13th ICCRTS

"C2 for Complex Endeavors"

Operationalizing Social Engineering for Offensive Cyber Operations

Topic(s): Cognitive and Social Issues, Organizational Issues

Authors:

Bryan Skarda, Major, USAF (STUDENT)
Dr. Robert F. Mills
Lt Col Todd McDonald, PhD
Dr. Dennis Strouble

Contact:
Dr. Robert Mills
AFIT/ENG
2950 Hobson Way:
Air Force Institute of Technology
Wright-Patterson AFB, OH 45433-7765

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Operationalizing Social Engineering for Offensive Cyber Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Institute of Technology,AFIT/ENG,2950 Hobson Way,Wright-Patterson AFB,OH,45433-7765**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

Operationalizing Social Engineering for Offensive Cyber Operations

All warfare is based on deception
–Sun Tzu

Abstract

Social Engineering describes a class of computer hacking that targets the user of the system rather than the hardware or software. It is a proven and viable vector that includes techniques like phishing, pharming, and persuasion. The Air Force uses social engineering to a limited extent as a validation tool when assessing the security stance of a unit or installation. Units like the 57th Information Aggressor Squadron based at Nellis Air Force Base routinely employ social engineering techniques as they perform their mission. However, this is the only employment of social engineering currently evidenced in the Air Force inventory.

Based on the widespread success of these techniques in the civilian world, anecdotal evidence gleaned from both interviews and literature reviews places their effectiveness at or near 100 percent [14], social engineering seems a logical fit for an organization looking for the next best weapon. Additionally, social engineering has the rare and enviable trait of being extremely low cost, both in terms of training and execution. These factors inspired this research along with the perceived lack of interest given the topic inside the Air Force. Further investigation into social engineering evidenced little academic attention devoted to the topic which seemed disproportionate to the technique's reported level of effectiveness. With the material presented here, we aim to demonstrate that social engineering as a concept already exists in current doctrine and that, with a little adaptation, a widely practiced methodology exists that can be used to structure social engineering attacks and evaluation.

Social engineering directly impacts both friendly and adversary decision cycles, making it a direct player in any discussion about command and control. It can provide information or misinformation depending on the application. Even a failed social engineering attempt, if recognized by an adversary, can undermine trust and confidence in the validity of uncompromised data. However, its blend of technical with the psychological makes it difficult to categorize. Perhaps the best fit would be in the realm of decision support systems where the traditional concept of a data warehouse with appropriate filtering technology is expanded to include the human element.

This paper takes the stance that social engineering is an under appreciated tool that is available for use. As the Air Force steps into the cyber arena with the creation of a new Cyber Command [8], the cultivation and employment of all possible methods to achieve supremacy in that domain must necessarily achieve primary concern. Answering the implicit challenge in this statement, we explore social engineering. We start with a discussion on the background of social engineering, reviewing the exploits of Kevin Mitnick who is perhaps the most famous hacker in the United States and who made many of his biggest breakthroughs using social engineering techniques. We will also discuss the essence of social engineering, persuasion, and review some research being done at Stanford University by Dr. Fogg on a new area of study called Captology. We will explore Influence Operations, a term we believe implicity points to social engineering. Chapter Three goes further into the realm of Influence Operations, drawing explicit parallels between concepts widely accepted in the Air Force and concepts familiar to the social engineer. Finally, Chapter Four takes social engineering and introduces a conceptual framework to apply it to the real world, a practical method for planning operations and performing Battle Damage Assessments (BDA) afterwards. This application and evaluation model is the real contribution of the research effort as it provides a starting point for the Air Force

to begin formulating an implementation plan for offensive social engineering.

Introduction

Based on the widespread success of social engineering techniques in the civilian world, anecdotal evidence gleaned from both interviews and literature reviews places their effectiveness at or near 100 percent [14], social engineering seems a logical fit for an organization looking for the next best weapon. Additionally, social engineering has the rare and enviable trait of being extremely low cost, both in terms of training and execution. These factors inspired this research along with the perceived lack of interest inside the Air Force. Further investigation into social engineering evidenced little academic attention devoted to the topic which seemed disproportionate to the technique's reported level of effectiveness. With the material presented here, we aim to demonstrate that social engineering as a concept already exists in current doctrine and that, with a little adaptation, a widely practiced methodology exists that can be used to structure social engineering attacks and evaluation.

Social engineering directly impacts both friendly and adversary decision cycles, making it a direct player in any discussion about command and control. It can provide information or misinformation depending on the application. Even a failed social engineering attempt, if recognized by an adversary, can undermine trust and confidence in the validity of uncompromised data. However, its blend of technical with the psychological makes it difficult to categorize. Perhaps the best fit would be in the realm of decision support systems where the traditional concept of a data warehouse with appropriate filtering technology is expanded to include the human element.

Background

Social Engineering and Persuasion

Dr. Brad Sagarin is an associate professor in the Psychology Department at Northern Illinois University and focuses his research in the area of persuasion. In fact, he is quoted several times by Kevin Mitnick in his book *The Art of Intrusion*. Sagarin's work in the area of compliance, persuading individuals to say yes to a proposition, yielded a set of influence principles that induce compliance [2]. These six principles are reciprocity, social validation, commitment/consitency, friendship/liking, scarcity, and authority. Interestingly, we see many of these same principles mentioned by Kevin Mitnick as methods available to a social engineer. Table 1 below displays these principles of influence as well as some descriptive characteristics.

Sagarin also discusses methods for employing or leveraging the influence principles, many of which again are very similar to techniques discussed by Kevin Mitnick. While Sagarin's research does not focus on social engineering, the social engineer makes use of these persuasion pressure points to gain the information desired.

Captology

Dr. B.J. Fogg, a professor at Stanford University, introduced Captology in 1996 and continues to be the expert this field of study. Captology is an acronym based on the term "computers as persuasive technology" [5]. Fogg does not view this persuasive relationship in terms of attackers and targets, but rather as a benign social interaction. However, given the focus of our research and the obvious applicability of Fogg's research, attention to his work is warranted. Fogg describes three main roles that computers play when they act in a persuasive role, one of which is Computers as Tools.

Table 1: Sagarin's Influence Principles

Principle of Influence	Description
Reciprocity	Returning a form of behavior that is displayed Creating a feeling of need to repay Sometimes manifests as feeling of banking a future favor
Social Validation	Correct action is determined by societal actions Actions are appropriate and good if others do them What others do carries even more value than what they think
Commitment/Consistency	Commitment equated with intellectual strength Once committed, subjects stay the course even if it is negative Able to request actions consistent with committed stance
Friendship/Liking	More favorably inclined to meet the needs of those we like Attractiveness is a huge advantage Similarity to subject indices liking and compliance
Scarcity	Opportunities are more valuable when scarce True even if opportunity has little value by itself Also invoked through feeling of losing a freedom (choice)
Authority	Legal authority is extremely influential Merits to possess authority not as important as position Seen as in control of rewards and punishments

As described by Fogg, *computers as tools* has seven subcategories:

- *Reduction Technology* provides the target with a range of options while ensuring that the option of most benefit is also the easiest to follow. Alternatively, it may also manifest by taking a complex task and eliminating the majority of the obstacles until all that remains are a handful of simple tasks leading to the desired outcome.
- *Tunneling Technology* presents a "predetermined sequence of actions or events" which ultimately lead to a desired outcome. This approach is effective as it generally simplifies task completion from the point of view of the subject. Additionally, there is a tendency for most people to stay with a course of action they have committed to, regardless of contrary evidence placed in their path.
- *Tailoring Technology* provides information that is specific to the user, giving the illusion of complete customization. Spear phishing, the practice of sending phishing e-mails containing personal information about the target [4], is an example of this tool. A subset is tailoring for context which makes the information specific to the intended recipient but also delivers that information at a time or place when the recipient is most likely to find it useful.
- *Suggestion Technology* presents desired behaviors to the user at the most opportune moment. An example from the military is psychological operations (PSYOP) that come after a particularly devastating battle. Suggestion Technologies often build on motivations or behaviors already in existence, presenting the suggestion at a time when it will have the most impact.
- *Self-Monitoring Technology* relies on the user to watch his or her own behavior and adjust performance accordingly. This tool assumes a certain amount of desire to change on the part of the target and so

offers limited benefit from an offensive military standpoint.

- *Surveillance Technology* monitors the behavior of the subject but is purposefully conspicuous. The subject is persuaded by knowledge that their actions are being watched and so they change those behaviors accordingly. Covert surveillance has a role in the military realm but when the stated goal is to persuade the target to change behaviors, the surveillance must be overt and noticeable.
- *Conditioning Technology* rewards the subject for displaying favorable behaviors. In relation to Captology, it does not include punishing for incorrect behavior. It is a time sensitive technology with the time schedule being driven by the subject as the positive reinforcement must appear within a limited window in order to have the desired effect. Interestingly, adding an element of randomness to the reward is also beneficial; that is the reward for the displaying the desired behavior always appears quickly if it appears at all. It does not manifest every time. In this way, an addiction of sorts is created.

A common theme among these technology areas is maximizing the cost/benefit ratio for a system user. A user interacts with a computer to accomplish some task, that is the base reason for the interaction. Accomplishing that task has some cost associated with it in terms of time, effort, thought, etc. The amount of cost required to complete the intended task can be viewed as a cost/benefit ratio. The cost of accomplishing the task (time, effort, thought, etc.) versus the payoff of task completion (having it complete). The tools function by maximizing this cost/benefit ratio. Since the benefit is fixed, the task is either complete or it is not, and the only variable remaining is the cost. By reducing the perceived cost of accomplishing a task, the system has in effect elevated the cost benefit ratio. The remaining two roles that Dr. Fogg discusses are not directly applicable to this research and so will not be covered here.

Influence Operations (IO)

Air Force Doctrine Document 2-5 (AFDD 2-5), *Information Operations*, discusses IO in terms of three capabilities: influence operations, electronic warfare operations, and network warfare operations. These capabilities are used in three domains of an the information environment, namely, the cognitive, information, and physical domains. Social engineering has a direct effect on two of these domains (information and cognitive) with the potential for affecting the third. As explained earlier, social engineering operates in the cognitive domain, that is, in the realm of thought and decision making. It is mental sleight-of-hand, an attempt to convince a target to think something that may not be entirely accurate. Information is the objective of social engineering, either in terms of system access and the associated knowledge that comes with that access or through knowledge gained about some target system or organization of interest. Social engineering is flexible enough that an operation that could conventionally be viewed as failed could in fact reveal vital information.

As the following section on Battle Damage Assessment will point out, there is always information to be gleaned. Potential for affecting the third, physical, domain comes in light of a demonstration produced for the Homeland Security Agency in which a generator was caused to self destruct by being fed attack commands over the network to which it was attached [9]. Social engineering will not produce an effect like this directly, although it could provide the access to the network which would enable this type of action.

Social Engineering and IO Capabilities

The three capabilities, Influence Operations, Electronic Warfare Operations, and Network Operations, that comprise IO must necessarily contain all things that could be considered Information Operations. That is, if an activity is considered an information operation, it must fit one or more of the three capabilities that

together form the sum total of IO. Therefore, working from the premise that social engineering is in fact a variety of information operation, we must demonstrate where in this framework it resides. The obvious choice is influence operations. As mentioned earlier, social engineers work through methods of persuasion. Persuade and influence are actually synonyms [3]. Influence operations are further broken down into capabilities of Counter Propaganda, Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Counterintelligence (CI) Operations and Public Affairs (PA). Social engineering is inherently misleading and therefore does not belong in PA [7]. OPSEC is chiefly concerned with the disclosure of friendly information rather than the discovery and exploitation of adversary information [15] and therefore will not be used in this discussion. Similarly, CI and Counter Propaganda Operations are primarily defensive, seeking to protect our assets against the espionage and intelligence activities of an adversary [7]. Social engineering as an activity is inherently offensive in nature and therefore does not fit well into any activity with protection or denial as its primary purpose.

We are left with the capabilities of PSYOP and MILDEC under the umbrella capability of influence operations. PSYOP is a natural sibling of social engineering as its primary target is the cognitive domain of the adversary [7]. In contrast to MILDEC which will be discussed shortly, PSYOP seeks to create influence or reinforce favorable ideas whereas MILDEC seeks to mislead or deceive although both influence the decision process of an adversary in similar ways.

Social Engineering in the Doctrine

Having identified potential siblings of social engineering in the doctrine, this section illuminates similarities to solidify the proposed links. Starting with a famous PSYOP operation example which took place during Operation Desert Storm in 1991, we connect key characteristics in PSYOP and MILDEC to techniques used by social engineers. Figure 2 shows a pamphlet used in an aerial drop.

This PSYOP example evidences a key characteristic, the reinforcement of a perceived truth favorable to friendly forces. The truth is that friendly aircraft operate at will, targeting adversary forces with impunity and is implicit in the declaration that a specific unit will be tomorrow's target. This statement carries less influence if the adversary does not believe in the statement's veracity. In this case, it is a reasonably close fit to the truth as the adversary perceives it and so has more impact. Basing PSYOP operations in truth generates more impact.

Military deception affects the adversary's decision process by causing them to use faulty information as the basis for their decision cycle [7]. World War II's Operation MINCEMEAT is a famous example of MILDEC [12]. The operation involved dropping the body of a supposed British Officer into the Mediterranean Ocean off the coast of Spain. This officer, Maj William Martin, was in fact entirely fictional, the identity created to go on top of the body of a 34-year old male who had died of pneumonia. Maj Martin was brought to life with a thorough background legend complete with pictures of his fiance and ticket stubs from movies he had attended. Also on his person when he was found in the water was a briefcase, chained to him, containing documents suggesting the long anticipated invasion of southern Europe by the Allies was planned for Sardinia and not Sicily as previously thought by the Axis powers. Despite objections by the Italians, the Germans accepted this misinformation and refused other evidence to the contrary, even after the Allies landed in Sicily.

There are several areas of interest here. First, the operation required a total dedication to detail. Aside from the props placed on the body, Maj Martin had paperwork generated in his name and was even placed on the next list of deceased soldiers published by the British. This detail was essential as it was later discovered

Figure 1: Sample Leaflet Used during Desert Storm in 1991. The writing roughly translates to "The 16th Infantry Division of the Iraqi army will be bombed tomorrow. Leave this location now and save yourselves." (from www.psywarrior.com)

that the Germans had checked many of these points when they got access to the body and the documents. Second, the operation allowed the enemy to discover the information rather than feeding it to them. Placing the body in the water was risky for the British; they could not be certain it would get into German hands. However, they understood that in order to give the set the most authenticity, it had appear to be an actual discovery. Finally, commitment to the deception was total. Even after getting the body back from the Spanish (who ensured the Germans viewed it and its attached paperwork before returning it), the British buried the body under the false identity. Indeed, it took until 1996 for an amateur historian by the name of Roger Morgan to discover evidence suggesting that Maj Martin was indeed a homeless Welsh man named Glyndwr Michael [1].

These same traits are visible in the realm of social engineering. As stated above, a key element of a successful PSYOP is that it be rooted in truth. Kevin Mitnick includes a section detailing the various weapons in the arsenal of a social engineer in his book *The Art of Intrusion*. One of these weapons is trappings of the role [11]. Trappings of the role is simply affecting characteristics that a person would expect someone in the claimed position to posses. For example, wearing a nice suit if claiming to be an executive or speaking with a slight drawl if claiming to be calling from the south. These small touches of truth reinforce the perception that all the information presented is the truth as well.

Attention to detail, the second characteristic, is also important to the social engineer. The Art of Intrusion recounts the story of a man hired to do a security audit on a casino in Las Vegas. As background for this

job, the man spent a week doing research before even heading out to the site. When he identified a potential target, he was able to ask her out to dinner where he gave her the background story of his assumed persona, complete with university attended and a fictitious recent breakup with a girlfriend [10]. Later, when he attempted to penetrate the casino with the information he gleaned, he made sure to dress the part of the junior executive he was claiming to be, even noting that the color of his suit was blue, a color he believed associated with trustworthiness. Like the creators of Operation Mincemeat, this individual knew that the details create the story.

The third characteristic noted was that the adversary was allowed to discover the information on their own, making it appear more valid. Again turning to Mitnick, this time in his book *The Art of Deception*, we find a parallel example in social engineering. In this case, the attacker began by cold calling a company, claiming to be from the help desk and warning users of an outage. He gave out his cell phone number to those people in case they did experience an outage. What they did not know is that he had put mechanisms in place that caused an outage and when it happened, they called the cell phone number of the friendly help desk employee that warned them of this possibility. During his help session with them, he got the individuals to download and run a small application on their machine under the guise of troubleshooting. When this did not fix the problem as he knew it would not, he walked them through the steps of erasing it. So he was able to get the users to download an application, run it, and then erase it. During this process, the users remained convinced that they were talking to their help desk and that this person on the other end of the line was trying to assist them [10].

The final characteristic is total commitment to the fabrication that the social engineer has created. Turning back to the man hired to do a security penetration test on a casino in Las Vegas, we see an example of this as well. This man was in an office he should not have been in and was "caught" by a security employee. The employee did what he was supposed to do and challenged the individual about their right to be where they were. Instead of admitting defeat, this person used the event to their advantage by admitting to some but not all of what the security person suspected. This broke the momentum of the guard and ended up defusing the situation [11].

Application

Attack Planning and Battle Damage Assessment

One of the keys for any military operation is to be able to assess the effectiveness of that operation after its conclusion. As succinctly stated by Gen Norman Schwartzkopf in his book *It Doesn't Take a Hero*: "...too much optimism could prompt us to launch the ground war too soon, at the cost of many lives; too much pessimism could cause us to sit wringing our hands and moaning that the enemy was still too strong" [13]. Stated another way, knowing what effect prior actions have had on an adversary is necessary to chose the right moment for further action. It also indicates whether more of the same type of action is required, if the desired state has been achieved, before proceeding to the next set of objectives.

Recognizing the requirement for a method to conduct Battle Damage Assessment (BDA) on social engineering attacks as a requirement for real legitimacy, we use a method called Aerospace Intelligence Preparation of the Battlespace (AIPB) which is an intelligence gathering and processing framework that leads to Predictive Battlespace Awareness (PBA) [6]. PBA, among other things, provides an ability to accurately anticipate changes to the battlespace. The focus of this research is not on the methodology of the existing AIPB process but rather on the best way to adapt that process to enable better planning and assessment of social engineering operations.

BDA is essentially a function of expectations. Dropping a bomb, we expect to destroy whatever it was dropped on, and we measure our success by that expectation. If we go back and look at the target after the bomb has exploded and the item is not destroyed, our expectations have not been met, and BDA indicates that the item needs to be targeted again. We found this idea intriguing and reasoned that if we could anticipate with a fair amount of certainty what the battlespace would look like given a certain set of actions, then BDA is nothing more than seeing how well the observed state matches the anticipated state. Extrapolating this concept to the cyber realm and more specifically, social engineering, we assume it is possible to plan, execute and evaluate a social engineering attack using something similar to the AIPB process.

The immediately noticeable drawback is that AIPB is a lengthy and labor intensive process, often begun well in advance of the coming conflict. It relies on large databases of information that are compiled and referenced by hand [6]. This method of operation is not acceptable given the speed with which information operations take place. For our purposes, while the model is sound, the prescribed method of execution is too cumbersome to be effective. Therefore, we trimmed the process down to as few steps as possible while keeping the core intent in place. The next section discusses in detail the revised process.

Planning Social Engineering Attacks and Performing BDA

The AIPB process has four phases, all of which will be used with some modification. These phases are:

- Define the Battlespace in the Environment
- Describe the Battlespace Effects
- Evaluate the Adversary
- Determine Adversary Courses of Action

Phase 1: Define the Battlespace in the Environment. Joint Publication 3-13 defines Cyberspace as a "notional environment in which digitized information is communicated over computer networks" [15]. This encompasses quite a large potential area of operation, so the first step of our process is to narrow down the scope to something manageable. The purpose is to set boundaries on the problem and identify specific areas and features of the environment for further analysis. For social engineering, this is a four step process.

1. Analyze the Mission. Review higher headquarters and local objectives in order to gain familiarity with the the desired end state. Source material for this phase can come from a wide variety of areas. Anything from National Military Strategy to local estimates of the situation may be used to enhance the battlespace picture. In some cases, information gathered may range beyond the scope of the current operation. This is acceptable as long as the information contributes to a more thorough understanding of the situation. The desired product from this phase is a full understanding of the mission requirements and the constraints the commander is operating under.
2. Identify Limits of Operational Area and Determine Possible Second Order Effects. This begins the process of scoping the mission. Creating a well defined Operational Area ensures that elements outside of our control or concern are not included in the planing process. However, it is important to stay aware of the area outside the defined Operational Area in order to accurately predict possible second order effects. Second order effects are the unintended consequences of some intentional action. Guidance for determining the scope comes from specific commander's objectives and Rules of Engagement.

3. Identify Knowledge Gaps and Set Priorities on Resolution. In this phase we should be aware of what we do and do not know about the Operational Area. If any mission critical information is missing it should be identified. Missing information is deemed critical if it is essential to the mission that was completely described in the first phase. After the gaps have been identified, prioritize their resolution knowing that in all likelihood several will not be resolved at the time of mission execution. To meet this constraint, different methods of prioritization such as utilizing a knapsack algorithm may be desirable. The desired product from this phase is a prioritized list of required information.

4. Collect Required Information to Complete Process. As time allows, collect the missing information in accordance with the prioritized list created in the previous phase. In reality, the collection of information is a continuous process. The desired product from this phase is a more complete view of the mission and items, both friendly and adversary, that impact that mission.

Phase 2: Describe the Battlespace Effects. This section of the process analyzes the battlespace for effects on adversary forces. It seeks to identify areas of advantage and vulnerability in order to more accurately predict how the battlespace affects both conflict contestants. The desired product from this section is a through understanding of the how the battlespace could influence the mission and courses of action for friendly and adversary forces. For social engineering, this is a three step process:

1. Analyze the Physical Environment. Analyzing the physical environment includes reviewing everything from geography and climate to equipment and facilities. Anything that has a physical form but interacts in some way with the cyber domain inside the Operational Area is included in this analysis, keeping in mind not to neglect space assets and weather. Key questions include but are not limited to what assets does the adversary have and how may they be employed? what is the weather forecast during the planned time of the mission? what political boundaries are in play? what are the physical connections to the target system? what physical limitations do we have? power constraints, HVAC constraints? The goal is to fully understand the role of the physical environment on the mission.

2. Analyze the Human Dimension. This incorporates all elements not already accounted for in the physical domain. Included are political factors, centers of gravity, international alliances, sociocultural considerations, psychological dispositions, economic situations, demographics and quality of life. The goal is to fully understand what motivates adversary forces and how those motivations change with time and pressure. It is important to note that this analysis may be required on a host nation if friendly forces are operating from inside their borders. Understanding the impacts of planned activities on the country that is providing a base of operations is an important and potentially volatile concern. Losing host nation support could turn a tactical success into a strategic failure.

3. Describe the Effects of the Physical Environment and Human Dimension on Friendly and Adversary Operations. Now that both the physical and the human environments are understood, they are applied against planned operations. If previous efforts to fully analyze both environments have not been thorough, the lacking areas will be exposed in this step.

Phase 3: Evaluate the Adversary. The purpose of this step is to gain a better understanding of the adversary. Review their Centers of Gravity (COG), capabilities and limitations, doctrine, tactics, techniques and procedures (TTP). In addition, evaluate their cultural attitudes, looking for indicators that make courses of action more or less likely. For social engineering, this becomes a three step process:

1. Identify and Analyze Adversary Centers of Gravity. This seeks to identify the vulnerabilities in the adversary's COG. A COG is a source of power, some characteristic from which a particular organization, be it public or private, derives strength. It can be tangible like a monument or a financial district or intangible thing, such as freedom. In conducting this step, the purpose is to identify exploitable vulnerabilities in those COG where possible. When not possible, the goal is to identify and remain cognizant of the COG throughout the mission process. It is also possible for a particular course of action to have a center of gravity. For example, the will of the American people to combat terrorism post 9/11 could be viewed as a COG.

2. Identify Applicable Cultural Nuances and Assess Their Impact. This step is vitally important to the social engineer. As identified earlier, details like cultural customs, norms and nuances are often the details that create a successful operation. The social engineer needs to understand the frame of mind of the adversary, what motivates him and how far he will go before feeling threatened. This step also includes identifying dialects and appropriate slang which can successfully add a more authentic feel to the communication. Finally, collect information about popular current events in the area. Items such as political news, sports news and weather can set an adversary at ease and create the level of authenticity desired.

3. Describe Current Adversary Situation. This step illuminates the current status of the adversary, matching assets with their locations, purposes and availabilities. Adversary assets that are particularly important to the mission, high value targets (HVT), are identified. Finally, attempt to predict adversary reaction to the loss of each indicated HVT, what behaviors they might display if this asset were lost. This effort is influenced by nuances specific to the adversary and so draws heavily on the understanding generated in the previous phase.

Phase 4: Formulate Mission Execution Plan and Determine Adversary Course of Action. This final step of the process solidifies the operational plan and adds an anticipatory element for use in BDA. This step identifies, prioritizes, and weights adversary Courses of Action (COA) taking into account the factors and variable noted in the previous three steps. For cyberspace, this step has two purposes depending on the situation confronting the commander. The first purpose is reactionary and seeks to identify what adversary response is likely if we initiate conflict. The second purpose is proactive and looks at all possible adversary COAs, identifying a small subset that are particularly advantageous to friendly forces and working backwards to find actions that would induce the adversary to pursue those COA. For social engineering, this is a five step process:

1. Explicitly Identify Assumptions. Friendly forces are working from an imperfect view of the adversary. While this planning process removes much of the fog of war, it is impossible to have total knowledge of what an adversary plans or will likely do. Realization of this shortcoming necessarily leads to a certain amount of best-guessing, making assumptions about the situation based on information and observed prior behavior. These assumptions are unavoidable but should be noted. The goal is to explicitly identify these assumptions in order to keep them in proper perspective.

2. Finalize Mission Plan. Drawing on the information gathered in the previous steps, draft the final plan to accomplish the mission objective. Review plan for last minute additions or subtractions keeping in mind that the plan must remain flexible in order to remain viable.

3. Identify Adversary Courses of Action and Desired End State. This brainstorming step seeks to identify all possible adversary COA in response to the planned mission. There is no concern for the likelihood

that these COA will occur, simply identify as many as are logical given the current circumstances. Everything is on the table and considered a possibility. Begin to narrow the list by identifying the adversary's desired end state, the situation they are most likely to attempt to attain. This will automatically eliminate those unrealistic COA, leaving only possible outcomes.

4. Weight COA. This step takes the remaining, realistic, COA and assigns a weight value to them in order to establish a probabilistic set of outcomes. Each COA is weighted by the number of indicators friendly forces currently have that the adversary COA is possible. For example, if the course of action under consideration is that the adversary will deploy more troops to a specific location, indicators could be items like reports that transport trucks have begun to move, that adversary TTPs prescribe this procedure or historically this has been their response. These are all indicators of the particular COA and contribute to its weight. Alternatively, a COA may be weighted more heavily based on a single indicator if it is the assertion of a subject matter expert that this is warranted. Using the same troop movement as an example, if the only indicator currently available is a TTP that states this troop movement will take place, we can assign additional value to this COA if we believe that it will take place even though a single piece of information supports that assertion. Ultimately, the decision to add this additional weight or not falls to the mission commander.

5. Identify Required Intelligence Assets Needed to Measure COA. This final step matches our most likely adversary COA with friendly forces ability to measure them. This is the heart of the Battle Damage Assessment for a social engineering operation. The weighted list of COA provides expectations and BDA is simply checking expectations against reality. Observation assets are tasked to observe the expected adversary COA and relative mission success is based on those observed behaviors. Not having expectations and reality match is not necessarily a sign of a failed mission. Social engineering operates in the cognitive domain which introduces a measure of uncertainty this process is unable to eliminate.

Conclusion

In this paper, we have discussed social engineering from both a doctrinal and a practical standpoint, demonstrating its inclusion and usefulness. As the Air Force goes through the process of standing up a cyber force, all tools and capabilities should be evaluated. While our research does not profess to have all the answers in relation to social engineering, we think it demonstrates the viability of such an option. When combined with its low cost nature, it delivers outstanding returns for the investment.

There remain many areas to explore. One possible avenue of research is to apply a predictive statistical model to this problem in order to achieve the desired robustness and flexibility. It is possible that the visible reaction of the adversary will not match what we expected to see and yet still indicates a successful operation. Or it may be that the particular adversary does not outwardly display the expected reaction but we can reasonably expect others in a similar situation to react in the expected manner. The current framework does not easily adjust to these unpredictable results but applying a mathematical approach to it might yield more flexibility.

Another area for future work is in applying the proposed framework to a past PSYOP or MILDEC operation. As demonstrated earlier, these are close siblings of social engineering and would provide a good approximation in lieu of real data from a social engineering operation. This would provide a better indication of the framework's viability.

Finally, this research focused on the Air Force and its doctrine. Expanding into Joint doctrine and the

doctrine of our sister services and other nations could yield a more complete indication of the direction needed in order to bring social engineering on line for military purposes. Additionally, it could increase its legitimacy in the Air Force if similar results were found when investigating other doctrine.

Disclaimer: The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

References

1. BBC. "Operation Mincemeat—The Man Who Never Was", 28 Jan 2005.

2. Cialdini, R. B. and B. J. Sagarin. *Persuasion: Psychological Insights and Perspectives*. Sage Press, Newbury Park, CA, 2005.

3. Dictionary.com. "Influence", 2006.

4. Downs, Julie S., Mandy B. Holbrook, and Lorrie Faith Cranor. "Decision Strategies and Susceptibility to Phishing". *Symposium On Usable Privacy and Security (SOUPS)*, July 12-14, 2006, Pittsburgh, PA, USA.

5. Fogg, B. J., *Persuasive Technology: Using Computers to Change What we Think and Do*. Morgan Kaufman Publishers, 2003.

6. Department of the Air Force. Air Force Pamphlet (AFPAM) 14-118, *Aerospace Intelligence Preparation of the Battlespace*. 5 June 2001.

7. Department of the Air Force. Air Force Doctrine Document (AFDD) 2-5, *Information Operations*. 11 January 2005.

8. Lopez, Todd C. Staff Sgt. "8th Air Force to Become New Cyber Command", Air Force Link, http://www.af.mil/news/story. 3 Nov 2006.

9. Meserve, Jeanne, "Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid," CNN.com, 26 September 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

10. Mitnick, Kevin D. and William L. Simon. *The Art of Deception*. Wiley Publishing, 2002.

11. Mitnick, Kevin D. and William L. Simon. *The Art of Intrusion*. Wiley Publishing, 2006.

12. Montagu, Ewen. *The Man Who Never Was: World War II's Boldest Counterintelligence Operation*. Oxford University Press, 1953.

13. Schwartzkopf, H. N. and Peter Petre. *It Doesn't Take a Hero*. New York, New York, 1993.

14. Skarda, B. Personal interviews with Air Force members conducting and training social engineering techniques as part of their duties.

15. Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*. 13 February 2006.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu