

Chapter 2

Bridging the Classical D&D and Cyber Security Domains

The reason why deception works is that it helps accomplish any or all of the following four security objectives:

- Attention—The attention of an adversary can be diverted from real assets toward bogus ones.
- Energy—The valuable time and energy of an adversary can be wasted on bogus targets.
- Uncertainty—Uncertainty can be created around the veracity of a discovered vulnerability.
- Analysis—A basis can be provided for real-time security analysis of adversary behavior.

Edward Amoroso (2011) *Cyber attacks: Protecting national infrastructure*. Burlington MA: Elsevier.

This chapter uses a traditional framework called the D&D methods matrix as a foundation for describing the basics of D&D in the physical world, extends the D&D matrix to cyber security, and then outlines a set of techniques for applying D&D in the cyber security context. These descriptions can be combined with the cyber-D&D TTP taxonomy in Appendix A to guide understanding of how D&D is used in the cyber domain. We examine the organizational requirements for planning and executing successful defensive cyber-D&D operations, introducing both physical and virtual D&D tactics relevant to each quadrant of the D&D methods matrix.

2.1 Classical D&D

Deception has proven useful in war, diplomacy, and politics (Bodmer et al. 2012; Rowe and Rothstein 2004; Whaley 2007a) for four general reasons. First, deception can divert an aggressor's attention from actual targets and resources, increasing the deception user's freedom of action. Second, deception may cause an opponent to adopt a course of action that works to the defender's advantage. Third, deception can help the defender gain the element of surprise over an adversary. Finally, deception may protect actual resources from destruction.

Deception is fundamentally psychological. We may think of deceptive behaviors by one actor (the deceiver) as influencing the behaviors of another (the target). Deceptions should have a concrete purpose: namely, the deceiver deceives the target

Table 2.1 D&D methods matrix

| Deception objects | D&D methods | |
|-------------------|--|--|
| | Deception: Mislead (M)-type methods revealing | Denial: Ambiguity (A)-type methods concealing |
| <i>Facts</i> | <i>Reveal Facts: NEFI</i> <ul style="list-style-type: none"> • Reveal true information to the target • Reveal true physical entities, events, or processes to the target | <i>Conceal Facts (Dissimulation): EEFI</i> <ul style="list-style-type: none"> • Conceal true information from the target • Conceal true physical entities, events, or processes from the target |
| <i>Fictions</i> | <i>Reveal Fictions (Simulation): EEDI</i> <ul style="list-style-type: none"> • Reveal to the target information known to be untrue • Reveal to the target physical entities, events, or processes known to be untrue | <i>Conceal Fictions: NDDI</i> <ul style="list-style-type: none"> • Conceal from the target information known to be untrue • Conceal from the target physical entities, events, or processes known to be untrue |

Source: Adapted from Bennett and Waltz (2007)

to cause the target to behave in a way that accrues advantages to the deceiver. This is the deceiver’s deception goal; the target’s actions are the deceiver’s desired deception effect. Thus, while the constituents of deception concepts and plans are psychological, the consequences of executing those plans are physical actions and reactions by the deceiver and the target.

Two essential deception methods create this causal relationship between psychological state and physical behavior. *Denial* represents deceiver behavior that actively prevents the target from perceiving information and stimuli; in other words, using hiding techniques that generate ambiguity in the target’s mind about what is and is not real. *Deception* denotes deceiver behavior that provides misleading information and stimuli to actively create and reinforce the target’s perceptions, cognitions, and beliefs. This generates a mistaken certainty in the target’s mind about what is and is not real, making the target certain, confident, and ready to act—but wrong.

The objects underlying these D&D methods, as shown in Table 2.1, are facts and fictions that are either revealed via deception methods or concealed via denial methods. These facts and fictions can be information or physical entities. The term *non-essential friendly information* (NEFI) refers to facts that the deceiver reveals to the target. Factual information that the defender cyber-D&D team must protect is termed *essential elements of friendly information* (EEFI), while the key fictions that the defender cyber-D&D team must reveal to the target of the deception are termed *essential elements of deception information* (EEDI). Finally, fictions that the deceiver must conceal from the target are referred to as *non-discloseable deception information* (NDDI).

Classical D&D literature focuses on the shaded quadrants the table—that is, on simulation to reveal fictions and dissimulation to conceal facts. The other two quadrants—revealing facts and concealing fictions—are also important to a successful D&D campaign. As with simulations and dissimulations, an effective D&D campaign results in the target perceiving and accepting the revealed facts, while failing to perceive the deceiver’s concealed fictions.

2.1.1 *Reveal Facts*

The upper left quadrant of the table shows deception (also called Mislead or M-type methods) for revealing selected facts—the NEFI. Given that these facts are verifiable, the deceiver must carefully edit and tailor them so that they can be leveraged to craft and reinforce the deception story presented to the target. The target should believe and accept the factual information, physical entities, events, and processes that the deceiver reveals, but these must be carefully engineered to lead the target away from perceiving and understanding the whole truth. The deceiver can also influence the target to disbelieve or reject the facts by discrediting them: revealing facts about the truth to the target in such a way that the target will discredit those facts and disbelieve the truth.

2.1.2 *Reveal Fictions—Simulation*

The shaded lower left quadrant shows revealing fictions—the EEDI—also known as simulation. This is an essential basis for creating false perceptions. In order for revealed fictions to deceive the target successfully, the fictions must “rest on a firm foundation of previous truth” (Masterman 2000). That is, the target must believe at least some of the revealed facts shown in the upper left quadrant when those facts are necessary to support the defender’s simulation.

In the present context, simulation means the invention, revelation, and leveraging of information, physical entities, events, or processes that the deceiver knows to be untrue. Informational fictions can include disinformation (i.e., the revelation of false or misleading information), paltering (i.e., revealing facts that apparently support the reality of a fiction¹), and lying (i.e., the deliberate transfer of known untruths). To increase the believability of disinformation, paltering, and lies, the deceiver can disseminate this information via a communication channel that also disseminates facts, such as press releases, white papers, or media outlets containing NEFI. In addition, the deceiver creates physical fictions and reveals them to the target via a variety of methods, such as decoys, diversions (e.g., feints, demonstrations), forgeries, doubles, and dummies of equipment or personnel. Psychological states (e.g., mood, emotion) can be simulated during interpersonal communications via the presentation of false facial expressions, body language, and vocal cues.

¹ *Paltering* is “less than lying ... the widespread practice of fudging, twisting, shading, bending, stretching, slanting, exaggerating, distorting, whitewashing, and selective reporting. Such deceptive practices are occasionally designated by the uncommon word *paltering*.” Frederick Schauer and Richard Zeckhauser. “Paltering” in Brooke Harrington, ed. *Deception: From Ancient Empires to Internet Dating*. Stanford, CA: Stanford University Press, 2009, pp. 38–54.

A previously classified espionage case, recently adapted into the movie *Argo*,² provides a good example of how to reveal fictions that rest on a firm foundation of truth. A small team of CIA specialists developed a plan for exfiltrating six U.S. State Department employees who had fled during the 1979 takeover of the U.S. Embassy in Tehran, Iran, and were “houseguests” at the Canadian Embassy in Tehran. The cover story for the exfiltration was that the employees belonged to an advance scouting party for the production of a Hollywood science-fiction movie, *Argo*. To ensure the credibility of the cover story, the team intertwined operational deception elements with genuine Hollywood business processes: the number and role of individuals involved in an advance scouting party, physical offices with functional telephones for the fake production company, studio press coverage in the most popular Hollywood trade papers, the use of a real movie script as a prop, a fake production portfolio, and customary “Hollywood-style” attire for the houseguests and their CIA escorts, to name a few. The operation was a D&D success; the six houseguests were exfiltrated from Iran, while in the United States the fake production company had received 26 new scripts (including one from Steven Spielberg) prior to being dismantled several weeks after the exfiltration.

2.1.3 *Conceal Facts—Dissimulation*

The shaded upper right quadrant of Table 2.1 presents denial, also called Ambiguity or A-type methods, for concealing the EEFI. Here the deceiver conceals the truth, thereby denying the target. Dissimulation, or hiding the real, involves the concealment of true information, physical entities, events, or processes from the target. Just as revealing facts forms an essential basis for revealing fictions, concealing fictions is an essential basis for concealing facts. For example, a double agent should reveal many facts as well as those few fictions the double agent’s controllers want to dupe the adversary into believing. Equally important, the double agent should hint at hidden and concealed fictions as if they were hidden facts. An agent who “knows and reveals all” is too good to be true; thus, to be believable, the double agent must hide both some facts *and* some fictions, so that the adversary must work to obtain them, presumably through the other deception channels managed by the double agent’s controlling organization. Luring the adversary to expend effort on piecing together these hidden fictions is one method the deceiver can use to “sell” the deception fiction to the adversary.

²*Argo* is a 2012 film distributed by Warner Bros. Pictures. This case was also adapted into a television movie in 1981, *Escape from Iran: The Canadian Caper*, directed by Lamont Johnson. Anthony (Tony) Mendez, the CIA officer involved in this case, has written about his experiences: “A Classic Case of Deception,” *Studies in Intelligence*, Winter 1999/2000, p. 1–16; and *Argo: How the CIA and Hollywood Pulled off the Most Audacious Rescue in History*, 2012 co-authored with Matt Baglio and published by Viking Adult.

Winston Churchill stated, “In time of war, when truth is so precious, it must be attended by a bodyguard of lies.” The truth can also be concealed via secrecy, which denies the target access to the deceiver’s most crucial truths, such as genuine intentions, capabilities, time lines, and of course, the D&D plan itself. Information can be kept secret via technological means such as steganography, cryptography, and honeypots, nets, tokens, clients that hide the real cyber environment. Physical entities, events, and processes can be kept secret via methods such as camouflage, concealment, and secure facilities. As with simulation, the presentation of false facial expressions, body language, and vocal cues during interpersonal communications can prevent the target from recognizing true psychological states

As an example of concealment, in 1962 the Soviets had to devise a cover story for their plan to emplace ballistic missiles, medium-range bombers, and a division of mechanized infantry in Cuba. Operations security (OPSEC) minimized the number of top civilian and military officials planning the operation; however, to execute the operation, these planners had to mislead both Soviet and foreign citizens about the destination of the equipment and forces. As a code name for the operation, the Soviet General Staff used ANADYR—the name of a river flowing into the Bering Sea, the name of the capital of the Chukotsky Autonomous District, and the name of a bomber base in that region. To support the code name illusion, the forces deployed to Cuba were told only that they were going to a cold region, and were supplied with winter equipment and ‘costumes’ including skis, felt boots, and fleece-lined parkas.³ Personnel who needed climate specifics, such as missile engineers, were told that they were taking intercontinental ballistic missiles to a site on Novaya Zemlya, a large island in the Arctic where nuclear weapons had historically been tested.⁴ The ANADYR denial was so successful that it fooled even senior Soviet officers sent to Cuba. One general asked General Anatoli Gribkov, a senior member of the Soviet General Staff involved in planning the operation, why winter equipment and clothing had been provided. Gribkov replied, “It’s called ANADYR for a reason. We could have given away the game if we had put any tropical clothing in your kits.”⁵

2.1.4 Conceal Fictions

The lower right quadrant of Table 2.1 shows concealing fictions, or NDDI: that is, hiding from the target information, physical entities, events, or processes that the deceiver knows to be untrue. This is the least intuitive quadrant in the matrix. To illustrate the concept of concealing fictions, Bennett and Waltz (2007) use the example of statements by “spin doctors,” which notoriously bear multiple

³Gribkov, A. I., Smith, W. Y., & Friendly, A. (1994). *Operation ANADYR: U.S. and Soviet generals recount the Cuban missile crisis*. Chicago: Edition q, p. 15.

⁴Fursenko, A. A., & Naftali, T. J. (1997). *One hell of a gamble: Khrushchev, Castro, and Kennedy, 1958–1964*. New York: Norton, p. 191.

⁵Gribkov and Smith (1994) p. 15.

interpretations. Such statements enable the spin doctors to use strategies to either avoid revealing that they are lying or to avoid revealing that their actions are a hoax. In the former strategy, the spin doctor denies a fiction by suppressing a lie, and in the latter, by curbing information that might expose a sham. The deceiver benefits by concealing from the target particular known fictions that support the deceiver's D&D plan. The concealment should arouse the target's interest and focus attention on piecing together these missing elements of deceiver information. For example, the deceiver may have a double agent sending deception information to the target (e.g., a concocted mixture of real but innocuous facts and deception—facts and fictions supporting the deceiver's deception) while hiding from the target the EEFI that the agent actually works for the deceiver. The agent's communications should hint at but conceal other fictions consistent with the deceiver's deception, motivating the target to collect and fill in those missing pieces. As the target works to assemble the jigsaw puzzles, the deceiver feeds the target's collection through other controlled deception channels. The pieces slowly fall into place, and the target assembles the picture the deception planners intended the target to perceive and believe.

One real-world example of concealing fictions comes from early twentieth century warfare. Colonel G. F. R. Henderson served as the British chief of intelligence for an assignment during the South African War (Holt 2007). During this assignment, Field Marshal Lord Roberts was to lift the siege of Kimberly using a traditional feint. Henderson's assignment was to deceive the Boers by keeping their attention on the location of Roberts's feint, and denying them the location of Roberts's planned attack. To mystify and mislead the enemy, Henderson sent out fictitious orders in the open (i.e., simulation), but then canceled them in cipher (i.e., concealing a fiction). Henderson's D&D succeeded: the Boers' attention stayed focused on the feint, they missed Roberts's movements, and the siege was lifted.

Likewise, during the Second World War, the British understood camouflage to mean not just hiding the real but showing the fake in such a way that its "fakeness" was concealed.⁶ The American 23rd Headquarters Special Troops⁷ followed suit and created faulty camouflage – that is, camouflage designed to draw attention to fake objects. They hid the fake by making it seem real enough that it was worth hiding. By doing so they sought to persuade the enemy to make decisions by altering the adversary's perception: things were not as they appeared.

For example, in the summer of 1944 the 23rd were assigned their first large-scale operation, ELEPHANT, in a town called St. Lô while the Allies massed their forces for the Battle of Normandy. Although Operation ELEPHANT was a disaster for the 23rd, the unit learned many valuable lessons.⁸ If they camouflaged equipment such

⁶Gerard, P. (2002) *Secret Soldiers: The Story of World War II's Heroic Army of Deception*. New York: Penguin Group.

⁷The 23rd Headquarters Special Troops was a group of U.S. Army artists and designers engaged in a variety of D&D activities against the Germans in World War II.

⁸One month after the operation, headquarters staff concluded that "The results of this operation are uncertain...However, no movement of forces to counter the move of the Armored division was made by the enemy and captured documents indicated that the unit which was simulated was still

as tanks too well, the enemy would never know it was there. If the camouflage was too conspicuous, the enemy would suspect it was a sham. The 23rd discovered a compromise: they mimicked the mistakes real tankers made when pulling into a “harbor” for the night. Such mistakes included leaving a length of the barrel sticking out of the net, leaving a gas can exposed to catch the morning light and flash a telltale glint to an enemy spotter, draping the net too loosely so that the shape of the tank stood out, and leaving a gap in the foliage surrounding the “tank.”

2.1.5 Deception Dynamics

As this chapter has shown so far, denial and deception go hand in hand. The deceiver uses denial to prevent the detection of EEFI by *hiding the real*, and deception to induce misperception by using EEDI to *show the false*.⁹ The deceiver assembles an illusion by creating a ruse to hide *and* to show. As shown in the D&D methods matrix, the deceiver also has to *hide the false*, that is, the NDDI, to protect the D&D plan, and *show the real*, that is, the NEFI, to enhance the D&D cover story. Deception is a very dynamic process and planners will benefit from the interplay of techniques from more than one quadrant in a deception operation. Table 2.2 builds on the D&D methods matrix in Table 2.1 to present some D&D techniques at a high level.

Several historical examples illustrate these dynamics of deception. For example, during Operation ELSENBORN, the 23rd was to convince the enemy that the 4th Infantry Division was at Elsenborn Barracks, a Belgian army rest camp just behind the front lines between Eupen and Malmedy.¹⁰ The 23rd handled all of the 4th’s actual radio traffic for one week prior to the operation while the 4th was still holding a sector of the front. When the 4th Infantry moved out to the Hürtgen Forest as reinforcements, radiomen from the 23rd continued radio communications using fake messages indicating that the 4th was slated for rest and recreation (R&R) at Elsenborn. The 23rd had coordinated with the signal operators of the 9th Infantry, which had been at Elsenborn the week before this operation, to stage a 3-day radio exercise. When the 23rd arrived at Elsenborn, they continued broadcasting as part of the supposed “exercise.” This provided them an excuse to stay on the air and

considered to be the actual Armored division in its original location several days after the conclusion of the operation.” Despite doing just about everything wrong, the 23rd had gotten lucky. One week after the operation, Lt. Fox wrote a memo to Col. Reeder, the commanding officer of the 23rd, and his colonels about the lessons to be learned: “...The successful practice of military deception by the 23rd Hqs requires the proper amount of SHOWMANSHIP and ARMY PROCEDURE. [emphasis in original]” To Fox, the 23rd had a “...lack of appreciation of the Fine Art of the theatre.” Gerard, P. (2002) *Secret Soldiers: The Story of World War II’s Heroic Army of Deception*. New York: Penguin Group, pp. 153–155.

⁹As shown in the D&D methods matrix, the deceiver also has to *hide the false*, that is, the NDDI, to protect the D&D plan, and *show the real*, that is, the NEFI, to enhance the D&D cover story.

¹⁰Gerard, P. (2002) *Secret Soldiers: The Story of World War II’s Heroic Army of Deception*. New York: Penguin Group.

Table 2.2 D&D methods matrix with examples

| | | D&D Methods | | |
|-------------------|--|--|--|--|
| Deception objects | Deception: Misleading-type methods revealing | Denial: Ambiguity-type methods concealing | | |
| <i>Facts</i> | <p><i>Reveal Facts (NEFI) Information:</i></p> <ul style="list-style-type: none"> • Release true information that benefits the deceiver by being disbelieved or rejected by the target (double bluff ruse) • Discredit true information so the target disbelieves it, e.g., make the information too obvious (double play ruse) • Coat-trail trivial facts to divert the target from larger truths • Create negative spin (take the blame for a lesser crime; exhibit contrition to conceal lack of true remorse) • Engage in paltering | <p><i>Conceal Facts (Dissimulation): EEFI Information:</i></p> <ul style="list-style-type: none"> • Implement secrecy and security programs (INFOSEC, SIGSEC, OPSEC) • Withhold information to create a false or misleading impression | | |
| | <p><i>Physical:</i></p> <ul style="list-style-type: none"> • Display real facilities or equipment (to condition the target, or to build a source’s credibility with target) • Display duplicates • Display distractors, misleading clues, coat-trailing evidence • Engage in feints, demonstrations (real) • Disseminate positive evidence to distract or mislead the target | <p><i>Physical:</i></p> <ul style="list-style-type: none"> • Deploy camouflage, concealment, signal and signature reduction; stealth designs; disguises; secure facilities • Dazzle to hinder perception (fine print) • Engage in nonverbal deceit • Engage in “Red Flagging” by hiding in plain sight (blending) • Hide negative evidence (dissimulated) by offering alternative or simulated evidence | | |
| <i>Fictions</i> | <p><i>Reveal Fictions (Simulation): EEDI Information:</i></p> <ul style="list-style-type: none"> • Disseminate disinformation; lie; provide information known to be untrue • Dazzle (to overwhelm understanding) | <p><i>Conceal Fictions: NDDI Information:</i></p> <ul style="list-style-type: none"> • Suppress a lie • Apply positive spin | | |
| | <p><i>Physical:</i></p> <ul style="list-style-type: none"> • Deploy decoys; mimics; mock-ups; dummies; forgeries, doubles; disguises • Engage in diversions; feints; demonstrations • Nonverbal deceit • Positive evidence (simulated) to mislead from real negative evidence (faking a crime scene) | <p><i>Physical:</i></p> <ul style="list-style-type: none"> • Hide a sham • Cover up falsehoods to avoid arousing target’s suspicion • Disseminate negative evidence (simulated) to conceal positive evidence (cleansing a crime scene) | | |

Source: Adapted from Bennett and Waltz (2007)

communicate misinformation when they would have normally been silent given the 4th’s R&R. The 23rd thus executed a fake within a fake.

On many occasions the 23rd used the magician’s “pull:” the trick of getting the audience to look at the flourishing right hand (i.e., showing the false) while the canny

left hand performed the trick (i.e., hiding the real). They would demonstrate Allied buildup and strength where in fact none existed. Instead, the 23rd was masquerading as forces that had moved under cover and silence to another critical attack location. While the Germans were busy watching and sometimes engaging the 23rd's flourishing right hand, they were lulled into complacency where the uncanny left revealed an Allied attack with forces that were believed to be located elsewhere.

Juan Pujol, a World War II double agent codenamed GARBO by the British, has been called the “most successful double agent ever.”¹¹ GARBO not only simulated and dissimulated, he also revealed facts and concealed fictions. When the Second World War broke out, Pujol decided he wanted to spy for the British. ‘I must do something,’ he told himself. ‘Something practical; I must make my contribution towards the good of humanity.’ Hitler was ‘a psychopath,’ Pujol concluded, and so he must support the Allies. ‘I wanted to work for them, to supply them with confidential information which would be of interest to the Allied cause, politically or militarily.’ In January 1941, the 29-year-old Catalan approached the British Embassy in Madrid, with an offer to spy against the Germans. The embassy firmly turned Pujol away.

Pujol next tried the Germans, pretending to be a keen fascist willing to spy against the British—in the hope that, once recruited by the Nazis, he could then betray them. The Germans told him they were ‘extremely busy’; then, mostly to get rid of him, the Germans said that they might use him if he could get to Britain via Lisbon. Pujol’s German intelligence case officer, Kühlenthal, duly equipped Pujol with secret ink, cash, and the codename ‘Agent Arabel.’ Once in Lisbon, Pujol again contacted the British, and again was turned away. Pujol was in a dilemma, since he needed to send intelligence to the Germans as soon as possible. On 19 July 1941, he sent a telegram to Kühlenthal announcing his safe arrival in Britain [*Reveal fiction*] although he was still in Portugal [*Conceal fact*]. Denied the opportunity to gather real intelligence for either side, Pujol decided to invent it, with the help of the Lisbon public library, second-hand books, and whatever he could glean from newsreels. He remained in Lisbon for 9 months, inventing what he thought his Nazi spymasters wanted to hear [*Reveal fact; Reveal fiction*].

In Lisbon Pujol continued to pester the British to recruit him. Despite producing evidence to show he was now in the employ of the Germans, he was repeatedly turned down. Pujol approached the American naval attaché in Lisbon, who contacted his opposite number in the British Embassy, who duly, but very slowly, sent a report to London. Finally, British MI6 realized that the German agent sending the bogus messages to the Germans must be Juan Pujol García, the Spaniard who had repeatedly approached them in Lisbon.

Now working for British MI5, GARBO sent important, real information to his German handlers, carefully timing his messages to arrive too late to be useful to the Germans [*Reveal facts*]. Pujol’s British controllers wondered how the Germans

¹¹ Macintyre, B. (2012) *Double Cross: The true story of the D-Day spies*. Great Britain: Bloomsbury Publishing. Also see: Andrew, C. M. (2009) *Defend the realm: the authorized history of MI5*. Alfred A. Knopf : New York.; Pujol, J. and N. West (1986) *GARBO*. Grafton Books: London.; McCamley, N.J. (2003) *Secret Underground Cities: An account of some of Britain’s subterranean defence, factory and storage sites in the Second World War*. Leo Cooper: London.

could fail to see their agents as people ‘who seldom or never say anything untrue, but who equally never say anything which is new.’ In German eyes, GARBO’s failure to supply high-grade information in a timely way was not his fault [*Conceal fact*] but theirs; and the more often he tried [*Reveal fact*] and failed [*Conceal fact*], the more they loved him.

Another interesting twist in GARBO’s career is a classic case of concealing fictions. Roger Hesketh,¹² who during the war served as a member of the deception section of Supreme Headquarters, Allied Expeditionary Force, provided an additional insight into the complexities of intricate story simulations: the value of creating interesting but flexible story elements that might have utility in future, as-yet-undetermined deception episodes. Though special means and other deception operations, the Allies built up various cover story contexts for future use. For GARBO, the deception planners concocted a mystery: strange secret goings-on at the famous caves of Chislehurst, well known to the Germans from as long ago as World War I. The British fed bits of this mystery (but not the full story) to GARBO, who used them to tease and tantalize his German deception target. GARBO and his notional subagents and nets conveyed:

... a rather mysterious story concerning the caves at Chislehurst ... For many months GARBO had been hinting at strange developments in these caves [One of GARBO’s subagents worked in the Chislehurst caves and another was a guard at the caves] which were in some way connected to the coming invasion [*Conceal fiction*]...The Germans took GARBO’s reports about the Chislehurst caves seriously, even if their interest was sometimes tinged with incredulity. When the invasion came, a suitable occasion for exploiting the story did not present itself and ... the Germans were ultimately informed that the caves had been used for storing arms for the *Maquis* [French underground]. [*classic blow-off for cooling out the mark*]

GARBO conveyed to the Germans pieces of a mystery for which even he did not have the whole story. Plan *Bodega* was an

... entirely fictitious development, in preparation for the opening of the second front of a huge underground depot with a network of underground tunnels or the distribution of arms and ammunition to airfields and anti-aircraft defenses in the London area. ...the build-up of this project (Plan *Bodega*) might later be exploited for deception purposes in conjunction with Operation *Overlord* but in fact no use was made of it.¹³

2.2 Translating D&D to Cyber Security

Classical D&D techniques can be extended to cyber security. Some “translation” of D&D techniques from the physical to the virtual world may be necessary. Table 2.3, which further builds on the cyber-D&D methods matrix, suggests some analogies by outlining a high-level set of cyber-D&D techniques (combinations of two or

¹²Hesketh, R. (2000) *FORTITUDE: The D-Day Deception Campaign*. Overlook: New York.

¹³Howard, M. (1995) *Strategic Deception in the Second World War*. Norton: New York.

Table 2.3 D&D methods matrix with Cyber-D&D techniques

| Deception objects | D&D methods | |
|-------------------|---|--|
| | Deception: M-type methods: Revealing | Denial: A-type methods: Concealing |
| <i>Facts</i> | <p><i>Reveal Facts: NEFI</i></p> <ul style="list-style-type: none"> • Publish true network information • Allow disclosure of real files • Reveal technical deception capabilities • Reveal misleading compromise details • Selectively remediate intrusion | <p><i>Conceal Facts (Dissimulation): EEFI</i></p> <ul style="list-style-type: none"> • Deny access to system resource • Hide software using stealth methods • Reroute network traffic • Silently intercept network traffic |
| <i>Fictions</i> | <p><i>Reveal Fictions (Simulation): EEDI</i></p> <ul style="list-style-type: none"> • Misrepresent intent of software • Modify network traffic • Expose fictional systems • Allow disclosure of fictional information | <p><i>Conceal Fictions: NDDI</i></p> <ul style="list-style-type: none"> • Hide simulated information on honeypots • Keep deceptive security operations a secret • Allow partial enumeration of fictional files |

Source: Adapted from Bennett and Waltz (2007)

more tactics), organized according to whether they are facts or fictions, and whether they are revealed via deception methods or concealed via denial methods. This “packaging” of tactics can be an indicator of a sophisticated deception capability for CD purposes.

Figures 2.1 and 2.2 are Venn diagrams of the offensive and defensive tactics, techniques, and procedures (TTPs), respectively. The categorization reflects whether a particular TTP generally reveals or conceals facts or fictions, or some combination thereof. These diagrams illustrate that the advantage in using D&D clearly lies on the side of the attacker, given the sheer number of offensive D&D TTPs. Also, as compared to the methods reflected in Table 2.2, the majority of the offensive cyber-D&D TTPs shown in Fig. 2.1 fall along the simulation-dissimulation axis. This suggests potential opportunity space for crafting new TTPs that reveal facts and conceal fictions along the other axis. Appendix A contains further analysis and presents a full cyber-D&D taxonomy: a comprehensive list of all these offensive and defensive cyber-D&D TTPs,¹⁴ categorized according to the D&D methods matrix.

These figures do not show all possible cyber-D&D TTPs, partly because those TTPs do not have naming conventions that make them readily identifiable, possibly due to the immaturity of the cyber-D&D field.¹⁵ Furthermore, given the ever-evolving

¹⁴The offensive TTP entries include examples of how they would be used by a financially motivated actor as well as by an espionage-motivated actor. The defensive TTP entries include examples of how they would be used against a financially motivated actor and a targeted espionage actor.

¹⁵As shown in Stech et al.’s 2011 paper “Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space,” the absence of a clear set of conventional terminology suggests the immaturity of that domain.

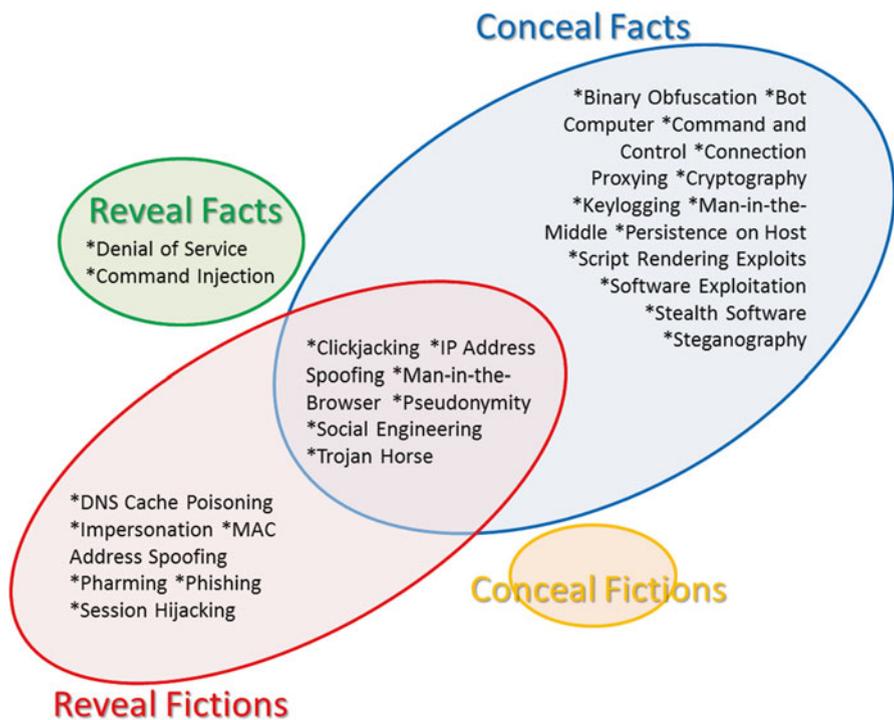


Fig. 2.1 Offensive Cyber-D&D tactics

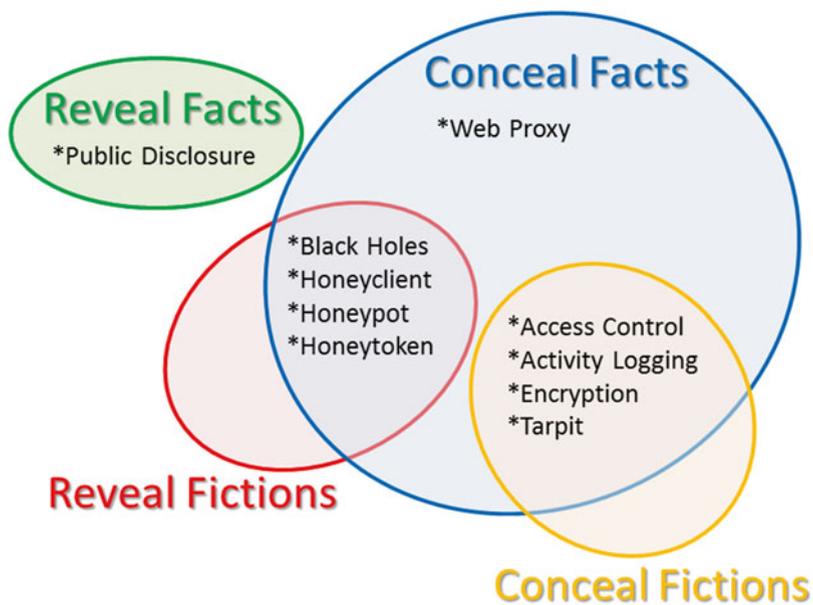


Fig. 2.2 Defensive Cyber-D&D tactics

nature of computer networking, technology, and software, these TTPs necessarily evolve as well, with some becoming obsolete, some being adapted, and new ones being created. As such, these diagrams have a moving window of validity.

2.3 Using D&D in Cyber Security

In *Defensive Computer-Security Deception Operations*, Yuill¹⁶ asserts that cyber-D&D complements other cyber security methods:

After years of research and development, computer security remains an error-prone task and, in some respects, perhaps a losing battle. Computer security's chronic problems call for wholly new approaches. Deception works in a fundamentally different way than conventional security. Conventional security tends to work directly with the hacker's actions, e.g., to prevent them or to detect them. Deception manipulates the hacker's thinking to make him act in a way that is advantageous to the defender. Being fundamentally different, deception can be strong where conventional security is weak.

This section, organized by the four quadrants of the D&D methods matrix, elaborates on each of the high-level cyber-D&D techniques presented in Table 2.3. Each subsection suggests some potential implementations of D&D for cyber security, particularly incident response in the context of a deception operation.

2.3.1 *Reveal Facts*

Revealing facts to an opponent can be an effective way of detecting malicious actors. By **publishing a limited amount of true information**¹⁷ about their network, personnel, and missions, defenders can selectively attract attention or reduce attacker sensitivity to defensive network surveillance (Bennett and Waltz 2007). For example, defender deception tactics may include revealing employee attendance at upcoming conferences via their company blog or public mailing list. Malicious actors who employ targeted social engineering may adapt their tactics to the new context; for example, a message to an employee could purport to follow up on a session at the conference. The resulting information would become a marker to distinguish spear phishing attempts from untargeted malicious email.

Defenders may show their hand by **revealing their deception capabilities** in a way that makes their opponent disbelieve information gleaned from past intrusions. The defender could build a virtual honeypot environment nearly identical to the organization's actual environment, with usernames, email accounts, software registration, and server names configured to accurately reflect real configurations. If they

¹⁶James J. Yuill. *Defensive Computer-Security Deception Operations: Processes, Principles and Techniques*. Dissertation North Carolina State University, Raleigh NC, 2006, p. 200.

¹⁷Phrases shown in boldface are techniques originally presented in Table 2.3.

discover the duplication, malicious actors may doubt the authenticity of the data found in both previous and future intrusions, and become wary when interacting with supposedly compromised systems. Sophisticated planners integrate such deception capability signatures into their production networks to create further doubt in the event of a true compromise.

Malicious actors intrude into networks to gain access to sensitive information. One channel of disclosure is to launch an actor's implant inside a virtual honeypot. By **seeding the deception environment with real documents** that have been publicly released or previously compromised, or that contain non-sensitive information, the environment presents a sense of realism with limited risk to the target organization. If a phishing email launched the intrusion attempt, the original message and its presence in the targeted user account also act as confirming evidence of the adversary's success.

Planners must consider deception along several dimensions of impact. For example, publicity about an intrusion can damage an organization's public image and stature. With the right emphasis, an organization can **reveal this apparent weakness to emphasize a capable security program** in order to discourage further intrusion attempts. Misleading phrasing such as "unverified claims of network compromise are being investigated as a matter of routine by teams of internal security specialists" adds a degree of urgency to intruder operations. A successful disclosure encourages the intruders to reveal operational methods and support, such as implants, tools for subsequent compromise and enumeration, command and control (C2) hop points that the intruders might hold back if they believed they had more time to execute. This tactic is most effective when the deceivers understand the adversary's open source collection abilities.

In a similar vein, but more direct, **overt—but incomplete—remediation actions can accelerate an intruder's pace of operations**. During incident response, network defenders isolate and sanitize infected machines in a coordinated fashion.¹⁸ After initial containment, security personnel could remove a subset of intruder access while leaving some portions intact to allow malicious actors to discover the remediation activities. The tactic encourages adversaries to reveal more TTPs in their efforts to reestablish footholds in the post-"remediation" environment.

2.3.2 *Conceal Facts*

Either side can conceal facts to gain advantages during a computer network intrusion. Ordinary access control policies—a formalization of **resource denial**—and their implementation form the long-standing first line of cyber defense. Firewalls, service proxies, email filtering, role-based account assignment, and protocol

¹⁸ Jim Aldridge, Targeted Intrusion Remediation: Lessons From The Front Lines, Blackhat 2012, <https://www.blackhat.com/usa/bh-us-12-briefings.html#Aldridge>

encryption all deny resources to legitimate network users in the event their systems become compromised.

Adversaries may create a **denial of service (DoS) condition** through traffic floods or excessive failed access attempts as partial fulfillment of their mission. More insidious intrusions can render physical resources inaccessible through compromise of industrial control systems.

At a lower level, malware can intercept anomaly detection and other warning messages, stopping them from reaching the resources that process them. For example, **stealth methods can conceal the presence of malware** from security software by altering kernel data structures to prevent display in process, service, and device listings. Malicious code commonly obfuscates its control and dataflow dependencies to inhibit analysis once the implants have been discovered. Encryption or steganography may conceal adversarial command traffic to infected machines, preventing defenders from realizing that their information is being stolen.

Defenders also benefit from **software stealth techniques to hide security software services**, such as host activity sensors, antivirus, and data loss prevention clients. Other defensive denial tactics include encrypting documents to prevent exposure of intellectual property, and disallowing commonly abused system commands such as ‘dsquery’ or ‘netcat’ to prevent use by malicious actors. While this does not prevent actors from transferring equivalent tools to victims, it forces the attackers to take more risks in the process.

Proxies and anonymization services **reroute traffic to conceal the source address of a machine**. For example, the Tor network routes encrypted data through a series of machines. As a defense, many organizations simply block the public list of last-hop machines. Threat actors often use more *ad hoc* proxy networks for their C2, combining compromised systems with distributed virtual hosting services. Routing traffic through other machines in this manner makes it more difficult for network defenders to effectively filter and investigate malicious activity, particularly when hosts span multiple owners and jurisdictions

Rerouting adversarial traffic forms the foundation of *active defense* technologies. Defenses such as “sinkholing” route known bad Domain Name System (DNS) requests to non-existent Internet Protocol (IP) addresses or perhaps to internal sensors. More aggressive responses would route malicious actors to honeypot systems.¹⁹ Defenders may also choose to deter malicious actors by performing system shutdown or logoff actions for contrived reasons. This straightforward response may be part of a plan to disable malicious access if the attackers appear close to discovering that they are in a ruse environment. As the responses become more active, such tactics more closely align with *revealing fictions* in place of *concealing facts*.

Organizations that gate access to the Internet with proxies have a structure for vetting requests to external resources. Conventional systems deny access to untrusted hosts, but active defenders may permit such connections at an enhanced level of monitoring while denying essential resources to the suspect host. Some enterprises attempt

¹⁹See Chap. 5 for an illustration.

man-in-the-middle intercepts on encrypted connections to web sites by issuing their own trusted certificates. While this practice may raise privacy concerns, its pay-off enables detection of malware that uses the Secure Sockets Layer/Transport Layer Security (SSL/TLS) for communication—especially significant given the recent events involving the Heartbleed bug in supposedly secure systems.

2.3.3 *Reveal Fictions*

Trend Micro reports that malware most commonly infects machines as a result of users' installing software from the Internet or opening malicious email attachments.²⁰ This finding underlies the defensive practices of network security operations centers that make large investments in Internet content and email filtering. Most users would not knowingly compromise their organization's network,²¹ so malicious actors commonly lie to gain and preserve footholds in protected networks. Attackers can **misrepresent the intent of software and media in order to install malware**, for example by using fake antivirus programs,²² Trojanized software in third-party application markets,²³ and pornography sites.²⁴ Phishing offers another instance of overt fiction intended to mislead users into opening documents that install malware. Malicious actors abuse webpage layout engines to simulate user interface elements that can trick victims into interacting with malicious content. In one notable example from 2012, the Flame malware used a control panel interface that resembles an innocuous web administration panel, presumably to evade discovery by suspicious system administrators.²⁵

While defenders can reroute local DNS queries to deny access to malicious resources, one powerful adversarial tactic is to **poison DNS responses with attacker-controlled IP addresses**. After corrupting the records, the adversary creates a mock-up of a website or service that users expect to see in an effort to exploit their trust in the destination. Common goals include collecting user login credentials or pushing content that exploits vulnerabilities in visiting systems to establish a malicious implant.

In addition to hijacking domains, malicious operators can passively monitor traffic to compromise poorly implemented authentication systems.²⁶ This **session hijacking** exploits the stateless nature of the Hypertext Transfer Protocol (HTTP)

²⁰ <https://blog.trendmicro.com/trendlabs-security-intelligence/most-abused-infection-vector/>

²¹ http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

²² http://static.usenix.org/events/leet10/tech/full_papers/Rajab.pdf

²³ http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2013.pdf

²⁴ <http://www.bluecoat.com/documents/download/2014-mobile-malware-report>

²⁵ https://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers

²⁶ <http://codebutler.com/firesheep/>

by targeting the authentication cookies with which websites create sessions. After obtaining the authentication cookies, the attacker may replay them to impersonate an already-authenticated legitimate user.

Defender missions also benefit from presenting selected fictions. Malware, like other software, comes from a code base that its developers alter over time to suit their ends. Zeus, Poison Ivy and Gh0st RAT are well known public examples of remote access tools (appropriately known as RATs), and threat specialists (e.g., Mandiant 2013) enumerated dozens more. Once the defender organization bins the threats posed by the RATs, it may analyze the C2 protocols that the tools use for the implants of their high-priority campaigns. This analysis informs the development of protocol parsers, modifiers, and defender-controlled compatible implants. Together, these technologies can **intercept and modify network traffic** to give attackers a deceptive view of supposedly compromised systems. Emulated implants provide basic capabilities, such as file listing and remote shell execution, but disallow hard-to-emulate operations such as file uploading or screenshot capture. Unsupported commands can silently fail with a network timeout, require an interminable amount of time to complete, or appear to be blocked by policy.

More generally, because the primary purpose of a honeypot is to be vulnerable to compromise, defenders can use *honeypots* to deceive attempted intruders by presenting a wholly fake system. Honeypots fall into two categories: low-interaction honeypots that passively respond to malicious actors and high-interaction honeypots that require care and feeding for best results. Like emulated implants, low-interaction honeypots are shallow simulations of systems that respond plausibly to attempted compromise. A honeypot can simulate a service on a node; for example, Kippo acts as a Secure Shell (SSH) listener that collects brute force attacks and allows basic interactions with a lightweight file system.²⁷ Instead of hosting a real SSH server on port 23, a honeypot system would listen with Kippo, giving intruders an apparent opportunity to attack.

Another approach, known as tarpitting, simulates nodes on IP addresses that are not allocated in the production network. LaBrea, named after the famous tar pits in Los Angeles, was one proposed solution to the flash infection of 339,000 machines over 14 h caused by the Code Red worm (Haig 2002). The concept was to slow Code Red's scanning by presenting fictional machines in unallocated IP space that permitted the worm to establish Transmission Control Protocol (TCP) connections on all ports but subsequently timed out. This approach tied up the logic of Code Red as it waited for TCP responses rather than infecting new machines. LaBrea's timeout response had a minimal impact on enterprise operations because production traffic only touched legitimate machines, not the unallocated IP space.

Benefits of low-interaction honeypots include flexible deployment and the ability to gather information on malicious actors without the risk of compromising real machines. These honeypots have proven effective against relatively unsophisticated actors who rely on automated exploitation scripts but do not possess the technical ability to discover the deceptive environment. Integrating low-interaction honeypots

²⁷<https://code.google.com/p/kippo/>

into production networks by re-allocating unused IP space gives an organization visibility into attempts to map and exploit hosts on their internal network.

By contrast, high-interaction honeypots offer a deeper level of simulation than the minimally implemented services intended to thwart automated tools. These honeypots seek to deceive a live adversary by presenting a range of services and vulnerable machines. Successful deployment enables network defenders to collect data on how malicious actors behave in the latter phases of an intrusion. For example, *honeyd* generalizes LaBrea's approach by providing deeper responses to traffic destined for unallocated IPs (Provos and Holz 2007). At the node level, *honeyd* simulates responses to network traffic at layer 3 and above by handing off interaction to both local and remote processes—for instance, a real HTTP web server on port 80, or a listener such as Kippo on port 23. Besides responding to local network traffic, *honeyd* simulates traversal of arbitrary network topologies with virtual routers and connections to other, non-local networks.

High-interaction honeypots require regular monitoring by network defenders, who should add artifacts over time to take advantage of changing adversary interests. Typically, defenders create plausible documents, emails, and user activity prior to launching a high-interaction honeypot. These so-called *honeytokens* documents need not be fully backstopped, but should be interesting to the adversary in question. Tracking honeytokens allows an organization to discover leaks or adversary distribution methods. As an example, if a malicious actor steals a fake list of email addresses during a deception operation, those emails may be subject to bulk public disclosure or be re-used to send phishing messages to the fake users. Tools such as *pastycake*²⁸ or Google Alerts can monitor popular distribution sites to detect public exposure of the “stolen” documents, and organizations can perform additional monitoring on the “stolen” email accounts.

The creation of fictional information, or honeytokens, such as fake user accounts, requires the defending organization to add them to its phone directory, email system, and employee domain. Organizations must treat any attempt to interact with these accounts as very suspicious, and investigate them immediately. On a production network, these accounts can be added to groups without dangerous privileges and have logon scripts that prevent abuse. As a proactive measure, organizations can use decoy email addresses for high-value targets such as executives or system administrators. Email addresses disclosed to external parties can be monitored for phishing attempts without affecting internal communications.

Finally, exposing a past deception to malicious actors may deter future intrusion attempts, depending on the attacker's perception of the organization's overall defensive posture. It may also cause actors to question the validity of any information taken from the organization's network in the past. The APT develops indicators of deception and uses them to guide subsequent engagements. A defender who integrates such features into production environments can make a real success seem like a honeypot to the adversary, potentially resulting in a loss of interest.

²⁸<https://github.com/9b/pastycake>

2.3.4 *Conceal Fictions*

Most denial technologies can become vulnerable through misconfiguration, failure to patch, or exercise of a capability for which the adversary has demonstrated counter-measures. Defenders should tune the weakening strategy to the adversary's standard operating procedures (SOPs), so that the attacker can discover the "hidden" resource. Possibilities include selecting moderate to weak passwords for accounts or encrypted media, using exploitable webpages to obtain fictional resources (e.g., the page may be subject to SQL [Structured Query Language] injection vulnerabilities), and deploying outdated access control technologies to protect internal resources. As adversaries work through more "clues," these denial methods should collectively guide the hostile actors to focus their efforts on resources of limited value.

Planting fictional but inaccessible documents can entice interaction by malicious actors without the risk of disclosure. For example, a document purporting to be a planned business acquisition may contain a random collection of bytes disguised as an encrypted file. Using such files on an internal network can attract both malicious insiders and external attackers who have compromised perimeter security. Discoverable metadata about files can enhance the perceived value of such files, for instance by indicating that the files were authored by executives or well-known engineers.

Defenders may also craft documents written in highly technical or domain-specific language. Tools used by malicious actors often have no way of reading documents directly due to concerns about detection and file size. Enticing titles and timestamps may be enough to prompt a malicious actor to upload these files to their server, thereby providing valuable information on their collection requirements and infrastructure. By implanting watermarks in these files, a defender can also prove compromise of intellectual property.

Proprietors of secured and protected credit card databases might choose to include a sizable percentage of fictional "fluorescent" identities and account numbers designed not to work, but to report the attempted use as fraud; (for physical transactions) report the use and summon security; or (for cyber transactions) honor the transaction, while reporting the use and installing covert tracking and beaconing software (e.g., via a clickable purchase link) on the user's machine. All of these fictitious accounts would be concealed and protected and would only work against the attacker if obtained illegally.

Defenders usually wish to hide deception to manipulate their opponents. To this end, they often **configure honeypots to return tampered values in response to system commands** such as 'uptime' or 'systeminfo' to enhance plausibility and conceal the deceptive nature of the environment. To create a fake honeypot, defenders construct a real system that appears to have the known characteristics of a honeypot system.²⁹ To reinforce the façade, systems can appear as poorly concealed pieces of low-interaction emulation software when queried in certain ways.

²⁹Neil C. Rowe. "Deception in defense of computer systems from cyber-attack," in A. Colarik and L. Janczewski eds. *Cyber War and Cyber Terrorism*. Hershey, PA: The Idea Group, 2007.

At the policy level, an organization may choose to **hide the existence of deception capabilities** with an OPSEC plan (Bennett and Waltz 2007). In contrast to publicly disclosing deception efforts, the OPSEC approach leaves malicious actors confident in their ability to compromise an organization. Security operations are sensitive as a matter of course, but deception operations are also vulnerable to counter-exploitation if disclosed without prior knowledge of deception planners.

2.4 D&D Operations

Planning and executing successful D&D operations requires a wide range of capabilities. They include an understanding of the theoretical and technical elements of cyber-D&D and an organizational capacity to plan, prepare, support, coordinate, control, and execute complex deception plans.³⁰ This D&D organizational element should be closely tied to the overall IT operations, cyber security and operational security elements, and threat intelligence efforts.

The deception cover story created and executed by the D&D team, as well as the EEDI, may be entirely truthful. For example, the story might represent a realistic course of action (COA) that the deceiver does not intend to execute. The D&D team could use plans for the rejected COA as the basis for the deception cover story. In this case, much of the deceiver's preparation for the selected COA will be identical or similar to actions that would be taken to implement the rejected COA. This ambiguity, together with an effective deception cover story, will cause the deception target to misconstrue preparations for the real COA as being consistent with the COA of the cover story.

For this approach to succeed, the deceiver organization must perform several critical tasks. The deceiver must induce failure in the target's perception or interpretation of environmental information and thus influence subsequent target actions. This means that the deceiver must either hide the "deception core" (EEFI) from the target, or simulate fictitious properties for EEFI (that is, create EEDI) to mislead the target. Then, the deceiver must develop a theory of the target's mind and behavior, including how the target seeks, scans, and accesses information in the environment; how the target categorizes and interprets this information; and how the target takes action, including further information sampling in the environment. Figure 2.3a, b show the tasks supporting the defender D&D team's deception goals through the use of D&D tactics.

The D&D team can use denial tactics to disrupt the target's perceptions of EEFI and NDDI (see Tables 2.4 and 2.5, respectively), while the deceiver's deception tactics disrupt the target's cognitive interpretation and understanding of the deceiver's true activities. The deceiver would convey the EEDI and NEFI so that the target misunderstands the deceiver's actions (see Tables 2.6 and 2.7, respectively). In other words, the deceiver's denial (ambiguity-type) tactics interfere with the target's

³⁰ See Chap. 7 for an analysis of organizational capability for cyber-D&D.

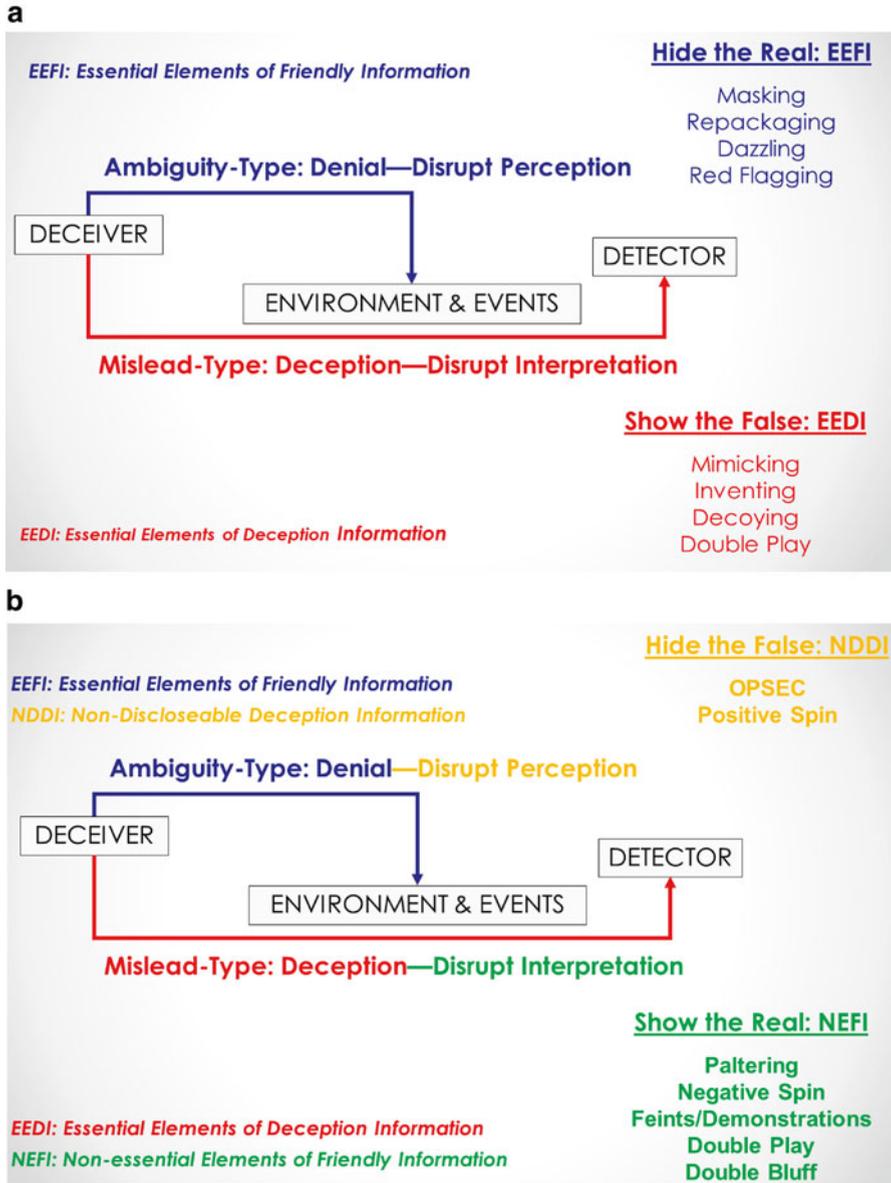


Fig. 2.3 (a) D&D types and tactics: EEFI and EEDI (b) D&D types and tactics: NDDI and NEFI

perceptions, while the deceiver’s deception (mislead-type) tactics distort the target’s interpretation of data.

The *deception goal* should always be to induce the target to take actions that will confer advantages on the defender. Those actions constitute the *deception effect*.

Table 2.4 Denial tactics (A-type: hiding the real: EEFI)

| | |
|--------------|--|
| Masking | Conceal key characteristics of one entity while matching those of another <i>Using pseudonyms, Steganography</i> |
| Repackaging | Add and change labels or characteristics <i>Showing different web site content based on geo-IP location, Cryptography, Footprinting</i> |
| Dazzling | Obscure characteristics, add overpowering alternative characteristics <i>Software obfuscation</i> |
| Red Flagging | Obvious display of key characteristics, “waving a red flag” <i>Disposable email addresses</i> |

Table 2.5 Denial tactics (A-type: hiding the false: NDDI)

| | |
|---------------|---|
| OPSEC | Employ an operational security program for protecting secrets <i>Keep deceptive security operations a secret</i> |
| Positive Spin | Exaggerate positive elements to suppress negative falsehoods <i>Allow partial enumeration of fictional files</i> |

Table 2.6 Deception tactics (M-type: showing the false: EEDI)

| | |
|-------------|---|
| Mimicking | Copy characteristics; create fictitious entities <i>Fake Twitter accounts, Clickjacking, DNS Cache Poisoning</i> |
| Inventing | Create new characteristics; synthesize realistic indicators <i>Phishing email</i> |
| Decoying | Create alternative characteristics by forming immaterial entities or indicators <i>Honeypots</i> |
| Double Play | Maintain characteristics; show the real in such a suspicious manner as to cast doubt on it <i>Evercookies</i> |

Table 2.7 Deception tactics (M-Type: Showing the Real: NEFI)

| | |
|-----------------------|---|
| Paltering | Reveal facts that are misleading <i>Reveal misleading compromise details</i> |
| Negative Spin | Reveal minor facts so as to conceal major facts <i>Allow disclosure of select real files</i> |
| Feints/Demonstrations | Attempt to divert adversary attention toward one area in order to weaken attention to another area <i>Reveal select technical deception capabilities</i> |
| Double Play | Discredit true information so target disbelieves it <i>Selectively remediate intrusion</i> |
| Double Bluff | Release true information that benefits the deceiver by being disbelieved or rejected <i>Publish true network information</i> |

Table 2.8 Deception team information and actions, and intended target reactions

| Deception team information & actions (friendly) | Deception target intended reactions (adversary) |
|--|---|
| <i>Attract adversary’s attention to EEDI and cover story information and actions</i> | Take notice of the EEDI and cover story |
| <i>Hold adversary’s interest in EEDI and cover story information and actions</i> | Assess EEDI and cover story as relevant and monitor them |
| <i>Confirm adversary’s expectations and experiences regarding EEDI and cover story</i> | Assess revealed elements of EEDI and cover story as congruent with expectations |
| <i>Modify adversary’s expectations and experiences regarding EEFI</i> | Fail to take notice of EEFI hidden elements |

The D&D team must have the knowledge and ability to develop D&D operations that protect the EEFI and the NDDI while contributing to the broader organization’s goals and objectives by creating EEDI, NEFI, and cover stories³¹ that can be expected to produce the deception effect. Table 2.8 summarizes the D&D team’s information and actions and the intended reactions by the target.

The D&D team actions and information shown in the table presuppose that the deceiver has considerable information and intelligence about the target: how the target reacts to information and actions, what appeals to the target’s interests, the target’s expectations, and the target’s blind spots.³² The more intelligence the deceiver has about the target, the better the defender cyber-D&D team can develop EEDI and cover stories to mislead and deceive the target.

The information elements of the EEDI and the principal and secondary deception cover stories may include simulation (manipulation) or dissimulation (concealment) of several information dimensions:

- Actions:
 - Intention (What is the activity?)
 - Place/target (Where is the activity?)
 - Payoff (Why is the activity happening?)
 - Style/Method (How is the activity carried out?)
- Actors:
 - Players (Who is engaged in the activity?)
 - Strength (How many people are involved?)

³¹The deception planner should prepare several cover stories that will be supported throughout a specific deception campaign. By sustaining more than one viable cover story, the deceivers have a fallback story if the principal cover story is compromised, or if the deception target does not seem to react to the principal cover story.

³²For ideas on identifying and exploiting blind spots in deception planning, see Van Hecke, M. L. (2007) *Blind spots: Why smart people do dumb things*. Prometheus Books: Amherst NY; and Sternberg, R. ed. (2002) *Why Smart People Can Be So Stupid*. Yale University Press: New Haven, CT.

- Stages:
 - Channel (By what means is the activity conducted?)
 - Pattern (In what way/order is the activity conducted?)
 - Time (When is the activity conducted?)

The deception cover stories must present believable information and actions covering all of these elements, just as a screenplay must address as many as possible of the audience's questions about and interests in the action and actors on the screen. Not all of these information elements need be false. In fact, the best deception cover stories make the greatest possible use of true information and activities, and present just enough EEDI and false or misleading information to cause the target to form the wrong picture of events, while making the target actors fully confident they understand the picture accurately.

Whaley (2007c) described a ten-step process for planning, preparing, and executing deception operations. These steps for creating effective deceptions (modified slightly to include the EEFI, EEDI, NEFI, NDDI terminology introduced in Table 2.1) are:

1. Use Blue³³ organizational goals to develop the deception goal, deception effect, and deception success criteria.
2. Collect intelligence on the Red adversary and estimate Red's preconceptions, expectations, and reactions.
3. Use real Blue COAs (that will not be executed) to develop the deception cover story: design the deception effect as Red's natural reaction to the Blue COA cover story.
4. Perform thorough Blue information value analysis (with cyber security and OPSEC partners): identify what must be hidden from Red (EEFI) and what must be revealed to Red (EEDI).
5. Plan denial actions to hide real information that provides Red with unique, unambiguous signatures of Blue plans and actions (EEFI), as well denial actions to hide the fictions that support Blue's D&D plan; detail the necessary steps to mask, repackage, dazzle, or red flag all EEFI and NDDI.
6. Plan to show the false: detail the necessary steps to use real information and actions (NEFI) and to mimic, invent, decoy, or double play the EEDI and actions (virtual and other) for the deception cover stories.
7. Develop the deception plan: organize the necessary D&D means and resources needed to support the cyber-D&D plan.
8. Manage the cyber deception operations: build the matrix of NEFI, EEDI, EEFI, NDDI, and deception cover stories to manage, coordinate, and control deception actions, information, and operations in conjunction with overall cyber operations, cyber security, and OPSEC partners.

³³Whaley uses "Blue" to refer to the friendly, deceiver organization and "Red" to refer to the adversary target.

9. Monitor the deception operations: observe Red behaviors, actions, and reactions (virtual and otherwise); estimate the effectiveness of the deception cover stories; coordinate D&D actions with all ongoing virtual and other operations.
10. Reinforce deception operation successes: redirect unsuccessful deception operations by using concealment, simulations, or other channels to reinforce, sustain, and maintain the deception cover story; ensure the deception operations produce the planned deception effect; and redirect deception operations that are not producing the expected reactions and effects on the Red deception target.

It is important to note that steps 1–6 of the deception process comprise *deception planning*, step 7 is *deception preparation*, and steps 8–10 are *deception execution*. The deceiver achieves the best results by planning deceptions well in advance of the operations they are intended to protect; deception preparations and execution should occur while other operational planning continues. Then, by the time the real operation commences, the deceiver has planted and supported the deception cover story, which manipulates the target to misperceive and misconstrue the ongoing events, erroneously confident that it comprehends the deceiver's operation.



<http://www.springer.com/978-3-319-25131-8>

Cyber Denial, Deception and Counter Deception
A Framework for Supporting Active Cyber Defense
Heckman, K.E.; Stech, F.J.; Thomas, R.K.; Schmoker, B.;
Tsow, A.W.
2015, XV, 251 p. 30 illus., 28 illus. in color., Hardcover
ISBN: 978-3-319-25131-8