.
25. Ibid.
26. Ibid.
27. "Strategic Deception at Pokhran Reported," *Delhi Indian Express* in English, May 15, 1998, 1.
28. Weiner and Risen, "Policy Makers, Diplomats, Intelligence Officers."
29. Holt, *The Deceivers: Allied Military Deception in the Second World War,* 54.