3-5-2008

Operationalizing Offensive Social Engineering for the Air Force

Bryan E. Skarda

Operationalizing Offensive Social Engineering for the Air Force

THESIS

Bryan E. Skarda, Major, USAF

AFIT/GCO/ENG/08-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this paper are those of the author and do not reflect the official policy or position of the United States, Department of Defense, or the United States Government, except where noted.

AFIT/GCO/ENG/08-07

Operationalizing Offensive Social Engineering for the Air Force

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science (Cyber Operations)

Bryan E. Skarda, B.S.

Major, USAF

March 2008

AFIT/GCO/ENG/08-07

Operationalizing Offensive Social Engineering for the Air Force

Bryan E. Skarda, B.S.
Major, USAF

Approved:

/signed/	5 Mar 2008
Dr. Robert Mills (Chairman)	date
/signed/	5 Mar 2008
Dr. Dennis Strouble (Member)	date
/signed/	5 Mar 2008
Lt Col Todd McDonald, PhD (Member)	date

Abstract

Social engineering is the art and science of persuading individuals to bypass in place security mechanisms causing the unintended release of information. It is a low tech solution to a high tech problem and is as much an art as a science. As is true of many such solutions, social engineering is both ill-defined yet extremely effective. Its low cost, high payoff nature makes it an extremely attractive alternative to adversaries that do not have access to all the resources of a nation state. However, with full backing, the weapon can become that much more effective.

Social engineering is something the Department of Defense already does. All branches of the military have Red Teaming organizations that use social engineering methods as part of their mission to assess and improve internal security measures. While network and physical protection mechanisms have become more robust, the human remains the weak point of any defense, and social engineering will nearly always succeed.

As the Air Force organizes, trains, and equips its new cyber warrior force, it will need to operationalize social engineering principles in order to grow a repeatable, sustainable capability. However social engineering remains a poorly defined concept for the Air Force in particular and the Department of Defense in general. It is something practiced but on a limited scope and with little standardization. Despite its successes, social engineering has yet to achieve widespread acceptance.

The focus of this paper is on the use of offensive social engineering. There are three main points. First, establish legitimacy and demonstrate that social engineering is in fact compatible with existing Air Force and Joint military doctrine. This is done with a thorough analysis of doctrine and historical writings about military deception, psychological operations, and related concepts.

Second, social engineering arrives in the operational realm by discussing a framework for measuring its effects. A primary concern for any implementation of a cyber weapon is measuring its effectiveness. A well known process, Aerospace Intelligence Preparation of the Battlespace, is extrapolated and adapted for use in this realm.

Finally, requirements for a training plan are developed as a first step in the implementation process.

Acknowledgements

No work of this scope occurs in a vacuum nor is it solely the result of my efforts. I owe a big debt to my advisor, Dr. Robert Mills, for his patience and subtle course corrections that kept me going down the right path. Also, to Maj Paul Williams for his encouragement to pursue an idea I might have otherwise overlooked. Additionally, I'd like to thank the men and women of the 39th Information Operations Squadron and the 57th Information Aggressor Squadron. Their willingness to share time and knowledge was as humbling as it was enlightening.

Thanks to my AFIT family, especially my Coach, those other students with whom I commiserated and celebrated during my time in this program. As always, the quality people I get to work with on a daily basis is the best part of my Air Force career.

Finally, I'd like to thank my family for their unending support and encouragement. Special thanks to my father for his guidance and wisdom. I'm where I am because of you, Dad.

Bryan E. Skarda

Table of Contents

List of Figures

List of Tables

Operationalizing Offensive Social Engineering for the Air Force

I. Introduction

An experiment performed in 2005 hooked six computers up to a DSL connection in order to record cyber-attacks against them. In less than four minutes, an automated attack had broken through the computers security defenses [28]

Social Engineering describes a class of computer hacking tools that target the user of the system rather than the system itself. It is a proven and viable attack vector that includes methods like phishing, pharming, and persuasion [35] [25]. The Air Force uses social engineering to a limited extent as a validation tool when assessing the security posture 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 [6] [43]. However, this is the only employment of social engineering currently evidenced in the Air Force inventory.

The Air Force has embraced cyberspace as an operational domain and has begun to organize, train and equip a force to operate in that domain [30]. As such, the Air Force should focus on the cultivation and employment of all possible methods to achieve supremacy in that domain.

1.1 Definition

Social engineering is a weapon that could deliver this supremacy. Social engineering has many definitions dependent on the context and personal biases However, Winkler and Dealy [49] provide a good definition with

> *the process of using social interactions to obtain information about a "victims" computer system*

While this is a good overview, it misses the elements of art and science so an alternative that incorporates the three key elements of social engineering is used. This definition is

> *The art and science of convincing a person to willingly provide information under false pretenses*

It fully encompasses the three key elements of social engineering which are:

- Information
- Persuasion
- Deception

Anecdotal evidence gleaned from both interviews and literature reviews places the effectiveness of social engineering at or near 100 percent [43]. Based on this widespread success in the civilian world, 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 [49]. These attributes indicate it is an attractive option to adversaries of the United States although their employment of it and US defense against it are outside the scope of this research. The discussion is limited to the Air Force although much of the research could be applied throughout the Department of Defense.

1.2 Implications

This research is firmly grounded in the reality and requirements of today's Air Force. Some forms of social engineering, like phishing, have become a top security threat currently facing civilian corporations [46]. From automated chat programs that impersonate people in order to collect personal information [22] to tactics used by current Air Force Red Teams attempting to assess the security stance of a particular unit, social engineering is inexpensive, low tech, and effective.

Figure 1.1 shows a briefing slide from a presentation recently put together by Hurlburt Air Force Base's Information Operations Office in response to some concerns

of their members. The information was posted to a social networking site billing itself as military only but with no military ties. In fact, the hosting server is based in Nova Scotia and the company that owns it is German [26]. Social engineering is everywhere.

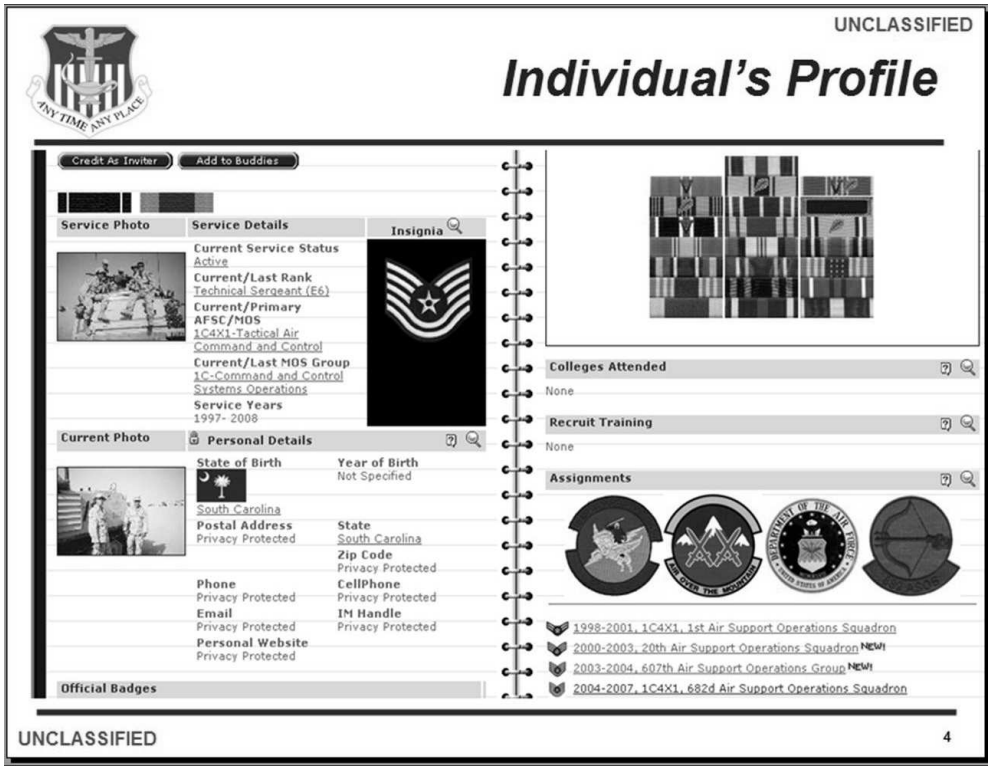

Figure 1.1: Member Profile on a Social Networking Website [26]

1.3 Purpose

Recognizing the advantages of social engineering and its current lack of incorporation in the Air Force arsenal, this research creates an argument for utilizing offensive social engineering in the Air Force. It outlines the underpinnings of social engineering, illuminating the powerful psychological cues that create the high success rate. It discusses where social engineering fits in current doctrine, drawing parallels to familiar concepts. It takes an existing, accepted, methodology and alters it for use in planning and evaluating a social engineering attack. Finally, it presents research done in task identification and the resulting training objectives.

The analysis begins with the background of social engineering, reviewing the exploits of Kevin Mitnick who is perhaps the most famous hacker in the United States [29] and whose most successful operations used social engineering techniques. The essence of social engineering, persuasion, is discussed as well as the psychological underpinnings that make it effective. Exploring human-computer interaction, research being done at Stanford University by Dr. Fogg on a new area of study called Captology is reviewed. This thesis reviews Influence Operations, a term that arguably points to social engineering. Chapter Three outlines the research methodology used and illuminates the iterative process involved. Chapter Four presents the results of the research, demonstrating the link between social engineering and Influence Operations, providing a framework for planning and evaluating social engineering operations, and suggesting objectives to consider when training social engineers.

Research Questions:

1. Is Social Engineering a legitimate weapon for the Air Force to consider?
2. Can we demonstrate a link between Social Engineering and Information Operations?
3. Can a Social Engineering attack be planned and measured?
4. What objectives need to be met to train Social Engineers?

1.4 Outline

- Chapter II reviews background information and provides a framework for thinking about social engineering
- Chapter III outlines the framework used to conduct the research
- Chapter IV presents the results of the research
- Chapter V summarizes the findings and conclusions drawn from this research.

II. Literature Review

All warfare is based on deception

–Sun Tzu

This chapter summarizes the literature reviewed in support of the research questions. First, it is important to come to a clear understanding of what exactly social engineering is and is not. To this end, background information on social engineering, outlining two broad categories to assist thesis scope definition are reviewed. Next, methods of social engineering, psychological underpinnings of social engineering, and psychological inroads for social engineering are discussed. Additionally, an overview of a relatively new field of study, Captology, is presented. It encompasses both types of social engineering by blending the technical into the psychological and provides meaningful insight into the human-computer interaction at the heart of social engineering. Finally, Joint Service and Air Force doctrine on Information Operations are examined. A requirement to properly understand where social engineering may fit in the future of the military is a full understanding of how the military views similar techniques today. Towards that end, concepts of psychological operations and military deception are explored.

2.1 Social Engineering Background

Social Engineering is fundamentally an issue with the system users rather than with the system itself making it somewhat unique in the realm of computer security. Computer security professionals tend to be more comfortable with technical challenges and their associated technical solutions, the sheer number of hardware and software based security solutions versus the number of user training solutions empirically bears this out [35]. Figure 2.1 shows a simplified attack which is countered with technology based security measures.

This is a simplified representation of the stance most often brought to mind when discussing computer security. It has the classic elements of "us" and "them"

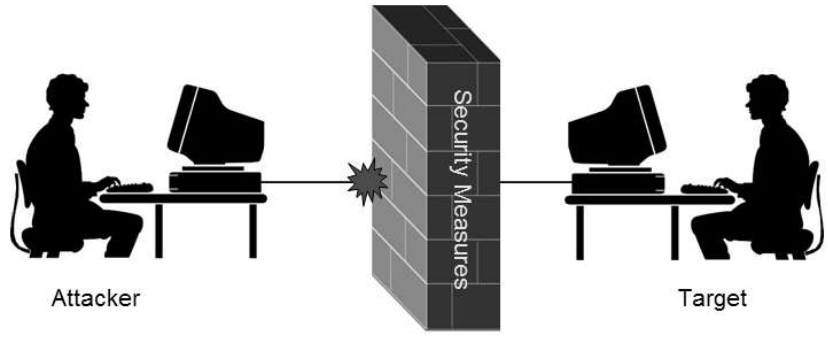

Figure 2.1: Typical Attack Thwarted with Technology Based Security Measures

represented by the attacker and the target, respectively. Also, it has the notion of some kind of security barrier between "us" and "them" that prevents intrusion.

Figure 2.2 shows how social engineering defeats all these security measures by targeting the system user rather than the system itself.

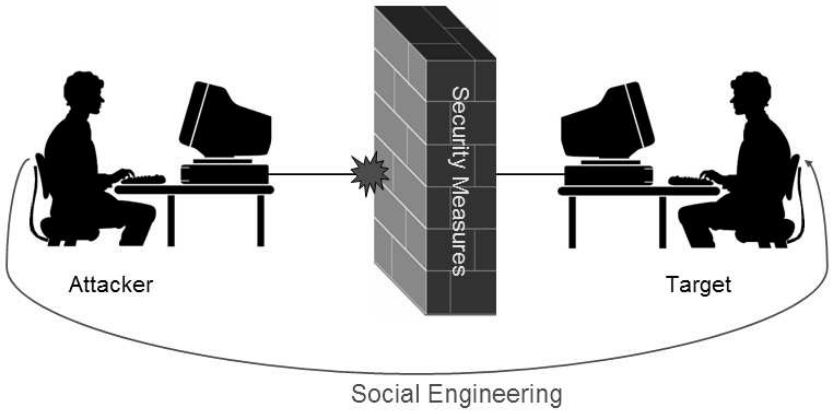

Figure 2.2: Social Engineering Bypasses Technology Based Security by Going Straight to the User

Social engineering blends two fields of study, pulling much of its power from lessons learned in psychology and leveraging them against a computer system, by way of the users of that system, thus blurring the line between the study of man and the study of machine. However, as a portion of this chapter will show, there are some researchers looking into this interaction and this thesis draws heavily on those efforts.

Social engineering remains an attractive avenue of attack for many hackers. The entry cost, which is defined as the funding and training required to effectively compete with a given tool or weapon, is arguably the lowest of any form of computer network attack [49]. Many of the techniques are familiar as everyone has tried to use persuasion at some point in time. With the increased performance from desktop computers, little more is needed than a network connection and a computer. For $3000 or less, an adversary can wield a weapon with more potential for disruption than anything they could acquire at 10 times the cost.

Social engineering is not a single idea but rather a collection of techniques. Some of these will no doubt be familiar, like phishing, while others, like tailgating, are probably only well-known inside the community of hackers and professional red teamers that practice them. This research is not concerned with illuminating and discussing the various implementations of social engineering, choosing instead to focus on the broad methods social engineers use and the key abilities that enable their practice. Drawing an analogy to the Air Force, the techniques discussed here are akin to the basic skills a pilot must have in order to successfully and safely maneuver the plane. The specific implementation is like the combat tactics developed for a given platform. The discussion is constrained to the key skills.

It is not the intent of this research to draw absolute boundaries on what is and is not social engineering. Like many technology-related areas of interest, lines of definition are difficult to distinguish and quickly outdated. However, this research does discuss many different techniques that fall under the social engineering umbrella. This discussion is not intended as endorsement of any techniques legitimacy over another's. Rather, the focus is on proven results, using this as the criteria for inclusion.

2.2 Types of Social Engineering

For ease of understanding, social engineering can be broken down into two basic types: Human-based and Technology-based [38].

Human-based social engineering is the form most familiar. It is defined for the purposes of this research as any social engineering effort that requires the active participation of an engineer. In this context, and throughout the remainder of this discussion, the term engineer is used to denote a person practicing social engineering. Examples include impersonation, cold calling and in-person attacks. All activities must be initiated and prosecuted by an engineer. Being the most hands-on type, these techniques require the highest level of personal sophistication and are the most difficult to teach.

Technology-based social engineering uses some degree of automation to achieve the social engineering results. Phishing, pharming, and the use of chat bots to impersonate people in online communities are all examples of this approach. The engineer is involved at some point, if only to give the tool its instructions but the attack is automated and occurs without direct human intervention. Since the third focus area of this research is training effective social engineers, focus is limited to Human-based methods.

2.2.1 Human Based Social Engineering. There are many different definitions for the categories of a human based social engineering effort, every article written on the subject seems to have different names for different techniques. However, many of the themes remain the same. The presented terminology comes from arguably the most famous social engineer, Kevin Mitnick [28]. Mitnick defines the following human based social engineering techniques [32]:

- Trappings of Role

  Trappings of Role is a technique where the social engineer exhibits a few characteristics of the role he or she has chosen as their cover. For example, if impersonating an executive, they might dress in a nice suit and speak with authority, using a tone that does not invite disagreement or discussion. Other trappings can be simple things like using industry jargon or mentioning other people that work in the organization. The effectiveness of this method lies in its simplicity;

only a few details are required to generate the image. Once the target has the engineer associated with the desired role, they naturally fill in any details that are missing, sometimes providing additional information in the process.

- Credibility

  Credibility is established in three different ways. First, the social engineer can argue a point that appears to be contrary to his or her best interest. A statement like "make sure not to tell me your password" is an example of this kind of tactic. Second, the social engineer can warn the target of an impending problem with the system that the social engineer has in fact caused. For example, calling a target to warn them of a service interruption and then causing the interruption. Finally, the attacker may help the target solve a problem, placing the target in a debt position relative to the attacker. This tactic is exceptionally effective when combined with the second method as the engineer warns the target of an impending negative situation, causes the situation, and then helps the target resolve the situation unbeknownst to the target. The engineer is in control of the entire process.

- Altercasting

  Altercasting refers to placing the target into a role chosen for them. This usually requires a good deal of skill on the part of the social engineer as the target needs to be comfortable with the selected role while remaining totally unaware that they are in it. The engineer needs to be able to read the comfort level of the target and adjust accordingly; this "on the fly" adjustment is an example of the art element to social engineering. For example, the social engineer can place him or her self in a position of disadvantage pushing the target into the role of a helper. Or the social engineer can become more aggressive, pushing the target into a more submissive role. The choice of which role is appropriate is made during the beginning of the interaction based on the engineers perception of the target.

- Distracting from Systematic Thinking

  Systematic thinking is careful rational thought leading up to a conclusion and is the enemy of the social engineer. It is the method of thinking used when following rules and procedures. Heuristic thinking on the other hand involves the use of mental shortcuts to arrive at conclusions more quickly. This type of thinking is invoked when external pressures or cues are present that suggest a certain decision to the target. For example, limiting the amount of time to reach a decision forces the target to jump ahead to the conclusion before all relevant factors have been considered. Alternatively, a person may use heuristic thinking when they believe the person making the request is in a position of authority and that this alone justifies the request. The engineer invokes this thought process by creating an environment of artificial pressure or by capitalizing on some pressure organic to the situation.

- Momentum of Compliance

  Social engineers also seek to create a *momentum of compliance* by asking the target for easy favors and gradually building toward what they really want. When the request(s) of real value are made, the target is accustomed to complying and so finds it difficult to shift behavior and deny the request. This is an advanced technique that also requires a lot of skill as the requests should build on each other incrementally in terms of importance. If the gap between the innocuous questions and the important questions is perceived to be too large by the target, the momentum may falter.

- Desire to Help

  People who help other people get definite benefits from the transaction, from a feeling of accomplishment to an elevation in mood. Social engineers seek to exploit this *desire to help* by casting themselves in a position that puts others in a position to help them. This effect is often magnified by the lowered value the target places on the information they hold. They do not fully understand its importance and so may think it harmless or even useless. Therefore, the

help the target provides seems like a low cost event for them, increasing the cost/benefit ratio and magnifying the positive feelings.

- Attribution

  Attribution is a technique for creating a perception about who the social engineer is. The engineer might hold a door open for someone, say please and thank you, pretend to return money they found on the floor, anything to cast themselves in a positive light. This in turn leads the target to ascribe other positive traits to the engineer, making them more trustworthy and the target more likely to help. Attribution can also refer to a technique for helping the target explain away behavior. In this usage, the social engineer tells the target that someone else said it was acceptable, or that the information requested is useless without some other piece of information. This helps the target transfer the responsibility for the situation to someone else, freeing them up to do what is asked.

- Liking

  Social engineers understand that people are much more inclined to help people they *like* so they try to be likeable. They mirror interests, backgrounds, values, anything they can to make the target like them. This, like altercasting, involves reading the target accurately and involves a good amount of skill.

- Fear

  Fear is an excellent motivator. The engineer uses fear by creating a crisis situation that requires handling in a compressed time frame, usually to avoid some other, more serious, consequence. This compels the target into the heuristic mode of thinking as they no longer have time to process all elements before making a decision. A favorite tactic involves the use of what Mr. Mitnick terms "self-referential fear". The impending dilemma only affects the social engineer, it has no impact on or relevance to the target. For example, the engineer could claim a need to access the system because they need a file it contains or else they will be fired. The threat of termination has no impact on the target; instead it places them in the role of someone who can help avert this outcome.

- Reactance

  Finally, *reactance* can be utilized to make a normally unacceptable request more palatable. The engineer impersonates the IT department and informs a user of a pending lengthy loss to network storage due to maintenance, for example. This disruption is obviously upsetting so the engineer offers a way out if the target will just supply some key information to assist the work around. The request for personal information that normally is met with skepticism is now viewed as a favor.

  Table 2.1 summarizes the information to this point.

2.3 Social Engineering and Psychology

A firm grasp on why social engineering works is required in order to completely understand and implement it. As stated earlier, social engineering crosses discipline boundaries, leveraging psychological mechanisms against a technological goal. A complete view of this interaction begins with a full understanding of social engineering's foundation. Additionally, the information outlined here will facilitate a later discussion on the most advantageous ways to train warfighters in this unique arena.

The heart of social engineering is persuasion, persuading a target to release some information that the engineer finds desirable. Much has been written on mechanisms of persuasion. Thomas Peletier's article titled "Social Engineering: Concepts and Solutions" condensed the information in an easily understandable fashion. Mr. Peltier outlines four human traits that social engineers exploit [38]:

- The Desire to be Helpful
- A Tendency to Trust People
- Fear of Getting Into Trouble
- Willingness to Cut Corners

If anything, these traits are magnified in the military culture. Every wing, group, squadron, flight performs some function which is in turn a service to someone else. Even combat operations are a service when viewed from the seat of the combatant commander. In fact, Service Before Self is one of the Air Force's three Core Values. This emphasis on service builds a strong desire to help. The Air Force is also a

Table 2.1: Summary of Human Based Social Engineering Techniques and Their Associated Characteristics

Technique	**Characteristics**
Trappings of Role	Small number of key traits for assumed role Allow target to fill in the rest Utilize jargon, names where possible
Credibility	Argue a seemingly contrary point Warn of upcoming system problem Help target solve problem
Altercasting	Read target to establish their most comfortable role Assume the opposite role Continue to read target and adjust accordingly
Distracting from Systematic Thought	Provide external pressure Provide implied reason to comply Do not let target think through the request
Momentum of Compliance	Ask easy questions at first, build toward goal Incrementally increase question sensitivity Do not end with desired information
Desire to Help	Target gains emotional benefit from helping Provide situation with low cost, high benefits Importance of information often undervalued
Attribution	Display favorable behavior Target assigns other favorable behaviors Provide target a way to explain their behavior
Liking	People help those they like Mirror interests, backgrounds, hobbies Requires social charisma
Fear	Create a crisis situation Compels target into heuristic thought Can also use self-referential fear
Reactance	Makes a distasteful request more palatable First offer unacceptable outcome Then offer work-around if information is provided

selectively manned force. While it remains all volunteer, applicants have to meet certain requirements to join. Those that get to wear the uniform are in some ways select and other members of the service respond to this. When someone else in uniform comes for help, they receive the benefit of the doubt if for no other reason than organizational affiliation. The Air Force is also very rank-oriented. It has a definitive hierarchy that all members know and necessarily respect. This rank consciousness has the side-effect of breeding a certain amount of fear, especially in those of lower ranks. When a higher ranking individual requests something, the request is not questioned, it is answered. Finally, the advent of Force Shaping coupled with increased deployment and operations tempo has left virtually all members with too many tasks to accomplish in too little time. This overabundance of work creates an atmosphere where any chance to save time by cutting a corner looks attractive.

2.4 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. Dr. 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 [13]. These six principles are reciprocity, social validation, commitment/consitency, friendship/liking, scarcity, and authority. Interestingly, many of these same principles are mentioned by Kevin Mitnick as methods available to a social engineer. Table 2.2 displays these principles of influence as well as some descriptive characteristics.

Dr. 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 Dr. Sagarin's research does not focus on social engineering, the social engineer makes use of these persuasion pressure points to gain the information desired. Indeed, another researcher is currently working on effective ways to defend against social engineering based in large part on Dr. Sagarin's principles [40].

Table 2.2: Overview of Dr. 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 scare 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

2.5 Captology

Dr. B.J. Fogg, a professor at Stanford University, introduced Captology in 1996 and continues to be the expert this new field of study. Captology is an acronym based on the acronym "computers as persuasive technology" [19]. It is important to note that Dr. Fogg does not view this persuasive relationship in terms of attackers and targets, rather as a benign social interaction. However, given the focus of this research and the obvious applicability of Dr. Fogg's research, attention to his work is warranted.

2.5.1 Computers as Tools. Dr. Fogg's book is organized into three areas, each devoted to one of the roles that computers play when they act in a persuasive role. The first of these is *Computers as Tools*. Inside of this broad categorization, Dr. Fogg defines seven persuasive technology tools that are available.

- Reduction Technology: Persuading Through Simplifying

  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: Guided Persuasion

  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: Persuasion Through Customization

  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 [17], is a timely 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: Intervening at the Right Time

  Suggestion Technology presents desired behaviors to the user at the most opportune moment. An example from the military is PSYOP operations 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: Taking the Tedium out of Tracking

  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: Persuasion Through Observation
  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: Reinforcing Target Behaviors
  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.

The common theme running through these tools is maximizing the cost/benefit ratio for a system user. A user interacts with a computer to accomplish some task, which is the basic 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 versus the payoff of task completion. Since the benefit is fixed, the task is either complete or it is not, the only variable remaining is the cost. Thus, by reducing the perceived cost of accomplishing a task, the system has in effect elevated the cost/benefit ratio.

2.5.2 Persuasive Media. The second role that a computer can assume when acting in a role to persuade humans is that of *Persuasive Media*. In this role, the

computer and the information it provides become the medium through which a user has an experience. Computer simulations are excellent examples of this.

As Persuasive Media, computers allow humans to try out new ideas, new scenarios and new behaviors without ever really changing them. If the experiment runs astray, they simply reset and try again. This no-fault method of trial and error can be a powerful persuader.

Of particular interest is the tendency of a target experiencing a simulation to discount the accuracy of what they are shown. People tend to get too wrapped up in what is being presented to worry about how accurate it is. This enables simulation designers to include their own biases into the virtual reality they have created and have those biases subtly accepted by the target.

2.5.3 Persuasive Social Actor. The third and final role that a computer can assume is that of a *Persuasive Social Actor*. This particular employment of social engineering is outside the scope of this research and is mentioned for background information only. In this role, a computer acts like and is treated as another social being. The computer may provide social support, model target behaviors or attitudes, or reward the target with positive feedback. In this way, the target stops thinking of the computer as a machine and starts looking on it as if it were alive. This role is also relevant to social engineering in light of some recent articles on bots being used to conduct chats with humans [22]. The computer displays one or more of five different social cues to achieve this effect

- Physical

  Physical cues can be very wide ranging. It could be something as simple as the customizable "Office Assistant" that was a part of Microsoft Office 2000 or as complex as the ASIMO robot from Honda shown in Figure 2.3. What is important is that the technology display some look or behavior that the user can identify with and therefore assign it the label of "alive".

- Psychological

  Psychological cues can be anything that directly or indirectly convey feelings, preferences, or attitudes to the target. An error message that apologizes to the user is a simple example. The key here is similarity, the computer must be able to establish some level of similarity with the target. Dr. Fogg conducted a study in which he paired subjects previously identified as either dominant or submissive with computers programmed to act in either dominant or submissive manners. What he found is that the subjects reported more satisfaction in working with the computers most closely associated to their personality.

- Language

  Language cues are also useful for creating a sense of social connection with computers. Often this is accomplished with a text box of voice response. Simple text can be used to convey a personality. For example, instead of saying Hello to a user that logs into a site, it can instead respond with a personalized greeting that reminds them how long they've been away, giving them the feeling of being missed.

- Social Dynamics

  Social Dynamics are unwritten rules pertaining to acceptable patterns of interaction. Computers can display these rules of interaction in the form of coercion or peer pressure. A nag screen that repeatedly asks a user to undertake some type of action is one example of this. A smartly worded reminder is another.

- Social Roles

  A computer can also assume the trappings and thus the importance of various *social roles* commonly reserved for humans. For example, a computer can be assigned the task of handling intake questions during a medical screening. Surprisingly, it is not uncommon for the human respondents to these questions to treat the computer like it was a doctor in its own right.

Figure 2.3: An Advertisement From Honda Showing the ASIMO Robot [27]

2.6 Doctrine

The first two foundational questions for this research pertained to the legitimacy of social engineering as a weapon for the Air Force and the relation, if any, of social engineering to the existing concept of Information Operations. These questions necessitated a review of existing doctrine for information. The review begins at the Joint level and works down to the Air Force.

2.6.1 Joint Information Operations Doctrine. Joint Publication 3-13, *Information Operations* (JP 3-13) is the definitive work for the Department of Defense for describing all aspects of Information Operations (IO). JP 3-13 defines IO as:

> *the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.* [44]

This definition contains some key concepts, highlighted here, that will become useful in chapter 4. First, JP 3-13 describes the integrated employment of the various components. This implies that no component operates on its own and that only when

the different elements are operating synergistically does effective IO exist. Second, the doctrine includes both technical (Computer Network Operations) and non-technical (OPSEC) elements. This suggests the full use of all elements available. Finally, the stated goal is to alter an adversaries access to their information system while simultaneously protecting our own systems. This indicates both an offensive and defensive component.

2.6.1.1 Information Quality Criteria. JP 3-13 also introduces the concept of Information Quality Criteria as shown in Figure 2.4.

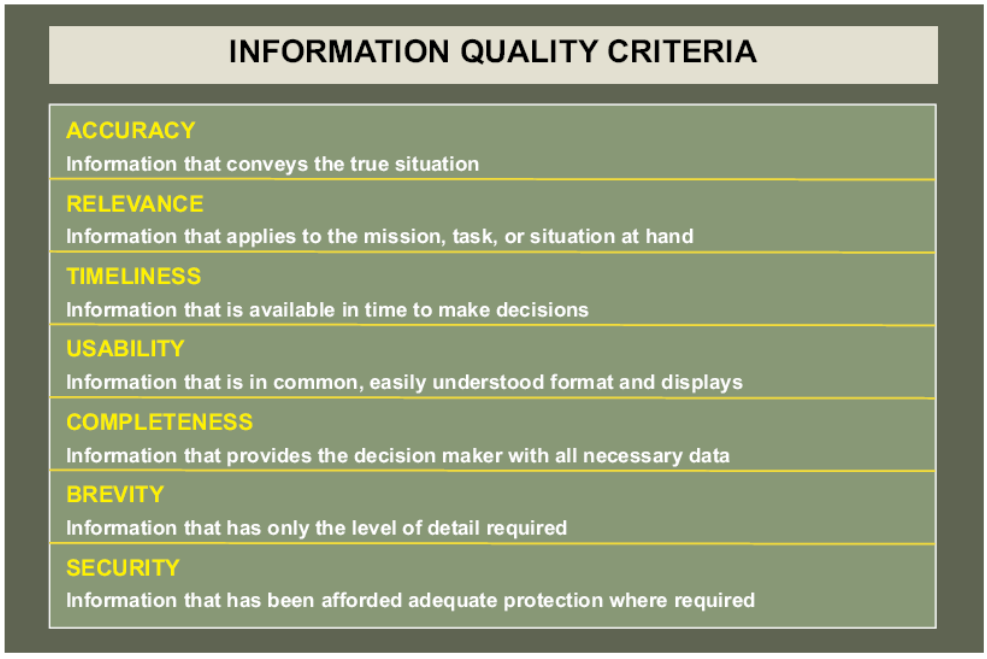

Figure 2.4: Information Operations Criteria [44]

These criteria are used to quantify the value of the information under discussion. Different circumstances require varying applications of the criteria. In a situation where a rapid decision is required, for example, the criteria that may be of the most value are brevity, completeness, accuracy, relevance, and timeliness. Perhaps security and usability are less important as long as the information is available.

On the other hand, if the information is to be stored in a computer database for long term planning purposes, accuracy, relevance, usability, and security might

warrant more attention. In this application timeliness is not a factor as the planning process is looking toward the future and can tolerate some delay. Completeness is similarly not a concern, there will likely be time to incorporate additional pieces of information as they become available at a later date. The information is going into a database so brevity is more than likely not a issue. Storage space is relatively cheap and it is just as easy to store one file as it is five in most applications.

These information quality criteria are useful to the social engineer. The goal of a social engineering operation can be to affect one or more of these criteria in the adversaries information domain. Alternatively, these criteria may be affected tangentially, where they are altered or perceived altered as an unintended consequence of a social engineering operation.

2.6.1.2 Cultural Considerations. JP 3-13 deals with information operations but in the Introduction it mentions cultural considerations as a factor that may shape the information environment.

> *(1) Long-term factors which may shape the information environment include the various ways by which humans: (a) Organize (nation states, tribes, families, etc.). (b) Govern. (c) Interact as groups (culture, sociology, religion, etc.). (d) Are regionally influenced (stability, alliances, economic relationships, etc.). (e) Are technologically advanced.* [44]

As a factor, cultural considerations have a large and long lasting impact on information operations. Cultural considerations have an even larger impact on social engineering due to its inherently personal nature. While it may not be necessary to directly interact with the chosen target, the engineer must still understand what motivates the adversary. In addition, many social engineering techniques involve impersonating someone else, so the culture of the person being impersonated must be considered.

2.6.2 Air Force Doctrine. Working down from the Joint level to the Air Force Level, Air Force Doctrine Document 2-5, *Information Operations* (AFDD 2-5). AFDD 2-5 defines IO as

> *Information operations (IO) are the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own* [21]

There are some subtle differences here from the joint doctrine, most notably the insertion of Influence Operations to cover the joint doctrine capabilities of Military Deception (MILDEC), Psychological Operations (PSYOPS) and Operational Security (OPSEC).

2.6.2.1 Levels of Information Operations. AFDD 2-5 defines three domains of operation. Figure 2.5 presents a graphical representation of these domains and their components.

Network Warfare Operations include the capabilities of Network Attack (NetA), Network Defense (NetD), and Network Warfare Support (NS). NetA is the "employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks" [21].

NetD is the "employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it" [21].

Finally, NS is the "collection and production of network related data for immediate decisions involving NW Ops" [21].

These levels of operations and their specific capabilities are an integral part of Chapter 4 and are presented here as familiarization only.

2.6.2.2 OODA Loop. Additionally, AFDD 2-5 discusses the OODA loop. OODA stands for Observe, Orient, Decide, Act and defines the process an

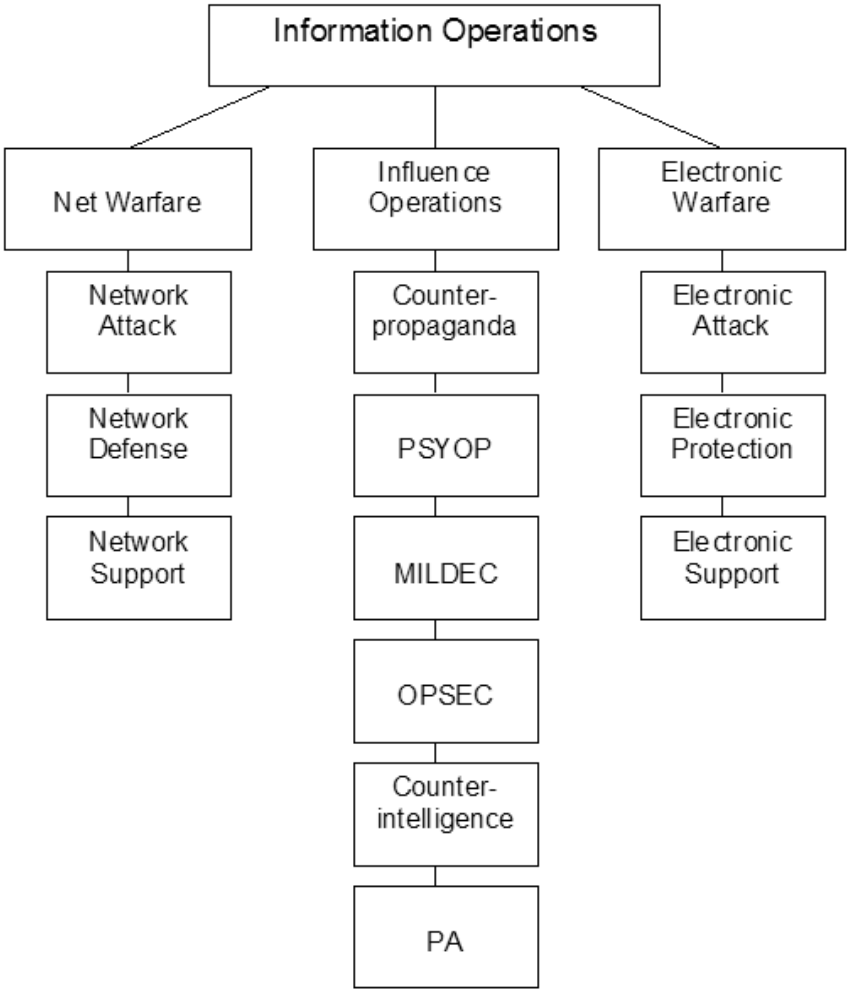

Figure 2.5: Hierarchical Representation of the Components of Information Operations as Outlined in AFDD 2-5 [21]

organization or individual goes through when making decisions and taking actions. It is a continuous process that is described by Figure 2.6

Notice the circular nature of the loop and the various components that influence its composition. Also notice that there is a time spent in each section as well as a time spent transitioning to the next phase; this was an intentional element from Col Boyd. This time is represented by the relative size of each section of the loop. Therefore, an entity with a fast decision process would be said to have a smaller OODA loop than another, slower, entity.

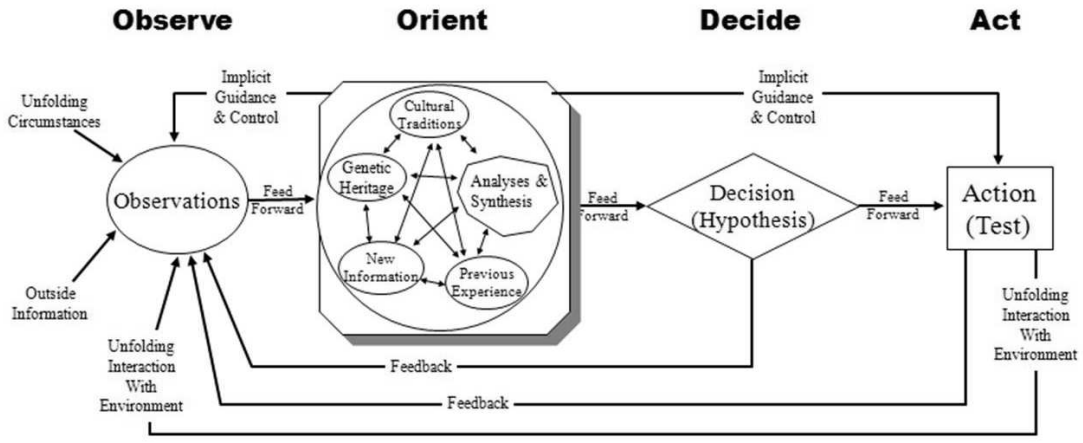

Figure 2.6: Col John Boyd's OODA loop as he sketched it shortly before his death [39]

AFDD 2-5 defines decision superiority as "a relationship between adversary and friendly OODA loop processes" [21]. Therefore, decision superiority is nothing more than the relative size of the Air Forces OODA loop to an adversaries. The greater the disparity in that relationship, the greater the decision superiority.

At this point, it must be noted that AFDD 2-5 concerns itself primarily with the adversary's OODA loop. It mentions the friendly loop but speaks about Information Operations only in regards to how it impacts an adversary's decision process. Social engineering is unique in that it has the ability to affect both friendly and adversary loops at the same time. Information gleaned from a social engineering operation may cause the friendly OODA to accelerate while misinformation planted by the same operation can decelerate the adversary loop.

2.6.2.3 Information Operation Threats. AFDD 2-5 mentions two distinct threats to Information Operations. IO threats can be described as structured or unstructured by looking at their organizational characteristics and purpose [21]. The structured threat could also be considered the nation-state threat as it is well organized, normally with significant financial backing, objectives and means for infiltrating the information environment. However, this threat need not be associated

with a particular nation; wealthy and well organized criminal and terrorist organizations could also fall into this category. This threat type usually has specific long term goals.

The unstructured threat is the opposite. It is usually a small group or an individual with little backing, politically or monetarily, which have a specific goal. Interestingly, a person can be part of both an unstructured and structured threat. Consider the person working for a state-funded Information Warfare unit that independently performs a seemingly random information attack. That person is a member of an organization that poses a structured threat but, through acting on his or her own has also become an unstructured threat. This attribute of an unstructured threat makes identify and prosecuting the adversary particulary difficult as it creates a requirement to confirm state sponsorship of any attack before appropriate retaliatory measures are applied.

2.7 Air Force Pamphlet 14-118

Aerospace Intelligence Preparation of the Battlespace (AIPB) is based on Intelligence Preparation of the Battlefield (IPB) which is a concept shared with the Army and outlined in Army Field Manual 34-130 *Intelligence Preparation of the Battlefield* [7]. While both concepts are similar, Air Force Pamphlet 14-118, *Aerospace Intelligence Preparation of the Battlespace*, (AFPAM 14-118) describes the process specific to the Air Force and is the basis for this research. It places more emphasis on effects than the process outlined by the Army and is more representative of the unique domain in which the Air Force operates. The ability to affect all areas of the battlespace at any given time is what sets the Air Force apart from the other services, a capability only magnified in Cyberspace.

2.7.1 Portions of AIPB. The AIPB process is a four phase spiral planning event shown in Figure 2.7.

Figure 2.7: The Four Pieces of the AIPB Process [20]

The goal is to achieve Predictive Battlespace Awareness (PBA). PBA is the ability for commanders to choose the effects they wish to cause based on how they believe the adversary will react. It is not intended to completely predict the future, rather to provide a better concept of what is likely to happen.

Phase One: Define the Battlespace Environment

The first step in the process seeks to limit the focus to only the battlespace in question. It starts with a definition of the entire area of interest, all things that could potentially be a part of the battlespace. Then the scope is contracted until it only contains the battlespace items of interest in this instance. This is accomplished by marrying the mission with the quantity and quality of information required to accomplish that mission.

Phase Two: Describe the Battlespace effects

The battlespace is the third actor in any conflict, along with friendly and adversary forces, so its effect on the outcome of any conflict must be analyzed. The

primary goal of this phase is to understand how aspects of the battlespace can be exploited to provide operational advantages or disadvantages.

Phase Three: Evaluate the Adversary

This phase develops a comprehensive view of the adversary. Doctrine, centers of gravity, capabilities, tactics, techniques and procedures are all examined in order to establish a complete picture. This phase has the added benefit of forcing the crystallization of perceived adversary capabilities into products that friendly forces can use.

Phase Four: Determine Adversary Courses of Action

This step identifies and prioritizes enemy courses of action (COA), taking into account previously identified centers of gravity. Once identified, these likely COA's can be exploited to further shape the battlespace into a form advantageous to accomplishment of the mission.

2.8 Summary

This section served as an introduction to concepts that factored heavily into this research. They will be revisited and made relevant during the discussion of the research findings. The following chapter discusses the methods used to conduct the research.

III. Methodology

There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind

–Napoleon Bonaparte

This chapter discusses the methodology behind the research conducted. It will introduce and explain the employed methods as well as provide some information as to why the particular methods were selected. These methods include a literature review, grounded theory exploration, and the review of course development material.

This research is primarily based on two separate efforts. The first is a literature review. While providing related background information is common to many research efforts, it is particularly important to this one as very little in the way of formalized research has been accomplished in the area of interest. Therefore, one task was to review as much related material as possible and investigate parallels with other concepts of interest. This comparative review and analysis forms the basis for this research effort. Exploring the identified interrelations identified by this research is our primary contribution.

The second effort follows directly from the first and is the employment of Grounded Theory. Grounded Theory is a subset of Qualitative Research. Its primary distinguishing characteristic is its focus on allowing the theory to evolve from the data in a spiral, evolutionary manner. This method was particularly well suited to this research as the constant ingestion of new data also spawned a near constant evolution as to where social engineering fit in those data.

3.1 Research Questions

The original intent of this thesis was to address the simple question "Where if anywhere, does social engineering fit in the Air Force tool box?" Out of this simple question, several other, more manageable questions arose which this thesis attempts to address.

These are

1. Is Social Engineering a legitimate weapon for the Air Force to consider?
2. Can we demonstrate a link between Social Engineering and Information Operations?
3. Can a Social Engineering attack be planned and measured?
4. What objectives need to be met to train Social Engineers?

Each of these questions generated an avenue of research.

3.2 Grounded Theory

Grounded Theory is a research technique that was originally introduced in 1967 by Barney Glasser and Anselm Strauss [14]. The original audience for the technique was the social sciences community as the emphasis is on generating theory from data through a repetitive reading process.

This theory approaches complex problems, viewing them as whole entities rather than collections of variables [15]. The entities are observed, normally through reading but the entities could also be information sources like interviews or observations, and a general sense of them is established. This sense is further refined through multiple reviews as well as the addition of other relevant information. After the researcher has developed an authoritative feel for the subject matter, key concepts are defined and relationships exposed.

For example, consider the following sentence taken from Joint Publication 3-13

> *Information operations (IO) are integral to the successful execution of military operations*

This sentence reveals the key concepts of INFORMATION OPERATIONS and SUCCESS as well as the relationship between them. Namely that Information Operations is INTEGRAL to success. While seemingly simplistic, it in fact reveals the

rigidity of the Grounded Theory methodology. Rigidity leads to reproducibility which in turn creates credibility.

3.3 Grounded Theory Process

Grounded Theory starts with a situation of interest, the research area. The task of the researcher is to understand what is occurring and why, to uncover relationships that connect the various pieces of the situation. Constant comparison is the key to Grounded Theory. At the start of the process, the researcher compares one data set to another until the beginnings of a theory emerges. This theory is then compared to more data in an effort to refine and perfect that theory. The desired end state is a theory that evolved from the data itself so the theory should describe the data accurately.

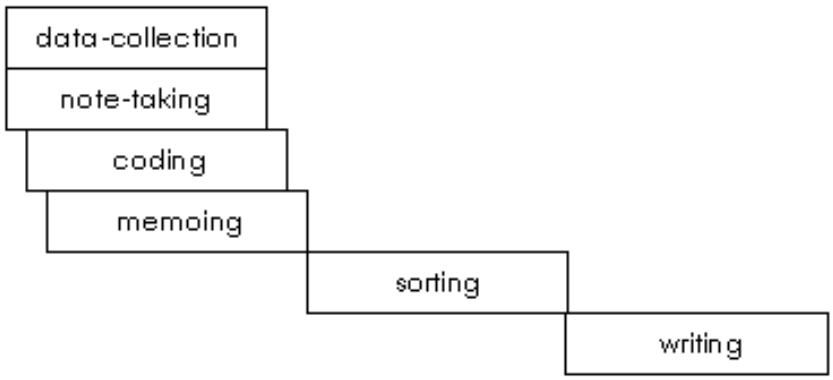

Figure 3.1: Classical View of Grounded Theory Process

What really separates Grounded Theory from other research methodologies is that it is completely emergent. It does not test a hypothesis, it seeks to identify the hypothesis that accounts for the situation *as it currently is.* This concept seems a little free form so to solidify the process, Grounded Theory consists of many steps, some of which occur simultaneously. Theses steps are:

- Data-Collection
- Note-Taking

- Coding
- Memoing
- Sorting
- Writing

Data Collection is the start of the process and also serves as the continuity throughout. The researcher continues to collect data all the way through the process until all areas of interest are saturated with information. As the researcher progresses through the Data Collection process, certain key concepts will emerge that must be kept track of. This is the *Note-Taking* step. With Data Collection continuing, the researcher is able to compare key concepts to each other, looking for similarities or differences that might lead to more data collection. The results of these comparisons are noted in the margins and become the *Coding* portion of the process. As the comparisons continue and their results pile up in the form of coding, theories will emerge that become apparent to the researcher. These theories can be about links between key concepts or about an emerging core concept, a concept that is central to the area of study. The theories are noted down and become the *Memoing* portion of the process. Data Collection continues, codes and memos accumulate. At this point, *Sorting* begins. Sorting is simply matching like information together in whatever way makes the most logical sense, whichever produces the greatest clarity of the theory. The final step, *Writing*, occurs after all categories are saturated with information and sorting is complete [12].

3.3.1 Grounded Theory Application in this Research. Adhering to the principles of Grounded Theory, this research began with Data Collection. Indeed data collection, in the form of interviews and literature review, was the single continuous thread of effort throughout this research. The revised Grounded Theory graphic in Figure 3.2 illustrates the process as it was applied.

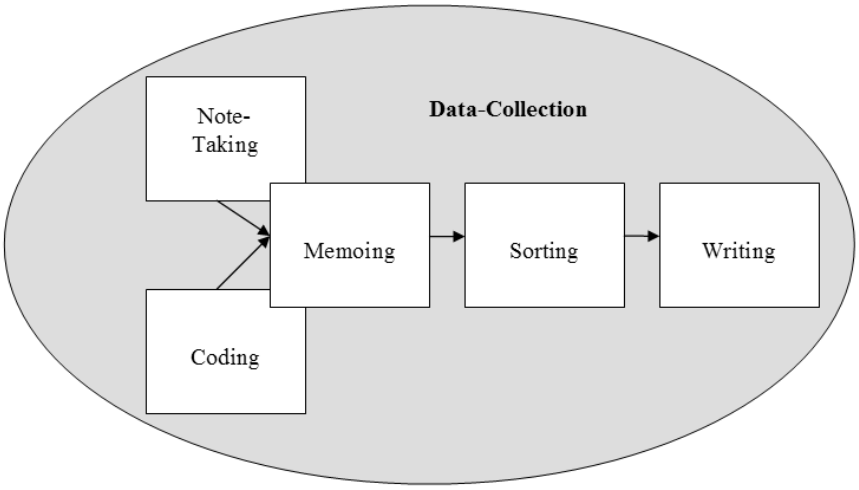

Figure 3.2: Author's Alternative Graphical Representation of the Grounded Theory Process

3.3.2 Legitimacy of Social Engineering. Grounded Theory methodology was applied to discover that social engineering is a concept already resident in Air Force doctrine. As is demonstrated in the following chapter, much of the existing doctrine mentions concepts that can be logically connected to social engineering. These connections are drawn using the iterative nature of the Grounded Theory methodology as well as transitive relations.

Transitive relation in logic is the binary relation between all elements of some set such that if A is related to B and B is related to C then A is related to C [2]. Written in predicate logic, assuming a set X and some relation R, this concept appears as

$$\forall\ a, b, c\ \epsilon\ X,\ \ aRb \wedge bRc \Rightarrow aRc$$

What this means in relation to this research is that if Air Force doctrine uses a specific key concept and that key concept is also a part of social engineering, then Air Force doctrine is expatiating on social engineering in some way.

To draw these logical connectors, specific areas of the doctrine are examined, highlighting key concepts. Furthermore, case studies of social engineering incidents

in the civilian sector provide comparable key concept information. When doctrinal and social engineering concepts are combined, the similarity becomes plain.

3.4 Adaptation Process

The second portion of this research effort is to adapt the existing framework of Intelligence Preparation of the Battlespace for use in planning, executing and measuring the effectiveness of social engineering operations. This effort made heavy use of inductive logic which is defined as "A process of reasoning that moves from specific instances to predict general principles" [1]. Inductive logic uses a relatively small number of observable events to extrapolate laws that apply to the larger system. However, the observations only suggest the law, they do not ensure it. For example, after observing several crows over a certain period of time, an observer might note that the crows are black. Inductive logic could in turn lead the observer to conclude that all crows are black. The conclusion is not guaranteed but is instead supported by observations.

Inductive reasoning is widely used in the area of legal discourse where it is commonly applied in cases of precedence [50]. In this instance, previous rulings that can be demonstratively shown to be similar to the current case are used as foundational pieces. The key portions from that foundation are then applied to the specific case at hand. This also illustrates the another characteristic of inductive reasoning, moving from general observations to specific applications.

Adapting Aerospace Intelligence Preparation of the Battlespace to a framework useful for measuring battle damage caused by social engineering, and indeed all other cyber attacks, is an exercise in inductive reasoning. Areas of this IPB framework that appear to have a direct application to the research are utilized.

3.5 Battle Damage Assessment

The solution suggested for accomplishing battle damage assessment is based on an existing framework, Intelligence Preparation of the Battlespace, which uses an effects-based outlook to accurately predict what an adversary might do or how the battlespace might change. The method attempts to predict the adversary reaction when presented with a particular situation, the goal being to "predict" how the battlespace and the enemy will change based on friendly activities.

Noticing the obvious usefulness of this concept, this research applies this effects based reasoning to cyber attacks, specifically social engineering attacks. However, the concept is approached from the other end of the spectrum. Instead of asking the question "How might an adversary react to this action" as a way of predicting what the battlespace will look like in the future, the same question is posed with an eye towards evaluation. Instead of trying to predict what an adversary will do in order to gain better situational awareness, the process is applied to develop observable indicators that a taken action was effective.

In order to formalize this process, predictive statistical models of behavior were considered. Modeling human behavior, which is a large part of what the proposed Battle Damage Assessment framework attempts to accomplish, is a complex problem of inferring unobservable information from observable actions [51]. In the past and even in the Intelligence Preparation of the Battlespace process this solution is adapted from, prediction of human behavior has been based on a hand-built knowledge databases. These information stores were essentially historical anecdotes of behaviors that precipitated reactions in the subject under question. They relied heavily on both builder input and the predictor' s ability to draw logical parallels between past situations and current events. In addition, these knowledge stores were not scalable and not tolerant of corrupted, distorted, inaccurate or otherwise unintelligible data.

A solution to the high resource demands and low fault tolerance of the knowledge base building method described in Air Force Pamphlet 14-118 is a predictive statistical

model. These models routinely fall into one of two categories, categorized by how they learn: content-based or collaborative [51].

Content-based learning is preferable when past behavior is determined to be a reliable predictor of future behavior. This approach builds a model of future subject actions based on past actions. This approach is specific to an individual (note: individual may mean an individual organization if the behavior of an organization can be accurately characterized over time) and is limited when a new situation is encountered. The heavy reliance on past behavior makes this approach poorly suited to situations when the subject finds him/her self in a new situation with no past behavior to draw on.

Collaborative learning is preferable when it is reasonable to assume that a given subject will behave similarly to other, like-minded subjects in a particular situation. This method is specific to a particular user or group but does not gather all its data from that user or group as content-based learning does. In this way, it is more flexible when encountering new situations as the behavior of the larger group, which the subject is a member, can serve as the historical example in the new situation provided enough data is collected to accurately categorize the subject's membership.

Predictive statistical models were not used in this thesis due to time constraints but are mentioned here as the model was built with the goal of being able to employ one. Therefore, this area is relegated to a potential future research area and is noted as such in Chapter 5.

3.6 Training

Having established the legitimacy of social engineering, the next logical step was to develop the beginnings of a training plan to bring this capability to the Air Force. Towards that end, the final piece of this research is to review the applicable course development guidelines and prepare objectives for training social engineers.

These objectives were created through use of the Grounded Theory process. Key tasks are identified as a starting point. An iterative and expansive literature review is conducted, looking for other key tasks in order to build as complete a list as possible. With the task listing built, the next step is to identify specific skills, knowledge or attitudes that are required in order to perform the tasks. This listing draws heavily on any anecdotal evidence available. Finally, specific objectives are created that, if met, would ensure the trainees possed the desired skills, knowledge, and attitudes.

IV. Results: Doctrine, Battle Damage Assessment Model, and Training

Violence is the first refuge of the incompetent

–Isaac Asimov

This chapter presents and discusses the results of the literature review along with a suggested method for conducting Battle Damage Assessment (BDA) of any social engineering operation and the beginnings of a training program. Since the focus of this research is social engineering, the BDA framework presented has a specific and noticeable bias towards this attack vector. However with little adaptation, suitable applications can be found to almost any cyber based attack. The goal of this literature review is to inductively prove that social engineering is a legitimate attack method for Air Force consideration by showing that Air Force Doctrine already incorporates common elements. This is accomplished by showing that social engineering, while not specifically mentioned in any doctrine, shares many of its key components with the concepts formalized doctrine discusses at length. Through application of the transitive property, the link is drawn between what is currently considered acceptable components of Information Operations and social engineering.

4.1 Social Engineering and the OODA Loop

From an Air Force perspective, no discussion about information processing and decision making is complete without discussing the OODA loop. OODA stands for Observe, Orient, Decide and Act and is the framework for viewing the decision making process originally postulated by Col John Boyd to describe fighter engagements which was then broadened to decision making as a whole [39]. Typical discussion of the OODA loop focuses on "shortening" our own or disrupting or "getting inside the adversary's".

Any doubt about the preeminence of the OODA loop is removed on the fourth page of Air Force Doctrine Document 2-5 (AFDD 2-5), *Information Operations*, which states that bringing the three portions of Information Operations, influence opera-

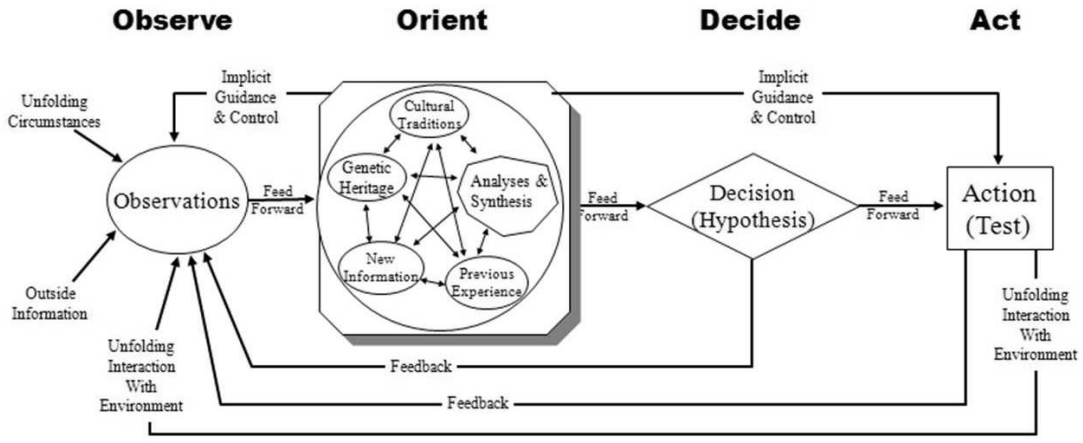

Figure 4.1: Col John Boy'd OODA Loop

tions, electronic warfare operations, and network operations, to bear on the OODA loop is the overarching goal of Information Operations [21]. In other words, the total impact of Information Operations can be viewed as how its three elements create effects on the OODA loop of friendly and adversary forces.

Social engineering has an interesting effect on the OODA loop that other information operations do not. Social engineering has the potential to shorten the OODA loop of friendly forces while simultaneously lengthening the loop of the adversary. As stated earlier, social engineering can take many forms and has potential for combined impact. In a situation where a social engineering campaign has effected a compromise of system access, the OODA loop on the friendly side is shortened by having better insight into what information the adversary holds; that is being better able to Observe and Orient. That access can also be used to inject misinformation into the adversary data stream thereby causing a lengthening of the Observation and Orientation portions of the their loop. Similarly, an unsuccessful social engineering attack can produce these results by engendering mistrust of information in the adversary, causing them to second guess and question information which is available to them. Reaching back to the Information Quality Criteria reviewed in Chapter 2, even an unsuccessful attack can affect the value of information. Friendly forces, having caused

this disruption, would remain unaffected and indeed could benefit as some of these effects may be anticipated.

This unique attribute of social engineering can create a rapid state of decision superiority. AFDD 2-5 defines decision superiority as the relationship between adversary and friendly OODA loops [21]. By degrading one and enhancing the other with the same operation, friendly forces advance towards the desired state of superiority in one step rather than two.

4.2 Influence Operations

AFDD 2-5 defines three domains that influence Information Operations. Figure 4.2 presents a graphical representation of these domains.

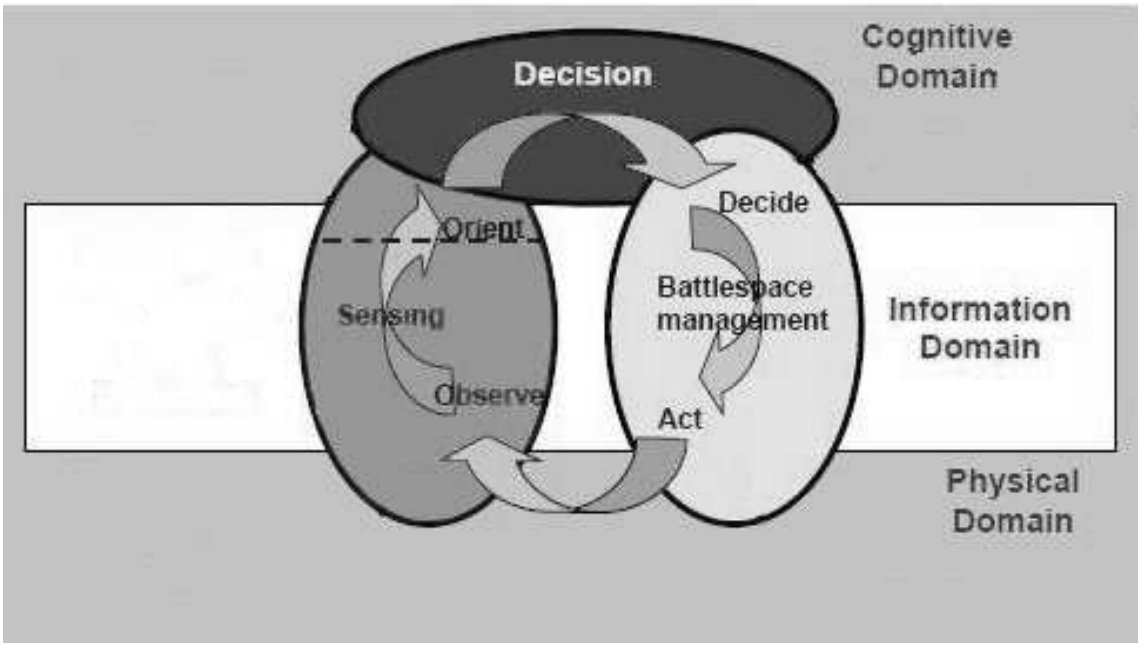

Figure 4.2: Domains of Information Operations [21]

Social engineering has a direct effect on two of these domains, the cognitive and information domains, with the potential for affecting the third. As explained earlier, social engineering operates in the cognitive domain, that is, in the realm of thought. 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 adversary system of interest. Social engineering is flexible enough that an operation conventionally viewed as failed could in fact reveal vital information. 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 connected [41]. 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.

4.3 Social Engineering and the Information Operations Capabilities

The three capabilities, Influence Operations, Electronic Warfare Operations, and Network Operations, that comprise Information Operations must necessarily contain all things considered Information Operations. 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 Information Operations. Therefore, working from the premise that social engineering is in fact a variety of information operation, it must reside in one or more of these capabilities.

The obvious choice is influence operations. As mentioned earlier, social engineers work through methods of persuasion. Persuade and influence are actually synonyms [16] so Influence Operations is the correct place to start. 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 [21]. OPSEC is chiefly concerned with the protection of friendly information rather than the discovery and exploitation of adversary information [44] and therefore will not be used in this discussion. Similarly, CI and Counter Propaganda Operations are primarily defensive, seeking to protect friendly assets against the espionage and intelligence activities of an

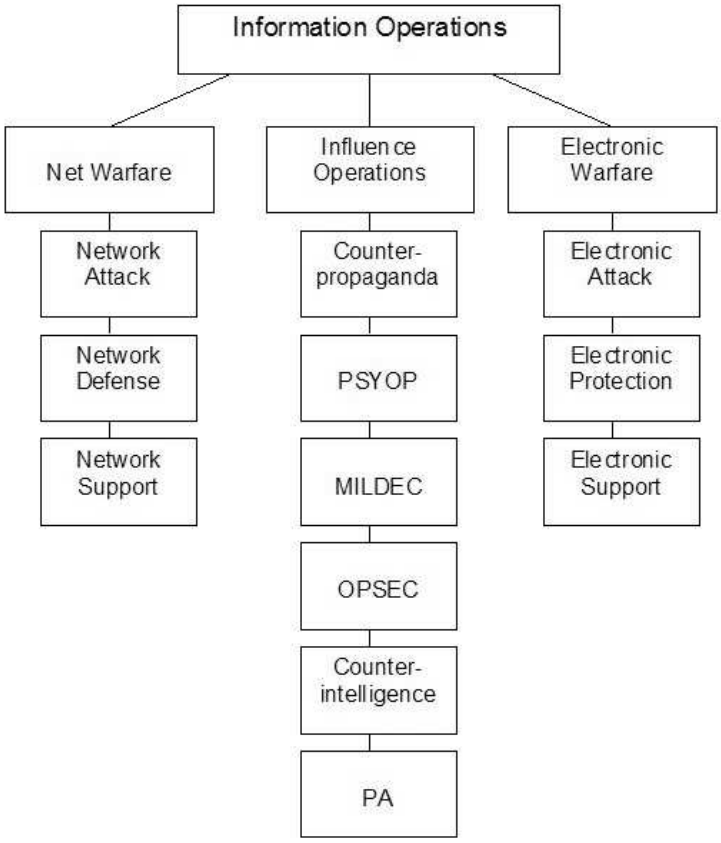

Figure 4.3: Hierarchical representation of the Information Operation capabilities and their associated elements [21]

adversary [21]. 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.

This process of elimination leaves 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 [21]. In contrast to MILDEC which is 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.

4.4 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, key characteristics in PSYOP and MILDEC are connected to techniques used by social engineers.

The PSYOP example in Figure 4.4 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 statements 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.

Figure 4.4: Roughly translates to "This is your first and last warning, the 16th Infantry Division will be bombed tomorrow". Originally dropped during Operation Desert Storm in 1991.

Military deception affects the adversary's decision process by causing them to use faulty information as the basis for their decision cycle [21]. World War II's Operation MINCEMEAT is a famous example of MILDEC [33]. 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 fiancee 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 key concepts 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 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 present 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 as shown in Figure 4.5. 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 [11].

WILLIAM MARTIN
BORN 29TH MARCH 1907
DIED 24TH APRIL 1943

BELOVED SON OF JOHN
GLYNDWR MARTIN AND THE
LATE ANTONIA MARTIN OF
CARDIFF, WALES

DULCE ET DECORUM EST PRO PATRIA MORI

R. I. P.

GLYNDWR MICHAEL
SERVED AS MAJOR
WILLIAM MARTIN, R.M.

Figure 4.5: Picture of the Grave of Major Martin/Glyndwr Michael [47]

These same concepts 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 [32]. 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.

Attention to detail, the second concept and evidenced in the MILDEC example, 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 break-up with a girlfriend [32]. 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 details create the story.

The third concept noted was the adversary was allowed to discover the information on their own, making it appear more valid. Again turning to Kevin Mitnick, this time in his book The Art of Deception, there is 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 [31].

The final concept 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, there is 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 [32]. Figure 4.1 summarizes the discussion of these key concepts.

Table 4.1: Comparison of Influence Operations and Social Engineering Traits

Influence Operation Characteristic	**Social Engineering Technique**
Deception rooted in truth	Knowing the lingo, Name dropping
Commitment to the deception	Dressing the part, Acting as if
Attention to detail	Cold reading, Establishing friendship
Planted information	Masquerading as help desk, Causing catastrophes

Many elements of social engineering appear in Influence Operations under the umbrella of Information Operations. Using the transitive property, if Influence Operations are a part of Information Operations and social engineering shares many similarities with Influence Operations, then social engineering is a part of Information Operations.

4.5 Battle Damage Assessment

One of the keys for any military operation is to be able to assess the effectiveness of that operation after the fact. 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* [42].

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 a desired state of affairs has been achieved, before proceeding to the next set of objectives.

This research noted this need for a method to conduct Battle Damage Assessment (BDA) on social engineering attacks. Through application of the Grounded Theory process, Aerospace Intelligence of the Battlefield emerged as a likely framework. The actual methodology of IPB was described in an earlier chapter so this chapter focuses on the ways in which it is adapted to fit in a BDA role. First, a quick discussion on the reasoning behind why this framework was chosen.

4.6 The Decision to Use AIPB

BDA is essentially a function of expectations. Dropping a bomb, the expectation is that whatever is hit will be destroyed and success is measured by that expectation. If reconnaissance of the target after the attack reveals it to be still intact expectations have not been met and BDA indicates that the item needs to be targeted again. Taken out to its fullest extent, this idea indicates that BDA is nothing more than seeing how well the observed state matches the anticipated state given a set of actions. Extrapolating this concept to the cyber realm and more specifically, social engineering, AIPB formed the basis for a method to plan, execute and evaluate a social engineering attack.

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 [20]. This method of operation is not acceptable given the speed with which information operations take place. While the model is sound, the prescribed method of execution is too cumber-

some to be effective. Therefore, it is streamlined into as few steps as possible while keeping the core intent in place.

4.7 Aerospace Intelligence Preparation of the Battlespace

Interestingly, the AIPB process introduced in AFPAM 14-118 is based on the Army process known simply as Intelligence Preparation of the Battlefield. It may seem redundant to develop a whole new service specific process but this makes sense. Each service views its role in its primary domain differently which necessitates different doctrine to maximize domination of that domain.

For instance, the Navy views their sea power dominance as something they always maintain. They leave port dominating the area in which they operate and as they travel to their final destination, they carry that domination with them [36]. This view is similar to the Army in that the Navy maintains physical control over a certain geographic area, identify and categorizing all actors that come into that area as friendly or hostile, but differs in that the area of this control remains fixed. As the Navy travels, it is constantly taking in new area it needs to control while leaving behind area that it no longer needs to control, like a bubble sliding over the water.

The Army on the other hand generally has to create and enlarge its area of dominance. It arrives in an area of operation, creates dominance over the domain and then pushes forward. The key difference is that their area of control does not remain constant, it increases or decreases depending on the movement of forces. This is due to the logistics tail a land army necessarily has which means they not only have to control new area but they have to maintain control over all areas to their rear [8].

Both of these approaches are clearly different than the way the Air Force views its domain of operations. The Air Force in fact does not focus on control; it focuses on effects although achieving control over the air is a way to ensure that the Air Force can create the effects it desires at will [4].

Given these different methods for viewing the primary domains of operation, and the differing implementations of processes, it follows that cyberspace as a newly defined domain will require its own version of the IPB process, tailored to its specific attributes.

The AIPB process has four components as described in Chapter 2. Likewise, the adapted process contains the same four components although the steps in each component are modified according to the demands of the domain. For review, these components are:

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

4.7.1 Define the Battlespace in the Environment. Joint Publication 3-13 defines cyberspace as "the notional environment in which digitized information is communicated over computer networks" [44]. This encompasses quite a large potential area of operation, so the first step of the 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:

Table 4.2: 4 Steps to Define the Cyber Battlespace Environment

Step	**Title**
1	Analyze the Mission
2	Identify Limits of Operational Area and Determine Possible Second Order Effects
3	Identify Knowledge Gaps and Set Priorities on Resolution
4	Collect Required Information to Complete Process

4.7.1.1 Analyze the Mission. Review higher headquarters and local objectives in order to gain familiarity with 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.

4.7.1.2 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 remain 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 commanders objectives and Rules of Engagement.

4.7.1.3 Identify Knowledge Gaps and Set Priorities on Resolution. In this phase what is and is not known about the Operational Area should become evident. 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 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.

4.7.1.4 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.

4.7.2 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 thorough 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:

Table 4.3: 3 Steps to Describe Battlespace Effects

Step	**Title**
1	Analyze the Physical Enviornment
2	Analyze the Human Dimension
3	Describe Effects of These Two Elements on Friendly and Adversary Operations

4.7.2.1 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 cyberspace 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 the following:

- 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.

4.7.2.2 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, socio-cultural 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 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 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.

4.7.2.3 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.

4.7.3 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, and 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:

Table 4.4: 3 Steps to Evaluate the Adversary

Step	**Title**
1	Identify and Analyze Adversary Centers of Gravity
2	Identify Applicable Cultural Nuances and Asses their Impact
3	Describe Current Adversary Situation

4.7.3.1 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 that a particular organization, be it public or private, derives

strength from. It can be tangible like a monument or a financial district or intangible like freedoms a populace holds dear. In conducting this step, the purpose is to identify exploitable vulnerabilities in the COG where possible. When not possible, the goal is to identify and remain cognizant of the COG throughout this process. It is also possible for a particular course of action to have a center of gravity.

4.7.3.2 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.

4.7.3.3 Describe Current Adversary Situation. This step illuminates the current status of the adversary, matching assets with their locations, purposes and availabilities. Adversary assets particularly important to the accomplishment of the friendly mission, termed 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.

4.7.4 Formulate Mission Execution Plan and Determine Adversary Courses of Action. This solidifies the operational plan and adds an anticipatory element for use in BDA. This step identifies, prioritizes, and weights enemy Courses of Action (COA) taking into account the factors and variables noted in the previous three steps. For social engineering, 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 friendly forces initiate conflict. The second purpose is proactive and looks at all possible adversary COAs, identifying a small subset which are particularly advantageous to friendly forces and working backwards to find actions that would induce the adversary to pursue those COAs. For social engineering, this is a five step process:

Table 4.5: 5 Steps to Formulate Mission Execution Plan and Determine Adversary COA

Step	**Title**
1	Explicitly Identify Assumptions
2	Finalize Mission Plan
3	Identify Adversary Courses of Action and Desired End State
4	Weight COA
5	Identify Required Intelligence Assets Needed to Measure COA

4.7.4.1 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 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.

4.7.4.2 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.

4.7.4.3 Identify Adversary Courses of Action and Desired End State. This brainstorming step identifies all possible adversary COAs in response to the planned mission. There is no concern for the likelihood these COAs will occur, simply

identify as many as are logical given the current circumstances. Consider everything 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.

4.7.4.4 Weight COA. This step takes the remaining, realistic, COAs 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 instance, if the course of action under consideration is the adversary will deploy more troops to a specific location, indicators could be items like reports 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 if this is warranted. Using the same troop movement as an example, if the only indicator currently available is a TTP which states this troop movement will take place, additional value is assigned to this COA if it is believed 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.

4.7.4.5 Identify Required Intelligence Assets Needed to Measure COA. This final step matches the 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 COAs provides expectations and BDA is simply checking expectations against reality. Reconnaissance assets are tasked to observe the expected adversary COA in order to determine success or failure.

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 unpredictability and uncertainty this process is unable to eliminate.

4.8 Training Social Engineers

The third and final piece of this research is to develop a preliminary outline for a program to train social engineers for the Air Force. This answers the final thesis question "What objectives need to be met to train Social Engineers?" The intention is not to provide a comprehensive training system for social engineers, which is beyond both the scope and expertise of this research, but rather to provide guidelines and examples of key elements of a successful training program, forming a starting point for its future creation.

This outline was created in accordance with AFMAN 36-2234 and the Instructional System Development (ISD) process outlined therein. Additionally, Air Force Handbook 36-2235 and Air Education and Training Command Instruction 36-2203 were consulted for supplemental guidance. Use of the ISD process is mandated in Air Force Policy Document 36-22 [5]. The ISD process consists of four interrelated phases. The third and fourth phases of Development and Implementation have been omitted from this research as the goal was to demonstrate viability of the concept rather than present a full training solution. Furthermore, ISD provides a mechanism for determining the need for instruction before beginning preparation of the training. This research operated from the assumption this training is indeed required and so omits that beginning phase of the process.

The first two phases, Analysis and Design, are introduced with a short description in general terms of the key components. Then each component is expanded and focused on the specific task of training social engineers.

4.8.1 Analysis Phase. The analysis phase requires the identification of job performance requirements and ties them to a task list. These are tasks someone

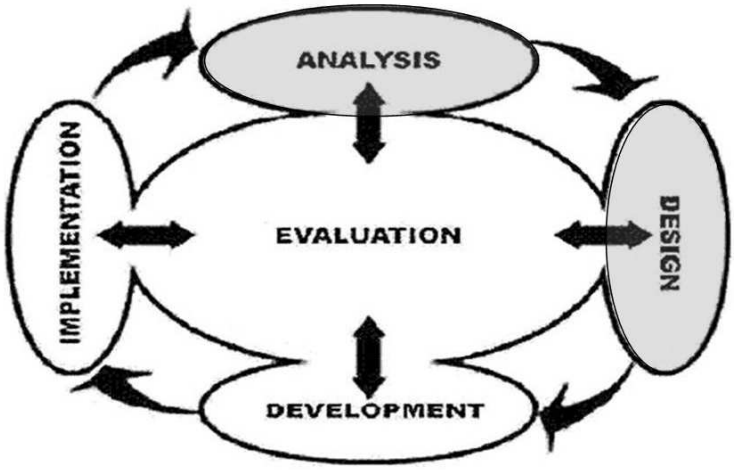

Figure 4.6: ISD process currently used by the Air Force [3]

proficient in the job would be able to accomplish. Ideally, this task list is compared to the skills, knowledge and abilities of the incoming students. However, the development of a method for ascertaining these factors in incoming students is outside the scope of this research. Therefore, it is assumed all students have some fixed level of knowledge, basically aiming training towards bringing the lowest probable level up to acceptable standards.

4.8.1.1 Job Performance Requirements. A student well trained in social engineering will be able to apply social engineering techniques in a given situation. Referring back to the discussion in Chapter 2, those techniques are:

- Trappings of Role
- Credibility
- Altercasting
- Distracting from Systematic Thinking
- Momentum of Compliance
- Desire to Help

- Attribution
- Liking
- Fear
- Reactance

4.8.1.2 Task Listing Development. The most logical way to develop the task listing is to look at the techniques and catalog the tasks required to perform each one individually. Figure 4.7 shows a summarized encapsulation of this effort. In full, this involved implementation of the Grounded Theory process and several pages of notes. It began with reading the descriptions of the various techniques listed in the book in order to gain familiarity with the definitions. Included were examples from Mitnick's previous book The Art of Deception which added further flesh to the bones of the concept. The referenced sections were read in full, getting a more full sense of what specific actions the attacker took in each example. This process of data collection was accompanied at every stage with note taking.

Other sources of information on social engineering were incorporated, noting as was mentioned earlier that many of the technique descriptions given matched some of the techniques provided by Mr. Mitnick. Accounts used included but are not limited to [48] [9] [45] [34] [18] [10] [24] [35] [38]. This literature review created many notes on the relevant elements which were then sorted into the appropriate categories based on the technique used rather than the name given.

This iterative process led to a full understanding of the social engineering techniques as well as what key tasks the social engineer performs when utilizing each technique.

4.8.1.3 Minimum Level of Skills and Knowledge Required to Perform Tasks. Using the task listing in Figure 4.7, the key skills and knowledge required to accomplish the tasks are interpreted. A few skills became immediately apparent. The social engineer should be comfortable talking to people, be comfortable with what

Technique	Tasks
Trappings of Role	- Identify appropriate attire for situation given assumed role - Perform background research (eavesdropping, dumpster diving, internet) - Prepare appropriate background for assumed personality
Credibility	- Identify potentially "soft" targets, those that require assistance - Identify vulnerabilities that will allow disruption in the system - Identify method of exploit based on assisting target remedy the problem
Altercasting	- Read target to establish most suitable role for them - Identify the opposite role and behaviors required to evidence it - Maintain role while remaining flexible to changes in the environment
Distracting from Systematic Thought	- Understand systematic thought, what it is, what causes it, why it is useful - Identify likely organic sources of pressure. Identify artificial sources - Observe target behavior and apply appropriate pressure
Momentum of Compliance	- Become comfortable with small talk, ask more questions that you answer - Plan where to place important question, keeping other questions for after - Learn importance of phrasing question, combining with altercating
Desire to Help	- Understand emotional benefit from helping, how it works and why - Understand what creates or destroys benefit and when to apply it - Identify common, plausible methods for putting target in position to help
Attribution	- Cultivate culturally sensitive awareness of what desirable behavior - Understand target motivations and concerns - Identify plausible avenues of explanation and provide as needed
Liking	- Become comfortable with small talk, ask more questions that you answer - Understand importance of appearance, present best possible look - Identify methods to mirror interests/background/hobbies
Fear	- Comprehend self-referential fear and identify those on whom it works - Identify likely organic sources of fear. Identify artificial sources - Apply sparingly, combining with other methods as necessary
Reactance	- Understand targets motivations, what they consider important - Identify plausible situations that put those important items at risk - Work backwards to create scenario jeopardizing then preserving interests

Figure 4.7: Key Tasks Summarized Based on the Techniques Established by Kevin Mitnick

is typically termed small talk. They need to be able to read the current situation and react to it. They need technical proficiency in order to know what exploits are possible in a given situation. They must demonstrate attention to detail and understand the point of view/culture/background of the target. Table 4.8 outlines these key points and others.

It is apparent after listing the skills and knowledge that there is some redundancy; some items appear in multiple locations in one variation or another. Thus, the skill and knowledge listing is reduced down to 12 components as shown in Figure 4.9. These form the basis for the objectives created as part of the Design Phase.

Technique	Skills and Knowledge
Trappings of Role	- Fashion sense, concern for appearance, attention to detail - Technical skills (internet search), situational awareness (eavesdrop) - Imagination, flexible thinking, broad general knowledge
Credibility	- Identify potentially "soft" targets, those that require assistance - Identify vulnerabilities that will allow disruption in the system - Identify method of exploit based on assisting target remedy the problem
Altercasting	- Read target to establish most suitable role for them - Identify the opposite role and behaviors required to evidence it - Maintain role while remaining flexible to changes in the environment
Distracting from Systematic Thought	- Understand systematic thought, what it is, what causes it, why it is useful - Identify likely organic sources of pressure. Identify artificial sources - Observe target behavior and apply appropriate pressure
Momentum of Compliance	- Become comfortable with small talk, ask more questions that you answer - Plan where to place important question, keeping other questions for after - Learn importance of phrasing question, combining with altercating
Desire to Help	- Understand emotional benefit from helping, how it works and why - Understand what creates or destroys benefit and when to apply it - Identify common, plausible methods for putting target in position to help
Attribution	- Cultivate culturally sensitive awareness of what desirable behavior - Understand target motivations and concerns - Identify plausible avenues of explanation and provide as needed
Liking	- Attentive listening, ability to pay attention, knowledge of social dynamics - Fashion sense, concern for appearance, attention to detail - Broad general knowledge, well read, knowledgeable of current events
Fear	- Self-deprecation, acting, identifying those more susceptible to technique - Cultural knowledge of what is important, what factors will induce fear - Apply sparingly, combining with other methods as necessary
Reactance	- Understand targets motivations, what they consider important - Identify plausible situations that put those important items at risk - Work backwards to create scenario jeopardizing then preserving interests

Figure 4.8: Summarization of Key Skills and Knowledge Based per Technique

4.8.2 Design Phase. The design phase creates a plan of instruction to include selecting the instruction methods and media. Any existing documents are reviewed to determine their continued applicability to the planned instruction. Objectives are solidified and an implementation plan is drafted for rolling out the new curriculum. Note that in this application, literature review played a role in every stage of development. This was a direct result of utilizing the ISD process inside the Grounded Theory research method.

4.8.2.1 Objective Creation. The objectives flow directly from the previously identified key skills and knowledge required in order to adequately perform the task assigned. Specifically,

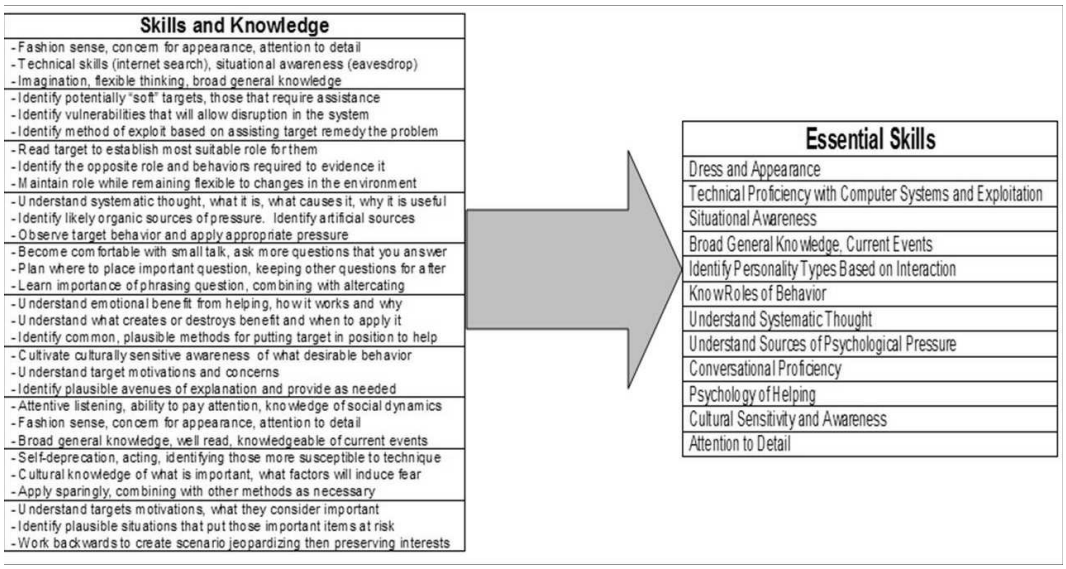

Figure 4.9: Process of Developing Training Plan

> An objective is a precise statement of the learned capability–skills knowledge or attitudes (SKA)– a student is expected to be able to demonstrate, the **condition** under which the SKA is the be exhibited, and the minimum **standard** of acceptable performance [3]

.

Following is a list of the 12 identified essential skills along with sample objectives for each. These objectives meet the criteria referenced above. Note that Understanding Systematic Thought and Sources of Psychological Pressure have been included underneath Knowing Roles of Behavior.

Dress and Appearance

- From any source available to the student, present elements of personal appearance that would be advantageous in the situation assigned by the instructor. At a minimum, the student must present three elements that are appropriate to the assigned situation. These elements may not be reused in further assignments.
- From any print or electronic periodical available, present to the entire class one element of personal dress and appearance per week. For the purposes of this objective, this element may be anything related to current clothing or grooming

trends. Students are encouraged to consider trends in other cultures. The brief will last no longer than 5 minutes.

Technical Proficiency

- Using tools provided by the instructor, exploit the target system within the assigned time frame. Success is determined by system compromise.
- Given the instructor provided scenario, present a plan for exploiting the system in as few steps as possible. Success is determined by system compromise although extra credit may be awarded for brevity.

Situational Awareness

- Tests provided by instructor ask the student to compare two similar images and find as many differences as possible. Passing grade is identifying at least 70% of the dissimilarities.
- Periodic "pop-quizzes" will be administered by the instructor. Without looking around, the student will be asked to identify and describe some item in their immediate area. Success is determined by completeness of the description. Students must be able to perform this task to the instructors satisfaction when asked.

Broad General Knowledge, Current Events

- Using any mainstream print or electronic newspaper available (i.e. CNN, New York Times, Washington Post), instructors will prepare a 10 question quiz for the students. Questions must be related to items of national or international interest including but not limited to politics, current events, weather, sports, and economics. Passing grade is 70%.
- Using any mainstream print or electronic newspaper available (i.e. CNN, New York Times, Washington Post), read at least one article about foreign affairs not covered in class.

Identify Personality Types Based on Interaction

- Using scenarios presented by the instructor, correctly identify at least three personality characteristics in each situation.
- Using the same scenarios, identify at least one event that could change your assessment of the personality type.

Know Roles of Behavior

- Without the use of notes, list all characteristics of systematic thought.
- Without the use of notes, identify sources of psychological pressure.

Conversational Proficiency

- Identify all methods of starting or sustaining a conversation.
- Without use of notes, describe to include examples, methods of mirroring background, interests and hobbies.

Psychology of Helping

- Without using notes, students will identify all psychological benefits related to "helping".
- Without using notes, students will provide at least one situational example for each benefit.

Cultural Sensitivity and Awareness

- Students will read and present one article per week regarding matters of cultural differences.
- Demonstrate knowledge of cultural nuances by correctly matching them with their region of origin.

Attention to Detail

- Briefings presented will follow strict template and time guidelines. Any deviation results in task failure.
- Weekly uniform inspections will be performed.
- Without referring to the knowledge book, students will be able to recite information from the book on the appropriate day.

To reiterate, the objectives above are created to instill the essential skills listed in Figure 4.10. These skills drive the creation of the objectives and are developed in accordance with AFMAN 36-2234.

Essential Skills
Dress and Appearance
Technical Proficiency with Computer Systems and Exploitation
Situational Awareness
Broad General Knowledge, Current Events
Identify Personality Types Based on Interaction
Know Roles of Behavior
Understand Systematic Thought
Understand Sources of Psychological Pressure
Conversational Proficiency
Psychology of Helping
Cultural Sensitivity and Awareness
Attention to Detail

Figure 4.10: 12 Unique Skill/Knowledge Items

4.9 Summary

This chapter reviewed the results of this research. It presented a doctrinally tied argument for the legitimacy of social engineering as a tool for Air Force use. Recognizing the need for metrics to measure effectiveness of any weapon, it then presented a framework for planning and performing BDA of a social engineering operation. Finally, it presented sample objectives, obtained according to Air Force course development guidelines, for training a cadre of social engineers.

V. Conclusions

In war, there is no prize for the runner up

–Gen Omar Bradley

The dominance of US forces in the military arena has created an unexpected area of vulnerability. Placing so much attention on being the best in the realm of conventional warfare has come at the cost of being slow to realize other, less conventional methods for conducting and winning battles. We have robbed Peter to pay Paul. Social engineering is one area where this is evident. It is a proven attack method, used in the corporate world for over twenty years by individuals like Kevin Mitnick and yet it remains largely ignored

5.1 Problem Summary

Social engineering as a multi-disciplinary attack method has received limited study in the academic world. It utilizes psychological pressure points in order to extract information from a computer system. This method of attack bypasses most if not all technology based security measures by turning a trusted system user into an unwitting accomplice. It is cheap, it is easy, it is coming.

Social engineering deserves a seat at the table where discussions about Information Operations are being held; it is consistent with existing doctrine specifically as it relates to practice of military deception and psychological operations. In order to earn that seat, or rather to facilitate a transition into that seat, social engineering must be defined in the framework of current doctrine and methods to implement and measure it must be presented. However, this is large issue and this research merely opens the door to let a small amount of light fall on it.

5.2 Future Research

One of the original research questions was "Can a Social Engineering attack be planned and measured?" This research provides one method for an affirmative answer to that question but refinements remain. One possible avenue of future 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 is expected and yet still indicates a successful operation. Or it may be that the particular adversary does not outwardly display the expected reaction but it is reasonable to expect others in a similar situation to react in the desired 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.

A third area of future research is in expanding the provided training objectives, building them into a full training plan in accordance with the ISD process. Methods of instruction and an implementation plan would be the next logical step.

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

5.3 Limitations

This research is a mental exercise, an attempt to draw links and propose a foundation to continue social engineering growth. As such, no real-world application was attempted and so the framework remains theoretical. Without the presence of a cyber operations force to test theories like this one, there is no way to implement and evaluate its efficacy.

Limitations were also found in the realm of information availability. Classified anecdotes and examples from real world operations were not included in the research. Additionally, there are few reliable published accounts outside of those cited in this text of social engineering events. This is likely due to the victims (usually corporations) of those attacks being unwilling to publicize the event as well as the inability to confirm individual stories of exploits.

Finally, the existence of what could best be termed a stigma against seemingly underhanded tactics like social engineering cannot be ignored. Much like the negative undertones that still cling to the military sniper [37], social engineering has a negative connotation for many. There are several possible reasons for this. It may be the close relation between social engineering and the classic confidence scam as evidenced by the way many authors use the terms interchangeably [23]. Or it may be that those in a position to study it are also those on the receiving end of day to day attempts. Finally, it could be a misconception about the implied integrity of a social engineer.

5.4 Impact

This research demonstrates the importance and relevance of social engineering to the Air Force. It serves as the beginning line in what is hoped will become a widely held discussion about the place social engineering should hold. Through connections to existing doctrine, it has shown that social engineering is reasonably close to tactics we are already using, making it represent a smaller shift in thinking and thus a more palatable option. In fact, Red Teams regularly use social engineering. By providing a rudimentary frame work for planning and evaluating a social engineering operation, which is based on an accepted and proven process, it took the first step in implementing it. It begins the training process by providing the first usable example of what is required to bring this capability to the Air Force.

5.5 Final Thought

Social engineering is a powerful weapon. If the Air Force does not task resources towards harnessing it, it can be certain that an adversary will. That, more than any other argument presented in this thesis, should justify further investigation of offensive social engineering.

Bibliography

1. "Induction". The American Heritage Dictionary of Cultural Literacy, Third Edition.
2. "Transitive Relation", 19 Nov 2007.
3. of the Air Force, Department. *Instructional System Development*. 1993.
4. of the Air Force, Department. *Air Force Basic Doctrine*, volume AFDD 1. Washington DC, November 2003.
5. of the Air Force, Department. *Air Force Military Training*, volume AFPD 36-22. March 2004.
6. of the Air Force, Department. "57th Wing Fact Sheet", Unknown.
7. of the Army, Department. *Intelligence Preparation of the Battlefield*, volume FM 34-130. July 1994.
8. of the Army, Department. *The Army*, volume FM 1. Washington DC, June 2005.
9. Baker, Jason and Belinda Lee. "The Impact of Social Engineering Attacks on Organizations: A Differentiated Study", Decmber 2005.
10. Barrett, Neil. "Penetration testing and social engineering: Hacking the weakest link". *Information Security Technical Report*, 8(4):56–64, 2003. Compilation and indexing terms, Copyright 2006 Elsevier Inc. All rights reserved.
11. BBC. "Operation Mincemeat-The Man Who Never Was", 28 Jan 2005.
12. Borgatti, Steve. "Introduction to Grounded Theory".
13. Cialdini, R. B. and B. J. Sagarin. *Persuasion: Psychological Insights and Perspectives*. Sage Press, Newbury Park, CA, 2005.
14. Coleman, Gary and Rory O'Connor. "Using Grounded Theory to Understand Software Process Improvement: A Sutdy of Irish Software Product Companies". *Information and Software Technology*, 49(6):654–667, June 2007 2007.
15. Dick, Bob. "Grounded Theory: A Thumbnail Sketch", 11 June 2005. This is where the Grounded Theory process picture came from. Looks like a waterfall to the right.
16. Dictionary.com. "Influence", 2006.
17. Downs, Julie S., Mandy B. Holbrook, and Lorrie Faith Cranor. "Decision Strategies and Susceptibility to Phishing". Jul 2006.
18. Duff, Alistair. "Social Engineering in the Information Age". *The Information society*, 21(1):67, -01-01 2005. Doi: pmid:.

19. Fogg, B. J. *Persuasive Technology: Using Computers to Change What we Think and Do*. Morgan Kaufman Publishers, 2003. ISBN 978-1-55860-643-2.

20. Force, Department Air. *Aerospace Intellligence Preperation of the Battlespace*, volume AFPAM 14-118. June 2001.

21. Force, Department Air. *Information Operations*, volume AFDD 2-5. January 2005.

22. Fried, Ina. "Warning Sounded Over 'Flirting Robots"', Dec 2007 2007.

23. Gragg, David. "A Multi-Layer Defense Against Social Engineering". *SANS Insitute Reading Room*, Decmber 2002 2002.

24. Granger, Sarah. "Social Engineering, Part I: Hacker Tactics", December 2001.

25. Granger, Sarah. "Social Engineering Reloaded". *Security Focus*, Mar 2006.

26. Hedden, Mark D. Maj. "Air Force Together We Served (AFTWS) "Military Only" Social Network Website", Jan 2008.

27. Honda. "ASIMO: The Honda Human Robot ASIMO", Unknown Unknown.

28. Huang, Gregory T. "The Talented Mr. Mitnick", Mar 2005.

29. Littman, Jonathan. "In the Mind of "Most Wanted" Hacker, Kevin Mitnick". *Computerworld*, 30(3):87, Jan 15 1996.

30. Lopez, Todd C. Staff Sgt. "8th Air Force to Become New Cyber Command", 3 Nov 2006.

31. Mitnick, Kevin D. and William L. Simon. *The Art of Deception*. Wiley Publishing, 2002. ISBN 0-7645-4280-X.

32. Mitnick, Kevin D. and William L. Simon. *The Art of Intrusion*. Wiley Publishing, 2006. ISBN 978-0-471-78266-7.

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

34. Munro, Ken. "Social engineering". *Infosecurity Today*, 2(3):44, 2005. Compilation and indexing terms, Copyright 2006 Elsevier Inc. All rights reserved.

35. Musthaler, Linda. "How Social Engineering Sinks Security", 9 Oct, 2006 2006. Talks about how SE bypasses many securirty measures in the middle of the article.

36. of the Navy, Department. *Naval Warfare*, volume NPD 1. Washington DC, March 1994.

37. Pegler, Martin. *Out of Nowhere: A History of the Military Sniper*. Osprey Publishing, Oxford, UK, 2004.

38. Peltier, Thomas R. "Social Engineering: Concepts and Solutions". *EDPACS*, 33(8):1, Feb 2006.

39. Richards, Chet. "Boyd's OODA Loop", 12 Aug 2006.

40. Scheeres, J. W., R. F. Mills, and M. R. Grimaila. "Establishing the Human Firewall: Improving Resistance to Social Engineering Attacks". *3rd International Conference on Information Warfare and Security*. April 2008.

41. Schneier, Bruce. "Staged Attack Causes Generator to Self-Destruct", 2 Oct 2007.

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

43. Skarda, B. "Interview with Air Force Members Conducting and Training Social Engineering Techniques As Part of Their Duties", 2007.

44. of Staff, Joint Chiefs. *Information Operations*, volume JP 3-13. 13 Februrary 2006.

45. Thompson, Samuel T. C. "Helping the Hacker? Library Information, Security, and Social Engineering". *Information Technology and Libraries*, 25(4):222, Dec 2006.

46. Unknown. "Security Threats Reach New Levels of Sophistication". *CRN*, (1254):11, 26 Nov 2007.

47. Wikipedia. "Clandestine HUMINT Operational Techniques", Jan 2008.

48. Winkler, Ira S. "Case Study of Indutrial Espionage Through Social Engineering". 306. 22-25 Oct 1996.

49. Winkler, Ira S. and Brian Dealy. "Information Security Technology?...Don't Rely on It: A Case Study in Social Engineering". June.

50. Zeleznikow, John, George Vossos, and Daniel Hunter. "The IKBALS project: Multi-modal reasoing in legal knowledge based systems". *Artificial Intelligence and Law*, 2(3):169–203, Decmber 1993.

51. Zuckerman, Ingrid and David Albrecht. "Predictive Statistical Models for User Modeling". *User Modeling and User-Adapted Interaction*, 11:5, 2001.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
27–03–2008	Master's Thesis	Jun 2006 — Mar 2008

4. TITLE AND SUBTITLE

Operationalizing Offensive Social Engineering for the Air Force

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Bryan Skarda, Maj, USAF

5d. PROJECT NUMBER

07-142

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCO/ENG/08-07

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RHX
Bldg 248 2255 H Street
Wright-Patterson Air Force Base, OH 45433
2Lt Julie Ann Janson
E-mail: julie.janson@WPAFB.AF.MIL Phone: 937-656-6542

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approval for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The focus of this paper is on the use of offensive social engineering in the Air Force. As the Air Force organizes, trains, and equips its new cyber warrior force, it will need to operationalize social engineering principles in order to grow a repeatable, sustainable capability. Towards this end, this paper is organized around three main points. First, establish legitimacy and demonstrate that social engineering is in fact compatible with existing Air Force and Joint military doctrine. This is done with a thorough analysis of doctrine and historical writings about military deception, psychological operations, and related concepts. Second, social engineering arrives in the operational realm by discussing a framework for measuring its effects. A well known process, Aerospace Intelligence Preparation of the Battlespace, is extrapolated and adapted for use in this realm. Finally, requirements for a training plan are developed as a first step in the implementation process.

15. SUBJECT TERMS

social engineering, offensive, doctrine, training, planning, execution, doctrine

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert Mills
U	U	U	UU	85	19b. TELEPHONE NUMBER *(include area code)* (937) 255–3636, ext 4527 robert.mills@afit.edu