CYBER WAR TACTICS OR CLEVER BEHAVIOR: UNDERSTANDING CYBER DECEPTION TECHNIQUES IN THE FIGHT AGAINST CYBER WARFARE

by

Jerome R. Auman

A Capstone Project Submitted to the Faculty of

Utica College

August 2014

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Abstract

The purpose of this capstone project was to examine known cyber deception techniques used by cyber criminals in order to enhance end-user awareness. The focal point of the assessment was to research the origin of distinctive cyber deception tactics and study cyber terrorist behaviors to identify gaps in current cyber deception research and develop counter-deceptive tactics that protect valuable computer and infrastructure networks within the United States. This capstone focused on the basic principles and techniques of cyber deception, the relationship of denial and deception tactics, cyber deception vulnerabilities leading to human biases and impaired thinking, and counter deception principles that leave computer networks in a consistent state of cyber threat vulnerability. A thorough examination of a wide range of literature and publications concluded that there is a disturbing lack of communication between military, government, and civilian organizations in regards to the threat of cyber security. Despite current research that identifies common cyber deception tactics, readers will deduce there is inadequate communication from the U.S. government to its civilian counterparts stressing the need to work together in developing mitigation strategies to counter cyber threats.

Keywords: Cybersecurity, Professor Albert Orbinati, threat, computer, network, cyber criminal.

Table of Contents

Statement of the Problem

Every week there are over forty-thousand blocked intrusion attempts on government and public computer networks worldwide (Ragsdale, 2011, p. 4). Government and civilian networks are habitual victims of daily attacks from hacktivist groups such as organized crime factions, state-sponsored surveillance groups, and sometimes amateurs who indulge in script hacking (Ragsdale, 2011). Cyber terrorism and cyber warfare continues to grow at an alarming rate and is currently regarded as a new type of weapon that holds mass destruction appeal to enemies and adversaries of the United States and its allies around the world. Cyber terrorism is a type of terrorism that is based on Internet attacks, which cause major interruption of computer networks that result in extensive damage to computer infrastructure services by using tools such as malicious viruses, malware, and Denial of Service (DoS) attacks (Matusitz, 2005, p. 137). Cyber warfare is the use of computers and the internet, normally politically motivated, that conducts warfare in cyber space. This type of warfare is typically used to incapacitate and/or gain intelligence on government and civilian computer networks (Post, 1983). The unfortunate ease of online cyber deception is an approach that online attackers use to attack others who wish to avoid detection (PRWeb, 2013).

Today, cyberspace is a front line for incalculable attacks and intrusions by cyber terrorists using cyber deception tactics for innumerable unlawful activities. The purpose of this research is to examine cyber deception techniques used by cyber criminals in order to enhance end-user awareness. This research will specifically address the types of distinct deception tactics that are used and what actions can be taken to mitigate the threat of cyber deception.

Definition of the Problem

Deception serves two functions within cyberspace. The first function serves as security protection for those that need identity protection, such as a government infrastructure or business networks. Thus, deception is a tactic used to help secure valuable information and data. The second function enables an outsider to find weaknesses in a network system as an aid in developing new tactics of deception, which in turn allows a criminal access to commit a crime. Because deception is about behavior, the purpose of it is to serve the deceiver in manipulating a victim into performing a specific behavior. A cyber attacker uses deception as an aid in developing new or improved ruses to obtain something illegally. Deception tactics are typically categorized into the following four security objectives: *Attention*, *Energy*, *Uncertainty*, and *Analysts* (Amoroso, 2011, p. 31-32).

The *attention* of an everyday user or company is susceptible to distraction while completing tasks that may unknowingly manipulate them to reveal personal information, such as in doing research or making a purchase on a fake website. Thus, it is a security objective that revolves around the victim, as opposed to the culprit. E*nergy* is a term used in reference to manipulating the interest of any user by distracting them into putting effort into a bogus asset that appears worthwhile. Users are deceived into believing that a particular website or network can be used for personal gain. Just as an innocent user will unknowingly give credit card information on a sham website, a hacker will attempt to utilize it for self-serving criminal activity.

Uncertainty is the ability to have insight that is built around the actuality of an exposed weakness in a computing system or network of systems. A relationship uncertainty example would show that when a person realizes that someone they are close to has lied to them, they will experience a great deal of uncertainty and betrayal. In the case of computer uncertainty, one assumes they are checking a valid email from a known email address. However, the end user will not have knowledge that this trusted email address could be used in an email phishing fraud attempt, calling into question of a deception uncertainty after the phishing fraud was successful. Lastly, when someone has been lured into a fake website, it provides an opportunity for *analysts* to study certain behaviors and methods used by the unsuspecting party. When an unsuspecting user taps into a sham site, it gives the recipient the chance to analyze by what means they were drawn to it, and thereby exposes the user's vulnerabilities (Amoroso, 2011, p. 32). Just as with the previous three security objectives, this fourth one can benefit both honest and dishonest website owners in creating deceptive tactics that are more effective.

Web applications are among the most frequently attacked surfaces in any organizations network. Conallen (1999), stated, "A web application is a collection of servers, web pages, and other internet resources on any application software that runs in a web browser and is created in a browser-supported programming language "(p. 64). A combination of these application layers is called web-layer applications. These applications are the most porous and the most accepted among cyber hackers (Roberts, 2012, para. 4). Edward Roberts (2012), stated, "There are five reasons why the web-layer applications are so easily penetrated:

- Millions of sites can be scanned for vulnerabilities very quickly and easily. Attacks are circulated and sized up using botnets.
- The entire code, and any vulnerability, are public on a website, providing a potential pathway in obtaining information or infiltrate a network.
- Web layers remain largely undefended within many organizations.
- The level of skill needed to exploit web vulnerabilities is fairly unsophisticated, due to the vast amount of public scripts that are downloaded. Consequently, there are a large number of unsophisticated script kiddies hitting sites without punishment.

- A web application is fixed, or stationary and does not move, and easy to profile for weaknesses" (Roberts, 2012, para.5).

Another type of hacker technique isknown as a *honeypot*, which is a hoax website that is designed to divert the attention of a network user. In a *honeypot*, a fake website is setup to attract and mislead users by impersonating another known or prominent website. It is specifically designed to entrap or trick a user into releasing personal banking or credit card information (McQueen & Boyer, 2009, p. 2), through the use of planting malicious malware or a Trojan horse virus. Due to their exposing and ensnaring capabilities, honey pots are a type of deception that can serve a dual purpose. Honeypots prevent criminal attacks by using very convincing and sophisticated visuals and graphics on a website, which presents it as one that is truly authentic. In turn it lures a cyber criminal away from a genuine sites and secured network, sometimes for an extended period, thereby providing another measure of online security (McQueen et al., 2009). On the other hand, a cyber criminal can deceive a common end user by setting a honey pot trap on a website designed to obtain critical personal financial information or as an aid to install a malicious virus upon opening an email (Amoroso, 2011, p. 31).

Justifying the Problem

The study of cyber crime is crucial in providing insight into preventing cyber victimization, primarily through cyber deception and theft, which is increasingly becoming more common. To understand cyber criminals, a continual study of their behavior must be ongoing. This should include analyzing cyber tactics, deception techniques developed by hackers, and abilities to hack into computer networks in cyberspace.

Cyber adversaries have long grasped deception by deploying tactics, such as illegally installing Trojan horse viruses, malicious codes, botnets, and obtaining personal financial information. Stech, Heckman, Hillard & Ballo (2011), described "Deception is described as any false belief held by an individual, or group of individuals, as the result of sensory information acquired via verbal or non-verbal means, or a misperception of sensory information" (p. 80). Based on this definition, deception may occur without a *deceiver*. Cyber-deception is from the transmission of fake or falsified information on the Internet (Stech et al, 2011). Cyber deception ranges from deceptive online advertising by means of illicit websites or *honeypots*, to criminals falsifying their own identity in order to elicit personal identity valuable information from innocent victims such as social security numbers or bank information. Cyber-deception can involve cyber-espionage in a number of ways: lying in emails, fraudulently using Skype or Voice over Internet Protocol (VoIP) phone conversations, and with fake photos or false advertisements on news outlet websites.

Cyber criminals began utilizing deception tactics when retail stores offered online shopping services through e-commerce. E-commerce was one of the first areas that fraudsters were able to deceive customers by supplying phony payment details or by using false addresses that reroute purchased items to a criminal instead of the customer (Holt & Schell, 2011, p. 69). A recent example of retail store compromise occurred during the 2013 holiday season, when cyber criminals successfully breached retail stores, *i.e.* Target and Neiman Marcus, and stole over one-hundred million personal debit and credit card numbers.

In its various forms, cyber crimes go beyond deception and theft, and are further defined in more distinct terms. Danqua and Longe (2011), listed cyber crimes in the following three categories: "*Cyber-Trespass*, *Cyber-Deceptions and Theft*, *Cyber-Pornography,* and *Cyber violence*" (p. 171). *Cyber-Trespass* involves crossing personal boundaries into another user's domain, through hacking that result in property damage of destruction, such as with DoS attacks and malware viruses. *Cyber-Deceptions and Theft* involves stealing money or property by using deception tactics on the internet through credit card fraud, intellectual property violation, and in some cases, piracy. *Cyber-Pornography* is online activities that breach laws on obscenity and decency of people to include children and adults. Danqua et al. (2011) stated, "*Cyber-Violence* entails causing psychological harm and provoking physical harm against others, therefore violating laws pertaining to the protection of a person" (p. 171). For the purpose of this document, *cyber deception and theft* is the primary focus of this research. Danquah et al. (2011) explained that, "*Cyber-deception and theft* comes in various forms, and falls into six categories: Identity Theft, Spoof or Page Jacking, Credit Card Schemes, General Merchandise and Auctions, Advance Fee Fraud, and email fraud called Phishing" (p. 171-172).

Gaps in Current Research

The intention of a cyber terrorist is to cause harm through deception over the internet in order to advance a specific agenda, *i.e.* social, ideological, religious, political, etc., without the threat of arrest or detection (Longe, & Osofisan, 2011, p.18). Investigation into the September 11, 2001 (9/11) United States attacks revealed that Osama Bin-Laden was aided greatly through the use of computers and technology to further his agenda in attacking the United States. Encrypted detailed plans for hijacking American airplanes were discovered on the laptop computer of Al-Qaeda member Ramzi Yousef. Many of Bin-Laden's aides utilized encrypted e-mails to transmit instructions to Al-Qaeda leader Mohammed Atta (Colarik, 2006, p.35). The 9/11 attacks was the first large-scale terrorist attack that represented a terrorist organizations use and exploitation of information technology.

Since looming concerns with cyber terrorism and online deception is a moderately new concern to our country, it is imperative to understand its cause and effect. Foltz (2004) stated, "Government officials and experts are often heard claiming that the world is unprepared for cyber terrorism; however, other officials and experts state that cyber terrorism does not pose a threat to anyone" (p. 154). Computer security experts do not agree as to what level of threat cyber deception and cyber terrorism pose to our nation's security, both nationally and internationally. Kim Taipale (2007), founder for the Stilwell Center for Advanced Studies in Science and Technology Policy, believed that, "terrorists will use any strategic tool they can" and that "the problem is that there is no united legal organization creating a breach between law-makers and authorities (p. 4). Taipale points out that there has yet to be a defined authority in reporting and dealing with cyber attacks, which poses a question as to whether a cyber attacks falls under domestic or foreign laws. As a result, there are gaps among international legal systems. Proper communication between legal systems of other countries is vital to track down and prosecute illegal cyber hacking. Sharing information about cyber attacks committed by these criminals must be reported in the future. The lack of communication will easily allow unknown illegal cyber threats and consequences of these unlawful actions will continue. These areas need to be further researched in order to develop future mitigation strategies to protect anyone against future cyber attacks.

Cybersecurity professionals are finally publicly acknowledging that the traditional approaches to protecting computer data and information are unsuccessful because the level of threat towards the environment has become incredibly complex (Kruger, 2012). Cyber deception is becoming an integral part of both offensive and defensive cyber operations for cyber criminals and the companies and networks that they attack daily. Computer hackers are increasingly becoming more talented and current network defenses in the United States and abroad have weaker unsustainable defenses. Kruger (2012) stated, "Cybersecurity has become unmanageably complex because the definitions of security do not match the operational environment—and they haven't for a long time" (p. 1). Kruger mentions three areas in which cybersecurity has not adapted to the modern Internet environment and lack the necessary methods towards protecting itself: *perimeters*, *processing capacity*, and *training*.

Perimeters are defined as the ability to control physical access to the building that houses a company's network and terminals. The network perimeter wall, *i.e.* firewall, of a computer network is violated when personal data is illegally accessed. When a wall collapses, all assets and information are in danger of being compromised or stolen. Cyber thieves can easily find this vulnerability and easily use any type of malicious virus or attack to steal valuable information.

Processing capacity refers to the actual power and amount of information and data that a computer's processor can handle when processing work. Computers and mainframes need more processing power and capacity in order to protect and store a company's valuable information and data. The more information and data stored on a network and computer servers, the more processing power that a network needs. In turn, when company information needs to be accessed, the data must be temporarily unprotected for completing a work task such as adding or editing data. A simple solution is to not only provide more processing power to company's mainframe computer, but to provide employees with the ability to use password encrypted logins to all shared drives that only the employees themselves will be able to access with their own created password. For added security purposes, encrypted passwords should be changed every three to six months.

In regards to *training*, all employees should be trained in cyber security on a regular basis. Training is mandatory for network security defenses to be maintained not just at the company hierarchy level, but at the individual level as well. Education is one way to help ensure that the policies and procedures of an organization are being adhered, and a prevention measure for which every employee is responsible (Kruger, 2012, p. 1).

Deception is defined as a fundamental misrepresentation of reality while using a computer. Distortion of reality, or unreality, may be self-induced, accidental, or deliberate (McQueen et al, 2009, p. 2). Such computer deception is usually thought to affect an innocent victim or adversary, but in fact, it affects a larger scope than just those two subject groups. For example, a deliberate deception may be relevant to the defense of control systems when its intention is to put an adversary at a disadvantage. Thus, there is no definitive definition of deception. Some are ethically neutral, while others are not, which leads to another area of focus: mitigation defense strategies using deception taxonomies.

Varieties of taxonomies have been proposed in regards to using mitigation deception and defensive techniques against cyber attackers. Deception taxonomies involve showing false information, through a deception, and using deceptive techniques to disguise a cyber criminal’s behavior or a fraudulent website. These taxonomies are façades used to disguise legitimate websites, etc. Some examples include *masking, repackaging, dazzling, mimicking, inventing,* and *decoying* websites or emails in cyber space (Bell & Whaley, 1991). For the purpose of this assessment, dissimulation taxonomies are the focus. Dissimulation taxonomy consists of the first three deception taxonomies that are used to protect against the actions of online attackers: *masking*, *repackaging*, and *dazzling* (McQueen et al, 2009, p. 2).

The deception technique called *masking* takes something real or significant, such as a website on the internet or the code on a computer’s hard drive, and alters it in a way that makes the original source appear unchanged to the eye of an attacker. After the masking is complete, the relevant object, *i.e.* hard drive, website code, will be invisible or blend into the environment and appear insignificant. Another example of masking is to insert a malicious program, or virus, as white space in a relatively benign looking program, such as JavaScript (Kolisar, 2008, pp. 4-11). Masking can also appear in something common, such as private text message, in where the deception itself can be embedded as white font in the spaces between words of an apparently innocent email message sent to a group or individual (McQueen et al, 2009, p. 2).

Repackaging is a dissimulation technique that consists of the ability to hide a real computer code, such as the code for JavaScript, and make it appear as something it is not. An email phishing attack may make use of a very harmless, official, or friendly looking subject line in a user's email in an attempt to persuade the email receiver to open a message. Once the email is open, the phishing attack could contain a Trojan or malicious virus in it that is unknowingly activated by the recipient. Similar to a phishing attack is an email containing an anonym-zing remailer, which is used to replace a person's e-mail identity with the identity of someone else's personal email. The recipient of an anomyzing remailer unknowingly provides the means and information to the attacker simply by opening an email message (McQueen et al, 2009, p. 2).

The mitigation technique *dazzling* masks false codes as a method of defense. It conceals real information on a person's computer or business network by making applicable objects and the server's location identification to appear unclear. This in turn confuses an adversary about the true nature of both the information and location of the victim's server or computer. One dazzling example is the ability to use a common randomization and encryption technique that deliberately takes of identifying elements of the victim's data location to make them appear in another Internet Protocol (IP) location related to the objective. This is referred to as data obfuscation, which is a data masking process of hiding original data with random characters or data (McQueen et al, 2009). Another dazzling example is to use an address obfuscation that randomizes the location of victim program data and code. By using random codes of data, an adversary may be confused and discouraged enough to reconsider attacking the victim at hand (Bhatkar, DuVarney, Sekar, 2003, p. 1).

Defining the Audience

The benefits of examining the practices and uses of cyber deception by cyber criminals, as well as the specific tactics used, serve to increase the safety and security of a country's infrastructure. Information gained from the study of cyber deception is invaluable towards identifying the need for better cyber protection and defined risk mitigation assessment strategies. The parameter for which this area of security reaches ranges from common everyday computer end-users, to CEOs of all types of businesses, government and federal entities, and all branches of the military. Ultimately, every individual or defined group of various sizes are just some of a larger population that will benefit from the need for better cyber protection and defined risk mitigation assessment strategies.

Literature Review

History of Deception

In 1943, during the height of World War II, the British Naval Intelligence (BNI) was tasked to develop a deceptive tactic, so Allied troops could move into Sicily, with little to no resistance from highly trained German and Italian soldiers, who were well-prepared for an onslaught (Bodmer, Kilger, Carpenter, & Jones, 2012, p. 31). In response to the BNI request, a very promising British staff officer named Ian Fleming created a ruse based upon an old spy novel. *Operation Mincemeat* was the plot name of this operation. The plot of the operation revolved around a fictitious British Officer name Major Martin, to whom false maps and documents were given, which contained mock plans for an attack by Allied troops against the Axis nations from Greece instead of Italy. Once the documents were obtained by the Germans and believed to be authentic, Hitler immediately relocates one of the German fortification divisions from Italy to Greece to prepare for a fabricated attack (Bodmer et al., 2012, p. 31). The false documents, a fabricated story and a fake army officer are examples of excellent deception tactics used in a specific way to trick the Axis powers, which resulted in an easier victory in Italy for the Allies.

During World War II (WWII), both the Axis and Allied powers used deception on a daily basis to try to gain the upper hand on the outcome of the war. Each side took guidance from two of the most famous historical war books on doctrine and strategies written centuries ago, which are still honored today: *The Art of War* written by Chinese General Sun Tzu and *On War* written by *Carl von Clausewitz*, a famous German (Prussian) general and military theorist (Bodmer et al., 2012, p. 37). Sun Tzu (544- 496 BC) was made famous during the Chinese Dynasty Warring years while Clausewitz (1780-1831) served during the Rhine Campaigns of the French Revolution (1793-1794) and served during the Napoleonic Wars (1806-1815). While both authors have some opposing views on war strategy, Tzu and Clausewitz are considered military scholars during their lifetime and continue to hold worldwide respect within their field.

Four Basic Principles of Deception

Practically all living creatures are prey to another species or some form of immoral human or animal intention. Thus, survival of all creatures depends on some collection of physical traits and intelligence (Bodmer et al., 2012, p. xvi). Bodmer et al. (2012) stated, "There are four basic rules of deception that apply to every being in order to survive. The four rules are:

- Do not be seen—hide
- If one is seen, then run away
- Counterattack only if there is no option
- When none of the preceding three is an alternative, use intelligence and resort to deception by stalling to resist the oncoming attack" (p. xvi).

The unique quality of deception lies in its principal purpose, which is to affect only the behavior of the person being deceived. Animals in the wild use survival deception techniques to protect themselves from predators. For example, a possum will fake its own death to keep predators away, chameleons will use the ability to change is color by camouflaging to blend into the background of whatever object it is on, and some ground nesting birds will lay speckled eggs of an undetermined color to trick bird-eating predators. Cyber criminals, however, use technology tricks and gimmicks to deceive and fool any end user as a potential target. Thus, the nature of criminal cyber deception is not for personal protection but for selfish gain.

These four basic deception rules lead to the core of what denial is, but in order to understand denial's place one must understand all four basic principles of deception. These four basic principles are *truth, denial, deceit* and *misdirection*. Bruce et al. (2008) stated, "*Truth* is needed in all deception and is the starting point of what is true which in contrast is exploited. *Denial* is the ability to deny targets admittance in selective aspects of truths and is a prerequisite for deception. *Deceit* is the requirement to obtain and utilize deception and *misdirection* is the action that a deception takes if a target is manipulated successfully" (p. 126).

When applying traditional deception techniques to criminal cyber activity, one must imagine the incoming of soldiers, i.e. botnet virus or malware data packet trying to infiltrate a computer network. Imagine this network being surrounded enemy soldiers aka malicious data packets. A computer network includes a perimeter, internal systems, and applications. This perimeter acts like a wall of allied soldiers making a stand against an enemy preventing the enemy from getting past the perimeter into their encampment. However, in this example a perimeter in cyber is like a firewall on a network keeping out malicious data traffic from entering in the network and keeping any malicious data from leaving the network as well.

If a network does not have protection set up properly with firewalls, and installed software for antivirus and malware protection, then an unsuspecting end user can easily be deceived into falling for any variety of cyber criminal frauds disclosing valuable data or information. It is easier for government and business networks to protect their own territory of computers, rather than try to protect it from unknown threats coming in (Bodmer et al., 2012). Deception is a powerful tool, especially for criminals in the cyber world. It is much easier to use deception in cyber space because an adversary can enter through a backdoor of networks and thereby be undetectable or cloaked. In addition, it is easier to use a remote location while an adversary is hiding behind a computer anywhere in the world thus not needing access to the actual physical organization (Bodmer et al., 2012).

Deception, defined as "the act of being deceived" or the "state of deception", is an embedded part of human behavior. The art of deception is carried out in a wide range of settings, ranging from military combat to everyday advertisements on television. Deception is also one of the most common techniques used by cyber hackers and criminals in cyberspace. Bodmer et al. (2012) stated, “Deception is a technique whereby we mislead people in to believing information that prompts them to behave in a way that is favorable to us” (p. 24). While deception may be beneficial for the one who created it, a deception must also protect the source of its identity and the true character of its ruse (Bodmer et al., 2012). Because technology and computers have become such an integrated part of life, deception is also part of the cyber world.

Why Use Deception?

The *Art of War*, written by General Sun Tzu during the Zhou Dynasty of China (475-221BC), is regarded as the oldest and most revered military strategy book. Tzu served with the Chinese government, in which he shared his knowledge and experience by writing “If you know your enemy and know yourself, you will not be defeated in a hundred battles” (Giles, translation, p.52). Like most modern day military strategists, Tzu believed that knowledge about the enemy is power, which in turn formed the map for victory in battle. He expanded upon this belief by saying that the most vital weapon of combat warfare was to obtain information about the adversary. These same principles still stand today, and apply to physical and cyber adversaries. Obtaining information about an opponent is the strategic key to getting the result for both sides. (Bodmer et al., 2012, p. 35).

Bodmer et al. (2012) stated, “General Tzu deduced that “All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive. Hold out baits to entice the enemy. Feign disorder and crush him” (p.38). Tzu was aware of the ability to ascertain control and command of the information environment wholly, would aid in controlling the decisions of the enemy and the outcome of a war. When

Tzu's deceptions worked properly, his troops were able to gain control of all adversaries even without employing armed conflict from his armies. The same principle is true for cyber criminals when developing enticing phishing emails or a DoS malware botnet. Once the enemy has obtained information about and knows the end-user, deception is very likely to result in victory. If an unsuspecting user has no idea that an email he or she is reading is false, then the criminal is reasonably assured a victory in cyberspace.

Cyber Deception MILDEC Principles

Now that the four basic deception principles have been explained, it is also important to know that the military and government entities typically use six military principles that are similar to the first four basic ones. By using the six MILDEC principles, *focus, objective, centralized planning, security, integration,* and *timeliness* in conjunction with the first four, will ensure civilian and government agencies alike will encompass all ten making practically invincible deception tactics against cyber attackers in which will be successful at any company level.

One highly regarded literary source that provides a complete comprehension of deception and deceptive techniques is a military publication entitled *Joint Publication 3-13.4, Military Deception*. Military Deception (MILDEC) is one of the many foundations of Information Operations, sometimes referred to as Information Warfare, who developed six techniques in *Joint Publication 3-13.4, Military Deception*, "Executive Summary" in January 2012 (Joint Chiefs of Staff, 2012, pp. vii-ix). The six MILDEC principles are *focus, objective, centralized planning, security, timeliness, and integration* (Bodmer et al., 2012, p. 25).

Six MILDEC principles of cyber deception. In MILDEC, *focus* is the part of taking action towards finding the cyber criminal by setting the deception trap (i.e., *honeynet*) in which to locate the source or Internet Protocol (IP) address in which the cyber hacker resides. A *honeynet* is a network system setup as a decoy to resemble a real system setup as an early warning system for malicious activity and for studying cyber criminal behavior (Bodmer et al., 2012, p. 208). The primary goal of *focus* is to find the criminal who is responsible for victimizing and cheating innocent end user recipients. An adversary's original exploitations against the victims are the target of the *focus* technique. In a deception, the attacker is someone who provides false information, distributes assets, or oversees a criminal cyber operation. The decisive purpose in the focus is to have the target commit a criminal act, by diffusing, wasting, or improperly spending stolen resources or assets on a deception trap aka *honeynet*. When such a criminal act occurs, identifying and attacking this primary person is a positive and legitimate worth of the time and effort put towards catching the criminal (Bodmer et al., 2012, p. 25).

Another part of responding to deception is called *objective*, in which the adversary must be baited to take action to commit a crime by carrying out an illegal activity. The objective's goal will not be met if the criminal has not followed through with a crime in cyber space. For example, an adversary browses a database server looking for an open email relay or open proxy server in order to send out spam email. However, system administrators of this company's network have created a *honeyclient* program that can be arranged to search websites for malicious content and client-side exploits, which in turn can alert security administrators of potential malicious websites. This is an excellent way to set up deception traps to track down IP addresses, proxy and web logs, known partner sites and organizations' internal and external sites (Bodmer et al., 2012, p. 208). This would be a great story, however if no cyber attacker knows of this company or has an awareness of some suspicious looking activity on the database server, then it is unlikely this *honeyclient* trap will succeed. In the cyber world, a deception must be designed to interest an adversary and the objective of a deception must attract him or her to come visit a ruse database for website and lead them to being captured (JCF, 2012, p. ix).

Bodmer et al. (2012) stated, "*Centralized planning* within MILDEC operations should be coordinated and synchronized with all other deceptions to present a seamless story across the organization" (p. 26). In order to achieve a successful unity of effort by an organization, such as a government entity or private company, an organization must be attentive to, and not overlook, even the slightest detail within its operation. Successful capture of highly skilled criminals is one of the most important accomplishments of deception. Continued success in preventing and catching cyber hacks within a certain network, ensures the trust and support of outsiders both personally and professionally. An institution achieves centralized planning within it provides security within its computer network system (Bodmer et al., 2012, p.26).

Security of a company's deception setup is critical for its success. Any knowledge by loyal employees about attempted or successful cyber attacks to the network they are defending will be disclosed to the company. In retrospect, no knowledge of any attack must be made public in order to sustain the trust of its customers and supporters. Public assurance will guarantee the safety of the company and make criminals unaware of their lack of success. The system administrators who set up the spam honeypot in the previous example will not let information be known to the public or other colleagues that a deception trap even exist while the trap poses as a real database. If somehow in information has been leaked to the public that a certain business is intentionally setting up traps to track cyber criminals, then the act of deceiving the hacker has failed. It is not a deception if other employees or customers of this company leaks out this valuable security information (Bodmer et al., 2012, p. 26). Practicing Operations Security (OPSEC) is imperative when protecting a company's reputation and confidence. Even the slightest error can be detrimental to the company and the deception that has been created to lure attackers (JCF, 2012, p. ix).

Timeliness is the process of planning a deception operation that is outlined in detail, which is then practiced and rehearsed to a high level of precision before being implemented. For example, a network system may be created as a ruse for the sole purpose of trapping a hacker by allowing them to obtain, or “steal”, information. If the location about classified data or information about the deception is revealed before the trap is set, then the threat may move quickly away acting on new intelligence it may have gathered on this system. The timeliness of this entrapment includes the confidentiality of the parties involved with intimate knowledge to foresee all obstacles, as well as presenting the deception operation at the most opportune time to ensure the highest level of success (Bodmer et al., 2012, p. 27).

Bodmer et al. (2012) stated, “*Integration* simply means to fully integrate each deception with all operations that it is supporting, including other deceptions” (p.25). Therefore, no deception set up should stand single-handedly by itself. If there is more than one deception set up for the ruse, then they should be organized together based facts and hard work. In other words, if honeypots are setup within an organization in a corner of the network without any activity, then the deception trap has no function (Bodmer et al., 2012, pp. 27-28). In order for a trap to be effective, systems administrators of a business network must organize methods that should leave traces of the deception trap’s existence across the company’s network, even with sub contracting networks that are employed. Leaving traces builds on important consistency to an attacker, who may perceive this his spam email is working effectively against the company while investigators use this as evidence when building a case. If an organization, group, or business, abides by the six MILDEC principles of the deception as outlined in the MILDEC publication *Joint Publication 3-13.4, Military Deception*, then preparation, coordination with other departments while using *focus, objective, centralized planning, security, integration,* and *timeliness* will be successful at any organizational level.

Denial

While deception refers to the misuse of information and intelligence collection, there is another action, or behavior, that compliments it and causes denial be even more effective, this is *denial*. Denial is also one of the four principles of deception. More importantly, denial is considered the root or foundation of deception (Bruce et al., 2008, p. 124). You cannot have deception without the use of deniability. However, in a technical or cyber sense, denial refers to the activities and programs designed to eliminate, take away, or defuse the effectiveness of information or intelligence collection (Bruce & Bennett, 2008, p. 123). An example of denial is often used in DoS attacks committed by cyber hackers to overwhelm a website, thereby denying availability to outside users, and granting internal access to the hacker. The packets of information sent from hackers during a DoS attack can be simultaneously timed to overwhelm a targeted network and the computers on it, rendering it unavailable for use.

Denial of information collection is a key ingredient to its deception partner. Denial has the ability to neutralize a collection of information, forcing an end user or attacker to either move to another network or victim respectively, or stop the behavior that is being committed such as a criminal act by a hacker or an end user being denied a false purchase on a website (Bruce et al., 2008, p.123). Denial and deception (D & D) tactics have plagued the U.S. Intelligence community and intelligence analysts for decades, i.e. the surprise military attack by Japan in 1941 on Pearl Harbor. The breakdown to warn of covert emplacements of Soviet missiles in Cuba in 1962 leading to the Bay of Pigs Invasion is one. The failure to warn U.S. Policymakers of impending nuclear tests in India in 1995 in the already volatile region of south Asia was a huge disappointment. Most recently, the U.S. government wide systemic failure of U.S. Analysts not reporting of multiple warnings that Osama Bin Laden and Al-Qaeda were planning to hi-jack several jet airliners and crash them into the World Trade Centers and Washington, D.C. on September 11, 2001 (Bruce et al.,2008, p. 192-200).

Bruce & Bennett (2008) stated, “Effective D&D has the potential to significantly degrade U.S. Intelligence capabilities by attacking vulnerabilities in collection and analysis” (p.123). The above examples are clear ways that other countries have used D&D over the years to achieve and gain information from the United States intelligence communities. For the U.S. to have the ability to defend or protect our citizens, our cyber security and intelligence experts must always be trained and updated with the newest technology and software and be educated on the newest attacks and what cyber criminals are doing on regular basis.

Computer Deception Vulnerabilities

Vulnerabilities in any type of deception are only human nature. Some people are more susceptible to deceit by others, enemies and friends, on a daily basis. Simply put, the human brain has its own limitations. Eventually everyone will fall for some type of deception in childhood and adulthood (Yuill, Denning, & Deer, 2007). Sadly, fraud artist and scammers exploit the human mind’s vulnerabilities every day on the internet. Not only is the average computer user vulnerable, but also the cyber criminal as well. Law enforcement has been using deceptive tactics against adversaries for years for the purposes of cyber security of networks and intelligence collection on cyber hackers. Yuill et al., (2007) stated, “Military, intelligence, and law enforcement communities have long used computer deception techniques for operational security, intelligence gathering on adversaries, and covert operations against organized cyber crime ” (p. 1). In modern times, law enforcement communities has discovered that these deception tactics have also offered a promising means for strengthening computer security through methods such as *honeypots, honeynets* and *honeyfiles* which will be described later. Psychological deception against hackers is one of the many ways that our intelligence and law enforcement communities are starting to use counter deceptive mitigation strategies to defend against cyber crime.

Honeyfiles were developed for the military as a intrusion testing system deployed originally on a *honeynet.* (Yuill, Zappe, Denning & Feer, 2004, p. 1) These honeyfiles were placed on the honeynet to observe cyber criminal behavior on the internet. Honeyfiles were made to find the biases, assumptions and misperceptions made by intelligence analysts and system security administrators of computer networks (p. 1). Yuill et al. (2004) stated, “Specifically, a honeyfile is a bait file that is intended for hackers to open, and after opening, an alarm is set off alerting cyber security administrators of the network” (p. 1). Yuill also specifies that honeyfiles can be used to detect unauthorized access to computers whose file space is mounted from a file server (p. 1). Standard industry practice for large organizations is to store user and application data on the file servers. By putting the file on the server from which the alarm is based, honeyfiles provide an extra security measure for a user’s file servers and clients (p. 1).

The following phrase is part of a famous quote by President Lincoln, in which he said “...and you can fool all of the people some of the time...” (Bell & Whaley, 1991, p. 97). Lincoln knew that to deceive, and to be deceived, is an inherent part of human nature and a life action that is to be expected. Being vulnerable to deception is a common state that all persons find themselves in at one time or another. Although some people are more susceptible to being deceived than others, eventually everyone is affected by a deceitful act intentionally perpetrated by someone else. Because human nature is not perfect, and therefore has weaknesses and blind spots (Yuill, Denning, & Feer, 2007, p. 1), fraud artists and scammers exploit the human mind's vulnerabilities on a daily basis over the internet. Vulnerability to deception is a standard human reaction because it holds basic limitations within the human psyche (Lambert, 1987, p. 15). Every man, woman, and child is unique in that each person holds their own individual perspective of reality, which is based on every persons unique physiological and psychological makeup.

On the other hand, if the average computer user is vulnerable to deception, so are cyber criminals. Law enforcement has been using deceptive tactics against adversaries for years, which includes the security of networks and intelligence collection against cyber hackers. Yuill et al. (2007) stated, "Military, intelligence, and law enforcement communities have long used computer deception techniques for operational security, intelligence gathering on adversaries, and covert operations against organized cyber crime" (p. 1). In modern times, law enforcement communities have discovered that deception tactics offer a promising means for strengthening computer security through different methods, i.e. such as honeypots. Using psychological deception against hackers is one way that our intelligence and law enforcement communities are utilizing counter deceptive mitigation strategies to defend against cyber crime. The vulnerabilities, to which people are susceptible, fall into two expansive categories: biases and impaired thinking (Yuill et al., 2007, p. 1).

Biases

Yuill et al. (2007) stated, "Biases are human tendencies of erroneous cognition or erroneous reasoning" (p. 1). Biases fall into two categories: perceptual and cognitive biases. A perceptual bias is the human inclination to perceive and have insight into things that are predictable in life. Cognitive bias is the human tendency to form general stereotypes without enough information. One example of cognitive bias is called *target fixation*. This fixation is when intelligence analysts may fixate on one hypothesis, looking only at evidence that is consistent with their preconceptions and ignoring other relevant views. Porch & Wirtz (2002) observed, on September 11, 2001 that “U.S. intelligence agencies already knew individually that al-Qaeda actions usually involve multiple, near-simultaneous attacks” however, “ the FBI, NSA and other intelligence agencies did not assimilate piecemeal information on oddly behaving foreign flight-training students into this context” (pp. 3-4). This was clearly an intelligence breakdown among the agencies. The breakdown happened partially because there was poor information sharing among analysts from other U.S. intelligence agencies. On the day of the hijackings, not a single analyst connected the multiple hijackings with the multiple-attack signature of al-Qaeda, much less noticed that foreign flight trainees were on U.S. soil learning to fly airplanes and asking their instructors specific questions about flying larger airliners.

The failure to conceive that a major attack could occur on U.S. territory left the country unprepared (Porch et al., 2002). Our country’s fixation that we are invincible of such an attack is an example of our country’s cognitive bias. The desire for rapid closure is a common need for this fixation technique. This is a more basic human tendency than many realize. Even cyber security analysts fixating on one hypothesis is one sure way that a deception by a cyber criminal may exploit an agency’s biases on a company’s computer network. Biases are commonly predictable in that one can expect humans to behave in a certain way. Al-Qaeda may have exploited our weaknesses knowingly and counted on the U.S. arrogance to make us vulnerable to an attack. However, biases provide no assurance that a particular person will conduct himself in a certain way at any given time. An operation depending on a person’s biased perception is a rare gamble and cannot be entirely reliable (Yuill et al., 2007, p. 1).

Yuill et al. (2007) described perceptual biases, “... human perception, and hence response to deception, is strongly influenced by expectations and desires” (p. 2). The mind can only process a small fraction of the information it receives from a person’s five senses including sight, sound, etc (Yuill et al., 2012, p. 2). The human brain must combine and create easy to understand models within itself to cope with the huge and complex information it receives daily. Examples are social models that explain how people take action in their daily lives and in cyber space. Network models can be developed that describe computer networks. These models are necessary for sorting out the overwhelming information obtained from the brain’s five senses. For example, when system administrators are sniffing out suspicious network traffic, a hacker’s network model (that he has created) defines the abundant amount of data received that a hacker can understand and know which systems are vulnerable to him in order for him to attack and steal data or information at a future date (Yuill et al., 2012, p. 2).

Perception is strongly influenced by the expectations an individual holds. Accurate expectations provide appropriate and true perception, which is essential in making informative and insightful choices. Incorrect or inaccurate expectations can impair perception or cause irrelevant and false perception. Types of incorrect expectations include *premature judgments* and *prejudices* (Yuill et al., 2012, p. 2). Yuill et al. (2012) stated, “In military and intelligence literature, one of the primary deception principles is to abuse the deception target’s expectations” (p. 2). If a targeted adversary has certain expectations that are identified and exposed, it is easier to know what deception technique to use in baiting the target in a criminal act. When those setting the trap understand the target’s true expectations, it is easier to convince the target to believe the deception trap. A consistent characteristic of expectations is that they are resistant to change. Therefore, once an adversary's judgment about the essential characteristics of a computer's network vulnerability is construed, a criminal will continue to perceive it in the same manner even if the data in trap is confusing or misleading (Yuill et al., 2012).

Impaired Thinking

Impaired thinking refers to a range of psychological influences from the relationships in one's life, such as parents, siblings, teachers, and friends, to immoral acts and decisions, such as self-indulgence and stealing (Yuill et al., 2007). In deception operations, one can attempt to induce impaired thinking webpage that causes the deception target to act hastily and recklessly. For example, a *limited time offer* ad on an internet website may result in an impulsive purchase. Deceptions that exploit impaired thinking and expose biases will be more likely to succeed in persuading a target to fall for the deception trap than ones that do not. It is important to identify and understand the psychological vulnerabilities to deception, as well as knowing how to create a cyberspace deception. Both are important tools in regards to preventing innocent victims from fraud, and as a lure to capturing cyber criminals.

Mitigation Strategies in Cyber Deception

Principles of Counterdeception

In order to defend against a cyber criminal or adversary in the cyber world a person, intelligence analyst and organizations must have some type of training and the proper mindset when knowing how to defend them against a cyber threat. These people need the education and training to build mitigation strategies for defense against cyber deception capabilities and traps. One way to build a good defense against deception is to use four basic *counter deception* principles, which can be easily applied to any end user or intelligence analyst's level of understanding (Bruce et al., 2008, p. 135). These counter deception principles are *Know Yourself*, *Know your Adversary*, *Know your situation* and *Know your channels*. Understanding the principles will go far in reducing vulnerabilities to D&D and will mitigate the deception casualties if an attack is successful.

General Sun Tzu, writer of *The Art of War*, made it very apparent that if one does not *know yourself*, then one will have no success in battle defenses (Griffith, 1963, p. 84). Relating to cyber, the same can be said between an adversary and his target. Again, if a target's expectations or biases are exploited due to the adversary gathering good intelligence on the target, then the adversary has already won. Succinctly put, knowing oneself is a person's first and best defense against a D&D attack. Simply knowing one's cognitive vulnerabilities and weaknesses is the first step in cyber defense (Bruce et al., 2008, p. 130).

The second most important principle is *know your adversary*. Once a target is comfortable knowing his own vulnerabilities and tendencies using his computer on the internet, then knowing a person's enemies or adversaries is by far the next big step. For an intelligence analyst, knowing the adversary is a constant reminder that one must know the motives, means and culture of the criminal. This means that an adversary could have at their disposal an arsenal of weapons ready for an attack. Experienced cyber attackers will have their own doctrine, training, possibly their own personnel, experience and of course technology for developing malware, spam or any number deceptive traps in cyber space. Motives of an adversary can range from internet traffic deterrence (i.e. DoS attack), blackmail, seeking revenge or prestige, concealing Weapons of Mass Destruction (WMD) and even planning terrorist attacks (Bruce et al., 2008, p. 130). Bennett and Waltz (2007) stated, "...being able to put yourself into the mind of the adversary may the counterdeception analyst's most effective weapon" (p. 154).

The third principle, *know your situation*, focuses on the obligation for constantly re-evaluating the situational awareness within a network for indications that a deception will inevitably happen. An analyst should think through carefully about the status of his network as the adversary is devising strategies, considering options, and making choices of whether or not he should take action against a target (Bruce et al., 2008, p. 131). D&D attacks by an adversary are most likely to happen at any time, despite the environment that a network is in today. Some situational factors, depending on the adversary, will offer clues on any given day. Major or massive attacks are extremely rare. Bruce et al. (2008) suggested, "...situational factors include, high stakes situations, asymmetric power relationships between participants, changes in leadership, motives or political goals, technology capabilities, potential surprise attacks, and events in the international environment that threaten security or provide opportunity" (p. 131).

The fourth counterdeception principle is *know your channels*. This principle is a thorough application and it means that an intelligence analyst must have a complete understanding of all of the intelligence collection channels. An intelligence operations channel is a casual or recruited source that provides source data and information to intelligence analysts (Dept. of Army, 1995, para. 4). This means an analyst has a complete knowledge of all capabilities, limitations and vulnerabilities to D&D. It is especially crucial to know the extent of any compromises that the collection of capabilities possessed and if any of the vulnerabilities remain exposed to exploitations by an adversary (Bruce et al., 2008, p. 131).

Vulnerable Minds and Organizations

Even the most trained and experienced intelligence analysts, and decision makers, can find themselves in a vulnerable position to any kind of D&D. Analysts or top decision managers are commonly blamed for ineffectiveness or ridiculed by those who are considered the top minds in their career field, despite the fact that every person is vulnerable to any type of deceit in cyber space. Understanding the natural weaknesses of human nature to deception is a tool in learning what actions must be taken to mitigate those vulnerabilities and what steps should be taken to prevent deceit from happening further. This starts by outlining the profiles of vulnerable minds and organizations (Bruce et al., 2008).

The *vulnerable mind* only sees and understands its own biases and preconceived perceptions and expectations of the world around it. The people, culture, and environment a person is brought up with develop and strongly influence a child's reality. Bruce et al. (2008) stated that the human mind is without question normally naive, arrogant and is easily influenced by believable stories especially from a trusted source (p. 131). Practitioners of the time believed that the human mind is the least prepared for D&D and naturally is not prepared for the world and cyber space. Thus, a vulnerable mind represents all the missing information an adversary is hiding behind his computer screen. Bruce et al. (2008) said, "Human vulnerabilities represent the end result when the biases meet contradictory, ambiguous or missing information" and " This is a formula for successful D&D" (p. 132).

According to Bruce et al. (2008), "A *vulnerable organization* however, exaggerates consensus, consistency, and being decisive" (p. 132). At times organizations and their networks are either uneducated about the dangers of online cyber criminals looking for vulnerable systems, not motivated in training their employees, or do not have the funding to educate and update technology to their networks. A vulnerable organization is one that is the least prepared for any type of D&D attack. They have insufficient learning processes, which often fail to protect from continual attacks by outside hackers. Failures to this extent are ones that are often repeated. Chief Executive Officers (CEO) and leaders of vulnerable organizations are either concerned or inattentive about the expenses needed to protect the computer networks. Training or upgrading systems is ignored until a disaster has occurred. Many executives understand the wide-open nature of any network computer attached to the internet. What they do not understand is how incorporating more training and education to their company will protect the organizational networks, customers, and employees (Bruce et al., 2008).

The prepared mind. The human mind needs preparation in order to recognize deception tactics. Such preparation requires time and training, because even the most advanced trained intelligence analysts will fall for D&D techniques used by cyber criminals. One way to reduce the mind's vulnerability is by training it to analyze what is being viewed online. When someone knows how to use an analytical process, they know what danger signals to be aware of in the cyber network environment. Bruce et al. (2008) stated, "The *know yourself, know your adversary, and know your situation* principles highlight the importance of two interdependent approaches: mitigating cognitive biases and adopting systematic or 'structured' methodologies" (p. 133).

The *know yourself* principle explains that the human mind's most exploitable weaknesses are its own preconceptions, expectations, and beliefs. Mitigating cognitive biases are critical to improving analysis. Any organization can improve this using hypothesis. Being able to change beliefs or expectations is a very difficult task, and creating a different way of thinking recognized in the intelligence community. Therefore, creating a new hypothesis about one's own preconceptions or beliefs about people and crime on the internet is an alternative analytical thinking (Bruce et al., 2008). When the mind initially believes that something is right, wrong, or ignorable, it is predisposed to see things that way. Once it understand there are alternate ways of viewing the same thing, or belief, then it is easier to see things or observe behaviors that represent D&D in the cyber world from a different of view.

Failure to generate multiple hypotheses about a dangerous situation increases the chances of falling for deceit, and also confirms the bias thinking about that deception. One important way of mitigating confirmation bias and overconfidence is to "*restructure the analytical task"* (Bruce et al., 2008, p. 133). This approach is designed to challenge the human mind's ability to stimulate cognitive bias and over emphasize confidence in one's thinking process. Some mind preparation methods to reduce susceptibility to deception include the following:

- Asking analysts and common users to list why their answers to questions might be wrong.
- Instructing analysts to consider the opposite interpretation of a judgment or forecast or explaining a different version of the same outcome.
- Encouraging analysts and organization employees to generate multiple alternatives or explain any single credible alternative.
- "Test for fixation" to namely consider what would be required to convince him or her that the interpretation of a particular D&D is wrong.
- Asking analysts and end users to assess how far they have "bent the map" or monitor any inconsistencies and discrepancies that are explained away.
- Having analysts or users monitor "tripwires "events that should not be occurring or levels that should not be exceeded (Bruce et al., 2008, pp. 133-134)

The *know your situation* principle centers on the continuous evaluation of the environment for clues that deception may be a factor in an actual D&D event. This also provides optional ways of reorganizing problems so that the preconceptions, assumptions, and mental models are not hidden by making them clearer, so problems can be examined and tested for symptoms of D&D. Davis (2008) believes, "such methods of examinations can be accomplished by Analysis of Competing Hypothesis (ACH), argument mapping, and signpost analysis. "Challenge analysis" techniques include: Devil's Advocacy, What-If analysis, and High-Impact/Low-Probability Analysis" (p. 168). By using these analytical methods, an analyst or end user can diminish the possibility that important biases or situational cues are not identified or overlooked (Bruce et al., 2008).

A prepared organization. There are four things that businesses and intelligence organizations can do to assist in mitigating counter deception and denial tactics against cyber adversaries. These four actions will prepare organizations and computer networks in being less vulnerable to D&D attacks. According to Bruce & Bennett (2008), listed the four actions of a Prepared Organization as :

- "Prioritize an effective counter D&D analytical capability and ensure that it is well resourced, motivational, and protected.
- Enable analysts and employees in organizations to better work together, access and share sensitive/top secret information and exchange alternative and unusual views.
- Create and encourage a healthy analytical learning environment that emphasizes lessons learned and structured analytical techniques.
- Emphasize anomaly detection to help ensure that little surprises do not become big surprises" (p. 134).

A truly prepared organization will be armed with strong and well developed counter deceptive techniques and will have obtained strong analysis abilities through training within their organizations. In order to determine an organization's mitigation abilities, a company will be judged by the analysts who employ them, the D&D skills of colleagues within the company, and the training support that focuses on counter deception missions. Proactive steps must be made in the future for the intelligence community and public organizations. Cooperation among all intelligence agencies is imperative in order to obtain better sharing of sensitive information and creating alternate views of countering D&D in the future (Bruce et al., 2008, p. 135).

Foreign denial and deception within the cyber world will continue to be a problem and challenge for agencies and organizations in the future. The best principles when countering D&D begins with a common understanding of the principles of deception. Bruce & Bennett

(2008) believed, “Truth, denial, deceit and misdirection require keen awareness of bias traps and cognitive vulnerabilities to being deceived” (p. 135). By knowing yourself, the adversary and observing the situation and channels, one can lessen the vulnerability to denial and deception and avoid defective analysis. The best possible environment for mitigating against D&D is having a prepared mind and prepared organizations in order to assure confidence that a defense against foreign denial and deception attacks are effective (Bruce et al., 2008, p. 135).

Discussion of the Findings

Major Findings

The purpose of this capstone project is to identify and understand the gaps and weaknesses caused by cyber deception, which hinders the ability of U.S. government organizations and civilian agencies to protect their personal identifiable information (PII), top secret or sensitive information and data on organizational computer networks. To obtain this purpose of the project the assessment focused on identifying the four basic principles and six MILDEC principles as well as the counter principles of online deception, the use of denial as the foundation of deception, the analysis of human deception vulnerabilities, and the ability to prepare an individual's mind and organizational groups against cyber threats. Examination of accessible diverse research literature was based on its academic value and appropriateness to the research gaps in cyber deception. Sources for this capstone project were discreetly chosen based on its abilities to support the assessment's results and themes.

Theme One: Deception and Cyber Deception

Theme one of this assessment focuses on cyber deception within the cyber world. According to Bodmer et al. (2012), "Deception is a technique whereby people are mislead into believing information that prompts them to behave in a way that is favorable to a criminal and in the same process prevents the victim from knowing the true intention and position of the person committing the crime" (p.24). Other experts like Bruce and Bennett (2008), refer to deception as "the exploitation of intelligence collection, analysis, or opinion by using false, misleading and sometimes modified information with the intent of influencing judgments and perceptions" (p. 123). Bodmer et al. (2008) explained that deception is about an influential behavior encouraged by an adversary and accepted by the one being deceived which can exploit a vulnerable computer network (p. Xvii). After completing this literature review, it is found that the use of cyber deception is two-fold in that it can be used to commit criminal acts and used to capture those who engage in unlawful activity.

Succinctly put, cyber deception is defined by its principles, vulnerabilities, and ability to entice others through deceit. This assessment shows various opinions by noted cyber deception and security professionals in defining the use online deception, and several noted commonalities that deception serves as a multifunctional tool by adversaries and organizations alike. This study does promote to classify the tools and tactics used by cyber criminals in perpetrating their agenda and by organizations in defending their networks from cyber threats. The proceeding sections of this study show how deception is used as a counter-deceptive tactic to catch cyber criminals, and the study of their behaviors. Having the ability to identify the principles and counter principles of cyber deception are central to provide cyber security professionals, system administrators, and governmental security personnel an aptitude to focus on customizing cyber defenses within their own networks to combat cyber attacks and evaluate their own levels of risk.

Theme Two: Cyber Deception Military (MILDEC) Principles

The emphasis of the second theme of this study focuses on the six MILDEC principles of cyber deception. It can be better understood by studying two components that make up a large portion of its definition – principles and techniques. There are six military, often referred to as the MILDEC principles within cyber deception that are used for both negative and positive gain, as well as identifying and capturing online thieves. Cyber deception techniques are construed as services that appear legitimate but are used to exploit the recipient for malicious purposes and ill-conceived gain (Bodmer et al., 2012).

According to Public Intelligence *Military Deception* (MILDEC), a *Joint Publication 3-13.4,* created by the Joint Chiefs of Staff (2012), “the six (MILDEC) principles of deception are *focus, objective, centralized planning, security, timeliness,* and *integration"* (pp. Vii-Ix). Practitioners and readers will learn after reading the assessment that MILDEC was created by the *Joint Chiefs of Staff* to help categorized online criminal behavior for a thorough understanding of the types of methods used to create cyber havoc worldwide. It is important to note that government and public organizations have online goals to develop stronger and more secure networks, unfortunately not all agencies, and companies provide educational training of the six principles, which fosters a lack of knowledge in developing counter deceptive tactics to protect their systems. As more knowledge is learned and gathered in this field, cross-cultural communication among government and civilian organizations must grow and expand to fight against continuing daily threats.

The six MILDEC principles of cyber deception are used in various ways to develop decoy firewalls, servers, and a sounder infrastructure that will aid in accomplishing counter deception successfully (Ragsdale, 2011). Organizations and agencies must be able to *focus* on the types of deceptions that are most commonly used by criminals. From that, readers will observe that the *objective* of counter deception is to have the adversary take specific actions that will aid in catching them while engaged in malicious activities. MILDEC operations develop *centralized planning* by team members that work together in order to achieve a united effort against cyber adversaries. *Security* forces protect allied units and collaborate by diffusing any knowledge that a company has attempted to outmaneuver their adversaries, and the particulars of successful counter deception attacks are kept confidential. *Timing* requires meticulous planning and precise action in a successful counter attack, and thereby is regarded as the most important process within the six principles. Finally, *Integration* simply means to ensure that each principle is fully incorporated and coordinated with the other throughout each step of a counter attack to provide interrelated support for a positive outcome. From this literature review, readers will conclude that in order for all six-deception principles to be fully effective, agencies must provide up to date training and have the newest technology within their networks.

It should be noted that all organizations and security professionals must adopt an approach that is appropriate and relevant for their company when building training sessions. Not all internal employees will have technical practical understanding. Through more research and preparation, training sessions should also include the skills that administrators will need in setting up honeynets with decoy firewalls, routers, and infrastructure. Cyber security specialist should pay attention to that when developing a deception trap, it should appear realistic, credible, and most importantly, enticing to a cyber criminal. Additionally, a decoy infrastructure system must be automated and clear of outside interference from average end users (DARPA, 2011, p. 6). In summary, the six principles illustrate the need for continued research and training among our nation's agencies and its allies. This research does not propose that all government and private companies have ignored the six deception principles. On the contrary, this theme shows that only further education and training is needed to educate cyber security future generations about unavoidable cyber threats.

Theme Three: Four Basic Deception Principles

Based on the findings, the focus of theme three centers on denial, which is the primary foundation of cyber deception. Bruce and Bennett (2008) defined denial as, "intelligence denied through effective operational security" (p. 122). "Deception is described as expectations of an attack reduced through manipulation of information and data by using false, misleading and at times true information to confuse an individual's judgment in decision-making" (Bruce et al., 2008, p. 122). If denial is the core basis of deception, then deception will be always effective.

Practitioners commonly note that denial is not only the root of deception, but also the main purpose of online deception as mentioned earlier in the assessment. To evade deception requires an understanding of its composite principles that are needed for a deception trap to be successful. The four required basic principles of deception are *truth, denial, deceit,* and *misdirection* (Bruce et al., 2008). From this assessment, readers will perceive that *truth* is needed in information context, which serves as the root of deception so that beliefs and expectations can be exploited. The average person will not be aware that an adversary is using *denial* against them. Military cyber security experts may use denial to deny targets access in areas on the internet or access to organizations susceptible information. From the findings, denial is the decisive prerequisite for deception *Deceit* is the requirement needed to obtain and utilize deception, and *misdirection* is the action that a deception takes when it is successful in accomplishing the goal of the act of deception (Bruce et al., 2008, p. 126). While it is important that readers notice the importance of the previous six military principles of cyber deception in theme two, it is also important to understand the actual four distinct principle requirements of deception in theme three. The principles of theme two are focused on military deceptive tactics, of which Bruce and Bennett (2008) clearly defined the differences between the six principles of theme two and the four principle requirements in theme three. Further examination is needed to explain differences between the military's use of cyber deception and the role of civilian organizations using similar tactics to defend against cyber threats. While there are several agencies who work in conjunction with their civilian counterparts, a deeper collaboration between agencies will enhance the military's six principles of deception and the four standard principles of deception used to comprehensively define deception.

Denial is a highly effective tool for cyber attackers. For a systems administrator of a large organization, denial can be a nightmare situation. An adversary can easily confuse an analyst by taking away strands of information that make the denial unreadable to the naked eye. From literary studies, D&D can easily frustrate and humiliate U.S. intelligence competence by infiltrating collections of evidence with malware and malicious viruses that prevents an analyst from completing an effective examination of a potential cyber attack (Bruce et al., 2008, p.123). This assessment confirms that denial is difficult to observe while surfing online websites. More research on the sharing of online deception among organizations is imperative.

After reading this document, it will be understood that the lack of visual access to a recipients physical expression regarding body language and non-verbal communication, contributes greatly to online deception gullibility. This research will impress upon the fact that information technology and virtual reality will show merit in an analysis that the lack of need for non-physical expression and interaction hampers the ability to decipher the intention and truthful actions of any computer user. (iPredator, 2014, para. 7). iPredator (2014) stated, “ It is at this point in human history that unknown aspects of the Information Age, temptation and curiosity act as accelerants driving online users to deceive their peers and unknown every day Internet users” (para. 4).

Theme Four: Deception Vulnerabilities

During this assessment, Bruce and Bennett (2008) explain that anyone is susceptible to a myriad of deceptions throughout their lifetime. Knowing how to detect online deception in cyberspace is the key to preventing deception from making someone into a victim. After reading through this assessment, organizations, employees, and everyday users will further understand bias traps and typical analytical vulnerabilities, which lead to impaired thinking (Bruce et al., 2008). Bruce et al. (2008) stated "...vulnerabilities can be attributed to biases, systematic errors in perception, judgment and reasoning" (p. 127). After examining, the six MILDEC and four basic principle standards of online deception, readers will discover that vulnerabilities fall into two extensive areas labeled as *biases* and *impaired thinking*. *Biases* can be cultural, personal, cognitive, and even organizational. *Impaired thinking* refers to psychological influences from relationships such as parents, siblings, teachers, leaders, and friends (Bruce et al., 2008).

For this assessment, biases are categorized as perceptual and cognitive, which result from incorrect interpretations and false reasoning (Yuill et al., 2007, p. 1). Bruce et al. (2008) said, "Preconceptions and belief biases are formed during childhood and based on personal experiences" (p. 127). The cultural or social environment of a child influences their overall knowledge, beliefs, customs, morals, habits, and basic decision methods. This assessment attempts to show the differences between understanding deception principles and the vulnerabilities associated with those principles that lead to deceitful behavior. Deception principles lead to the limitations and vulnerabilities within human nature that originates in childhood. Such limitations lend itself to habitual thinking that is initially resistant to change, thus making someone vulnerable to deception. This assessment will enable the reader to decipher how biases influence them personally, and model how to develop possible solutions from analyzing their own weaknesses and perceptions.

Upon reading the analysis, readers should be able to understand how perceptions and biases lead to analytical flaws when overlooking personal bias signals within a deceptive environment that is created by an adversary. Examining organizational biases reveals that similar company prejudices and misconceptions about online deception are compatible with cultural biases, just as with individual biases previously mentioned. Future research will show that organizational biases are associated with the limitations and weaknesses of large agencies lead by civil servants who make a majority of all biased and opinionated decisions within their organizations (Bruce et al., 2008). Ultimately, cyber criminals depend on flawed thinking and biased perceptions to lure unsuspecting victims into an opening in a network security defect previously discovered by the adversary, allowing them to create and sustain cyber traps. Therefore, government and civilian organizations must continue to use current and future research analysis designed to study criminal behavior, which in turn will lend to developing proper mitigation strategies against adversarial deception behavior.

Theme Five: Mitigation Strategies

The focus of theme five revolves around educating organizations and individuals of how to use deception as a mitigation strategy and develop specific ways of protecting sensitive computer networks connected to cyber space. In order to plan for mitigation against online deception, the principles of counterdeception must first be taught and subsequently learned. With proper training and a full understanding of these principles, organizations will implement counter deception techniques as weapons in fighting against unwanted cyber threats that affect their livelihood. Bruce et al. (2008) stated “To succeed against smart adversaries from whom denial and deception are weapons in their arsenals, analysts and administrators must master counter D&D skills and develop expertise in analytical judgments” (p. 130).

The five counter-deception principles are referred to as *Know Yourself, Know Your Adversary*, *Know Your Situation*, and *Know Your Channels*. After researching these skills, the reader will have a fuller knowledge of better understanding on acting and implementing each one. Organizations and individuals will observe and learn that these principles in particular are essential in preparing system analysts and administrators for building confident future counter-cyber attack methods in support of government or organizational computer networks (Bruce et al., 2008).

As analysts constantly check and examine systems for malicious activities, cyber adversaries are continually using any type of deceptive activity at the same time. Therefore, an analyst will always face a continuous bombardment of a range of cyber attacks on a daily basis, primarily with multiple deception techniques. In turn, analysts and readers alike can learn from previous attacks by deriving information on how each one was planned, devised, and implemented, and which ones resulted in gainful information that aids in helping to create a more refined deceptive process in identifying and creating future counter-attacks. The following list by Bruce and Bennett (2008, p.131) are situational factors that can lead to counter-deceptive operations:

- High-Stakes situations
- Asymmetric power relationships between participants
- Changes in leadership, motives, political goals, doctrine or technological capabilities.
- Potential surprise in high risk/gain strategies
- Events in the international environment that threaten cyber security (p. 131).

Information was also obtained from *Vulnerable minds* and *vulnerable organizations* which is described as a referential state that adversary's use in developing specific cyber deceptions against a target, just as mitigation strategies can be created by identifying those same vulnerabilities in preparing for a foreseeable threat. Once common users, companies, and organizations understand that everyone is susceptible to an attack or damage by a deception, accepting that weakness and learning from it will help prepare against cyber crime (Bruce et al., 2008). The *vulnerable mind* is described as “the one least prepared to counter D&D and sees reality innocently shaped by its own biases, preconceptions and expectations” (p. 132). Readers will gain knowledge about themselves with understanding that a *vulnerable mind* has the ability to overstate the significance of limited information that he or she reads on the internet. In turn, a person's mind will exaggerate the simplicity of cyber space reality and remain unaware of online deceptions. Once a human's mind does realize the damage deceit inflicts upon people as well as vulnerable agencies, the adversary or criminal will have moved on to other targets. A vulnerable mind will thereby rationalize the possibility of an attack; i.e. that one's own personal computer or an entire company is already, and will continue to be, protected against outside offenders. Further analysis shows that a *vulnerable organization* will over compensate the extent of their knowledge and its ability in protecting their networks. Bruce et al. pointed out that "Organizations that fail to exploit its collaborative potential, have inadequate performance in the sums of its parts, and has insufficient training for its employees, will consistently fail to learn from its failures and past performances" (2008, p. 132). The status of a company that has been spared from previous cyber attacks may inevitably fall into a deceitful trap of maintaining a false sense of security, which will always be at the expense of their employees and safety of the computer networking system.

While Bruce and Bennett pinpointed how vulnerable the human mind and business organizations can be, they also summarize that in order to user counter attacks, individuals and organizations must learn about their own vulnerabilities. Education will lead to proper preparation. Those two primary items, in that order, will help to prevent, mitigate, and defend private identities and business operations. *Vulnerable minds* and *vulnerable organizations* are now in a position of strength as they will have turned into *prepared minds* and *prepared organizations.*

Readers of the assessment will learn about the desired goals of a *prepared mind*, which is to educate employees and analysts to use new skills obtained from recent training and carefully apply them to make accurate judgments before an attack, and to help prevent the effects of denial and deception within their working environment. Bruce and Bennett stated that, “The four principles of counter deception highlight the importance of two mutually dependent approaches: mitigating cognitive biases, and adopting organized or ‘structured’ methodologies” (2008, p. 133). This research also revealed that when a prepared mind is fully equipped with the knowledge and tools of counter attack and crisis management, it is able to maintain order in complex analytical situations and verify the credibility of its data sources upon analyzing a D&D situation (Bruce et al., 2008).

Readers of the assessment will also learn about the desired goals of a *prepared organization*, which Bruce and Bennett (2008) define as having, “four common items in its arsenal to be prepared to make itself less vulnerable to D&D:

□ Prioritize an effective counter D&D counter analytical capability with promising resources, motivations and protection.

Ensure analyst and administrators have cooperative cross over communication with sensitive information and exchange of observations.

□ Encourage healthy learning environments that show past learning experiences and new solutions.

Emphasize irregularity detection analysis to ensure small issues do not become huge issues” (p. 134).

A positive step in creating an online society of *prepared organizations* is to encourage a mutual sharing community between intelligence agencies, federal agencies, and civilian companies about the cyber criminal community and their D&D behavioral tendencies. Upon using the skills needed to prepare an organization to a sufficient level of readiness against an attack, further research and analysis within this area will reveal improved relationships that will raise the expectation of communication between government and civilian companies, ensure situational awareness and develop guidelines of behavioral mental models of criminals (Bruce et al., 2008). Learning organizations are simply prepared organizations. Continued preparation and insight obtained from collaboration with others will lead to an overall stronger defense against attacks. Every civilian and federal agency must have an aggressive intelligence-training program that is readily accessible and at a minimum completed yearly. Understanding and having a keen awareness of the four principles of counter-deception, including typical bias traps and cognitive vulnerabilities, will greatly reduce how susceptible organizations are to ongoing denial and deception tactics (Bruce et al., 2008, p. 135). Teaching available counter-deceptive tactics allow security specialists, organizations, and individuals to recognize that an attack is coming and how to prevent them. In summary, the findings of this research shows that prepared minds and organizations who continue to work together will result in the best preparation in preventing all targets from D&D entrapment by cyber threats.

Limitations

The purpose of this section is to investigate the limitations of cyber deception analysis, to locate possible limitations in using deception principles for countering cyber threats, and to study online cyber criminal behavior. It will specifically address limits concerning the lack of review on current literature to ensure a focused study about online deception and its foundational characteristics. In addition, this analysis will show the differences between various cyber threats, and obtaining the ability to learn deception tactics for methods of counter attack, and the study deception behavior. The deception principles and methodologies used were developed to evaluate the levels of risk for corporate and government computer networks in regards to the current cyber threats of today. Limitations affecting this study were frequent during the identification of cyber deception, its characteristics, examination and analysis of unique traits among deception principles, and the vulnerable behaviors of organizations and individual computer users.

In order to reveal the existence of common foundational characteristics across all cyber deception uses, this literature review located and referred to the use information on early deception tactics used throughout previous centuries in wars throughout history. The first known literature to discuss modern day deception was by the famous Chinese tactician and military general, Sun Tzu in *The Art of War*. General Tzu is the first person known to state a widespread belief that "All warfare is based on deception" (Bodmer et al., 2012, p. Xxii). Tzu's book was written during the Chinese feudal warring dynasties of 554 - 496 B.C. Modern examples of warfare deception occurred in ones such as WWII, the Vietnam War, and the War in Iraq. Although the warfare that Tzu referred to was battles fought on land, obviously there was no use of cyber deception until recent times showing that modern online deception is warfare, which is fought in unseen territory.

An awareness of cyber and technology deceptions was not known until the era of the Internet in recent decades. Subsequently, there was a limited amount of information on the use of online deception against technology in modern day cyber-attacks. The earliest incidents of cyber deception occurred in the 1970s, but were not reported until recently, once computers became available to average citizens. Therefore, scholarly journals focusing attention on cyber technology security were a challenge to locate. However, the last fifteen years has produced several scholarly modern books, articles, and publications addressing and emphasizing the problem of online deception. Unfortunately, due to the fast pace at which computers advance, the fact remains that as soon as material is published about the subject, the technology and tools used by hackers even six months prior will have adapted or changed to some effect.

Other limitations found in this assessment lay into the foundation for further investigations into more in-depth assessments of how the Public Intelligence (2012) release of the six principles of MILDEC are either more or less effective against cyber threats as opposed to the traditional four deception requirement principles. There is a divide between military deception experts and civilian deception experts. This is in regards to which set of principles is more productive and proper for counter deception use. Further research is recommended to determine if the U.S. Military is sharing new technology and abilities that can help prevent cyber attacks with civilian organizations. Additional questions are raised in regards to the U.S. military discovering new cyber criminal trends, and what research can be shared with corporate and civilian organizations to further the education of network security. Such questions reveal weaknesses in the relationship between the military and its country and need further examination towards a conjoined effort in fighting against cyber crime.

The current level of communication between the U.S. government and civilian agencies is clearly not enough, insufficient and needs to increase. Classic miscommunication examples include one of the most recent events such as the terrorist attacks of September 11, 2001. Common examples of miscommunication occurred when local police, firefighters, and military personnel did not know what each group knew, what emergency responders had been dispatched, if other agencies had been called for backup, who was performing survivor rescues, and so on, during the aftermath of the attack. The reason, cause, and effect of these limitations go further than the scope of this assessment, and deserve further investigation, which will have a direct influence in decision-making process for the federal government, cyber security professionals, IT professionals, CEOs of prominent organizations, and the entire civilian business world.

James B. Bruce and Michael Bennett (2008) did a thorough job explaining the studies associated with identifying unique characteristic traits associated between vulnerable minds and organizations as compared to prepared minds and organizations. However, very few examples in this research were evident in the limited constraints of a published book or article. More research is needed in regards to enhancing communication among organizations that have been trained and those businesses not fully aware of cyber threat preventive measures. Any organizations or business that is unaware and uneducated about cyber threat prevention will eventually fall prey to a cyber attack with a wide range of ramifications. Despite the limited education studies, Bruce and Bennett did an excellent job acknowledging these weaknesses within the human mind.

Very little documentation is found on the four principles of counter deception in terms of limitations around mitigation strategies and preparation against threats. Bruce and Bennett (2008) once again have thoroughly laid out a systematic process to help train and prepare organizations against attacks in writing about four counter-principles called the *Know Yourself* principles. These principles are excellent choices of preparing the mindset of employees who work on network systems daily and are unaware of cyber deception tactics that loom as a constant threat. Unfortunately, no actual models or research examples were found in regards to proving how effective these four counter principles work within top government or civilian agencies. Knowledgeable and comprehensive study of organizations utilizing and incorporating these skills will present an even greater realization of how vulnerable any computer system is to cyber threats. Eventually all cyber attacks and threats, both past and present, should be disclosed by every government and civilian agency for study and learning purposes in regards to what tools are working effectively and which ones can be discarded (Bruce et al., 2008). With the increasing pace of new technologies and coinciding strategies, also come new levels of ever increasing elevated threats. Therefore, newer methods need to be continuously adopted in maintaining an offensive stance by using a more targeted threats approach.

Recommendations

This capstone project is based on literature and information gathered from a number of authors who recognize a lack of research in regards to cyber and online deception. These authors emphasize cyber deception as the primary tool used by cyber terrorist and hackers, which is hampering the U.S. government's capability to fully understand and address this problem (Bodmer et al., 2012; Public Intelligence, 2012; Roberts, 2012; Bruce & Bennett, 2008; Yuill et al., 2007). Based on results of accredited information from various sources, the following plausible recommendations provide a structured outline of actions to be considered to educate and train cyber security administrators, specialists, and individuals to obtain knowledge on the long-term issue facing cyber threats with deception. Some of the latest recommended deceptive techniques by Neil Rowe, of the U.S. Naval Postgraduate School, include the use of *honeypots, counter deception*, *counter-counter deception for honeypots*, *disinformation, deceptive delays, defensive lies, deception to identify attackers*, and *strategic deception.*

The use of defensive deception in cyber space is not just a recommendation, but is mandatory, almost crucial, as a means in maintaining certain levels of security among professional organizations and government agencies. *Honeypots* are a specific type of defensive deception that are designed to only collect information about data attacks being performed against a victim organization. Groups of honeypots, called *honeynets*, provide multiple targets of attacks in order for system administrators to study cyber criminal behaviors that can be further analyzed later.

As for *counter deception*, it is recommended for administrators and cybersecurity experts research examples of attackers who also search for evidence of honeypots, as a counterdeception tactic, on network systems daily before the criminal decides to infiltrate them (McCarty, 2003).

Another counter deception tactic for criminals is the use of intrusion-detection systems in cyberspace. Proctor (2001) stated, "...this counter deception could look either for statistical anomalies or for features or "signatures" that suggest a honeypot" (p. 100). Honeypot 'signature' anomalies show up in statistics in many types, sizes, and dates of files and directories of many networks around the world. Many adversaries are aware of honeypots and counter deception techniques and as a result, the use of *counter-counter deception* tactics are recommended to security administrators and necessary to use in conjunction with honeypots in order catch or document such hackers. Counter-counter tactics are highly efficient ways of tracking down and pressing charges against criminals, in addition to learning and studying their methods. McCarty (2003) stated, "...some attackers search for evidence of honeypots on systems into which they trespass, a form of counterdeception" (p. 79).

Disinformation is essentially false information and a technique that is recommended for everyday common computer system networks. Rowe (n.d) stated, "*...disinformation* can be planted on computers for enemy spies to find as a counter intelligence tactic" (para. 10). Disinformation tactics include counterfeit mission plans, false logistics data, bogus intelligence, and phony orders. False information can also include sham operating-system data such as replica temporary files and fake audit logs developed with the appearance that an average end user is using a system (Rowe, n.d). Research throughout the area of disinformation is highly recommended for the purpose of implementing it among all government and civilian organizations. This is an area that is sorely lacking in research labs in regards to the amount of disinformation that thwart finding and catching adversaries committing cyber criminal acts.

Deceptive delays, defensive lies, and *deception to identify attackers* are three areas that need to be explored more effectively to examine the affects and success rate by organizations that implement these techniques. *Deceptive delay* is recommended as a helpful technique when a system administrator protector needs time to assemble a defense capability, or when a user is awaiting support from an administrator to catch an adversary committing a crime within their honeypot or their networks. *Defensive lies* are recommendations that are not normally recognized by authorities, but can be a very effective way to help defend computer systems from an attack as well. Software can be designed intentionally lie to a user in some cases in order to influence or coax someone into hacking, which in turn will expose the intruders. Rowe (n.d.) suggested, “Host Web browsers will suggest that a site is not working when given a misspelled Web link (as a lie), apparently flatter the user” leading to “Information systems can lie to protect themselves against dangerous action” (para. 11). More research is needed to determine the effectiveness of software lying and manipulation and its effects on government and civilian computer networks. One of most serious issues facing cybersecurity professionals defending against a cyber attack today is finding the source location of the attack itself.

By using *deception to identify the attackers*, agencies and organizations can stop the attack, use deception to counterattack, impose sanctions once caught, or start legal proceedings. Thompson (2005) stated, “Spyware installed could remotely report user activities” and “Trojan horses or programs containing concealed processing can be used to insert spyware onto attacker machines by offering free software (like attack tools) through "hacker" sites or via email or spyware” (p. 41). Such software or spyware can be loaded stealthily onto an attacker’s computer without their knowledge. This type of deception needs to be researched more and is perfect tool for government and civilian use in attacker defense. Once installed the spyware can track when a criminal logs into a computer, what illegal programs are running, and which Internet a hacker may visit.

Colarik et al. (2006) stated that *strategic deception* "...can be used at a strategic level to make the enemy think you have information-system capabilities you do not have or vice versa" (p. 102). An example of strategic deception being used before a certain technological advance occurred during the 1980's when the Strategic Defense Initiative (SDI) of the United States used strategic deception deceive the Soviet Union into thinking that the U.S. could shoot down missiles from space. This caused panic and paranoia among the Russians and lead to an exorbitant amount of over-spending on its military (Rowe, n.d). Modern day computer strategic deception is highly recommended for government agencies as a valid deception tool that has proven successful in the past, such as during the decades of the Cold War. Additionally, these recommendations are intended to persuade key decision makers in the U.S. government and corporate executives to ensure appropriate steps to mitigate risks to protect sensitive data and information for their business, employees, and clients.

Each one of the following books and documents clearly educate and form potential processes on how to define and understand the definition of online deception. Furthermore, in some studies, authors try to formulate a distinct method of counter-deception method to protect a network or computer system. It is recommended that additional research and strategies be committed towards the development of a proper legal method, or road map, in which government entities and civilian sector agencies can follow in order to properly educate citizens of the online threats and dangers that are a permanent staple of society. It is common place for agencies and organizations to have some type of emergency plan or network protection in place to defend their vital assets. Companies and businesses who ignore or fail to update their computer networks will eventually realize that a cyber attack may have been prevented with proper training and education. Having full collaboration and communication among all government and civilian agencies will form a tight knit network that can prevent further cyber threats. The more cooperation among networks, the more secure any system will be.

Recommendation for Government and Civilian Sector Organizations

To date, there is only one recommended type of strategy for defending against online deception within the ranks of the military. This analysis highlights different approaches taken by corporate and government security personnel in analyzing threat vulnerabilities on networks. Both of sectors are distinct and lack unity and communication with one another. The MILDEC six principles were developed by the *Joint Chiefs of Staff* to provide rules and strategies to protect valuable and top secret information on military network systems. It is highly recommended that these six principles be used in collaboration with executives and system administrators of all government and civilian organizations as mentioned above. The MILDEC six principles were established to develop decoy firewalls, along with other deception traps, to lure cyber hackers. With the help of the military, and through collaboration of the armed forces and non-military enterprises, civilian businesses can develop deception traps, called *honeynets* or *honeypots*, as an aid in catching cyber criminals in the act of hacking into an agency's network.

The lack of research and analysis in this area is surprising, and therefore research is recommended and should be advanced to corporate and government security personnel. Once assessments are implemented among civilian agencies, then a majority of CEOs, executives, and civilians can more accurately assess respective levels of vulnerabilities within their own networks. When an agreement to collaborate and sharing information on the MILDEC principles has been reached, the military can train civilian sectors, and organizations will be able to recognize similar threat within their networks that have been successfully diverted by military partners. This detail is extremely important because government and public sectors will only work together once an understanding and awareness of the range of vulnerabilities to cyber threats has been understood. MILDEC principles will work well in the civilian sectors if followed.

Recommendations for IT Professionals

Another component of this capstone project involved an examination of the four basic principles that make deception a part of everyday human life. They include *truth, denial, deceit* and *misdirection*. Of the four basic principles, *denial* is the key component of deception. Denial is thoroughly discussed in several publications and highly recommended that more research models and examples be conducted for a complete understanding of why the human brain tends to use denial to cheat or take what does not belong to them. Further research and examination within groups of models is needed in order to understand the effects of how denial manipulates deception. It is advised that cyber security professionals read and learn D&D techniques to be able to understand the behaviors of an adversaries mind. When security professionals and IT specialist learn to implement denial techniques, then self defense becomes an option. This assessment was comprised of several accredited D&D authors who thoroughly explain the connection of denial and deception (Bodmer, Kilger., Carpenter, & Jones, 2012, Bruce & Bennett 2008, Bennett & Waltz (2007) and Yuill, Denning, & Feer, 2007).

Recommendations for All End-Users

Throughout past centuries, deception was used as a stable military tactic in winning battles that have shaped what our world has become today. When used successfully, deception can determine who is in control on the battlefield and eventually lead to who is charge and of control of the life of others. Therefore, another recommendation of this project is that research be committed to develop cyber threat tactics for use as counter defense made freely available on open source websites to anyone using the web and cyberspace. If known tools are available for individuals and civilian sector companies, this will allow others to individually read and research what tools are needed to protect their own networks. There was a lack of studies available to verify that tools and training were available for companies and individuals that desire education during this assessment. Proper education will allow room for more mitigation strategies to be developed as cyber threats become more frequent and more complex for the future.

Study on the four counter-deception principles from Bruce et al. (2008) in *Analyzing Intelligence: Origins, Obstacles and Innovations*, with research on the *Know Yourself* and *Know Your Adversary* counter-deception principles, indicate that one easy way for public sector companies and individual computer users to be educated about deception is to simply know the four principles. They reveal organization vulnerabilities, biases, and preconceptions about which individuals remain unaware. When cyber criminals become aware of an individual's or businesses particular vulnerabilities, they will use this weakness to lure innocent users into danger. It is highly recommended that all civilian and private sector companies be made aware of these easy-to-use counter principles. Although they have been published, it is also strongly suggested that more government, public analytical, and research models be published and evaluated to determine the effectiveness in the prevention and countering of cyber threats among government and civilian sectors.

Conclusion

The purpose of this capstone project was to identify cyber deception tactics and techniques used by cyber criminals in order to enhance end-user awareness, and what actions can be taken to mitigate the threat of cyber deception. In order to achieve the purpose of this capstone project, this assessment focused on identifying different characteristics of cyber deception and counter-deception, cyber deception principles and techniques, understanding denial and deception working together, vulnerabilities in deception, and mitigation strategies against deception. As technology advances, so does the ability and tactics of a cyber criminal's use against a government or private sector organization. The latest offensive and defensive cyber deception tools are constantly changing within both the federal government and civilian arena of networks. Some of these tool examples include *honeypots*, the use of *counter deception*, *counter-counter deception for honeypots*, *disinformation*, *deceptive delays*, *defensive lies*, *deception to identify attackers*, and *strategic deception*.

There are numerous advantages to be gained by having a collaboration of minds between the feds and executives of the civilian world. Such collaboration would provide access to counter-deception tools between government and civilian organizations, and create lucid communication between all organizations. The cost of sharing valuable information with each other and our allies will save the government extensive upgrades and provide a significantly stronger infrastructure for all military, government, banking, and private organizations in this country. However, as with all learning processes, educating, and convincing, all parties, will only be successful if there is full corporation between all government and entities is agreed upon. Failure by anyone person, committee or company to learn about online deception could be detrimental in the future. Learning about online deception is a significant portion of cyber threat prevention. An organization is only as strong as its weakest link. If educating system administrators, employees, and cyber security professionals is not an option, then the responsibility of protecting one's private and confidential information is a solitary one. If cooperation does exist between agencies then all can be reassured that learning counter deceptive tactics will only serve to enhance the protection of its classified and sensitive data from getting into the wrong hands and being vulnerable to unauthorized access by cyber criminals.

References

Amoroso, E.G. (2011). Deception. *Cyber Attacks: Protecting National Infrastructure*, *2*, 31-50. Retrieved from http://web.a.ebscohost.com.ezproxy.utica.edu/ehost/ebookviewer/ebook/bmxlYmtfXzM0NTcxM19fQU41?sid=87551448-c1e1-4483-bbfe-dbf3930ffc7d@sessionmgr4001&vid=1&format=EB&lpid=lp_31&rid=0

Bell, J. B., & Whaley, B. (1991). The Structure of Deceit: A Theory of Cheating. *Cheating and Deception,6*, 45-75. New Brunswick, N.J.: Transaction Publishers.

Bell, J.B. & Whaley B. (1991). Deceivers and Dupes: Profiles. *Cheating and Deception*, *4*, 97-112. Piscataway, N.J.: Transaction Publishers.

Bhatkar, S., DuVarney, D.C., & Sekar, R. (2003). Address Obfuscation: an Efficient Approach to Combat a Broad Range of Memory Error Exploits. *Usenix*, 1- 7. Stony Brook, N.Y.: Stony Brook University. Retrieved from https://www.usenix.org/legacy/event/sec03/tech/full_papers/bhatkar/bhatkar_html/

Bennett, M. & Waltz, E. (2007). Counterdeception Principles and Applications for National Security. In M. Dewar (ed.), *The Art of Deception in Warfare, 5,* 143- 181. Newton Abbot, London, UK.: David & Charles Pubs. Retrieved from http://www.artechhouse.com/uploads/public/documents/chapters/ben_waltz_935_ch05.pdf

Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). What is Deception? *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, 23- 247. New York, NY: The McGraw-Hill Companies.

Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). Foreword. Definition of Deception. In *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, Xvi-Xix. New York, NY: The McGraw-Hill Companies.

Bruce, J.B. & Bennett, M. (2008). Foreign Denial and Deception: Analytical Imperatives. In George, R.Z. & Bruce, J.B. (Eds.), *Analyzing Intelligence: Origins, Obstacles and Innovations*, 122-135. Washington, D.C.: Georgetown University Press.

Colarik, A.M., & Janczewski, L. (2006). Steganography. In M. Warkentin, M.B., Schmidt, & E. Bekkering (Eds.). *Cyber Warfare and Cyber Terrorism,* (5) 50-57. Hershey, N.Y.: Information Science Reference.

Colarik, A.M., & Janczewski, L. (2006). Deception in defense of computer systems from cyber-attack, Strategic Deception. In M. Warkentin, M.B., Schmidt, & E. Bekkering (Eds.). *Cyber Warfare and Cyber Terrorism*, (8) 99-102. Hershey, N.Y.: Information Science Reference.

Conallen, J. (1999). Modeling Web Application Architectures with UML. *Magazine Communications of the ACM*, *Vol. 42* (10), 63-70. New York, N.Y.: Association for Computing Machinery.

Danquah, P., & Longe, O.B. (2011). Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. *Journal of Information Technology Impact. Vol. 11*, 3, 169-182. Retrieved from http://www.jiti.com/v11/jiti.v11n3.169-182.pdf

Davis, J. (2008). Why Bad Things Happen to Good Analysts. In George, R.Z. & Bruce, J.B. (Eds.), *Analyzing Intelligence: Origins, Obstacles and Innovations*, 157-170. Washington, D.C.: Georgetown University Press.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, 17(1), 61-80. Boca Raton, FL: Information

Dunnigan, J., & Nofi, A. (2001). Deception and Trickery in War. In J. Dunnigan & A. Nofi (eds.) *Victory and Deceit*, (2), 1-342. San Jose, California: Writers Club Press

Systems Research.

Foltz, C. B. (2004). Cyberterrorism, Computer crime, and Reality. *Information Management & Computer Security*, *Vol. 12* (2), 154-166. Greenville, N.C.: Emerald Group Publishing Limited. Retrieved from http://www.emeraldinsight.com/journals.htm?articleid=862870&show=abstract

Giles, L. (1910). Chapter III, Attack by Stratagem. In L. Giles (ed.), The Art of War by Sun Tzu, 46-53. Portland, OR.: The Puppet Press.com. Retrieved from http://www.puppetpress.com/classics/ArtofWarbySunTzu.pdf

Griffith, S.B. (1963). Sun Tzu, In S.B. Griffith, (Ed.), The Art of War, 84. New York, N.Y.: Oxford University Press.

Headquarters Department of the Army (1995). Chapter 4: Counterintelligence Collection Activities, Control of Source Information. *FM 34-60 Counterintelligence*, (para. 4). Retrieved from http://www.fas.org/irp/doddir/army/fm34-60/f34-60_4.htm

Internet Crime Complaint Center (2014). Internet Crime Schemes, Nigerian Letter or "419". In Ic3.gov, para. 14. Retrieved from http://www.ic3.gov/crimeschemes.aspx

iPredator (2014). Online Deception. *iPredator.co*, *Q & A Online Deception*, (para. 6). Retrieved from https://www.ipredator.co/online-deception/

Kolisar (2008). WhiteSpace: A Different Approach to JavaScript Obfuscation. In *DEFCON 16*, 1-29. Retrieved from http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-kolisar.pdf

Kruger, D. (2012). Radically Simplifying Cybersecurity. *Absio, Persistent Information Ownership*, 1-7. Littleton, CO.: Absio Corporation. Retrieved from http://www.absio.com/sites/default/files/pdfs/Radically_Simplifying_Cybersecurity_V1.4.pdf

Lambert, D. R. (1987, October). 5.0.: Results, Discussion and Conclusion. *A Cognitive Model for Exposition of Human Deception and Counterdeception*, 15-16. Retrieved from https://www.researchgate.net/search.Search.html?query=A%20Cognitive%20Model%20for%20Exposition%20of%20Human%20Deception%20and%20Counterdeception&type=publication

Lynch, J. (2005). Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Cyberlaw*, 20. Berkeley Tech. L.J. 259. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/berktech20&div=36&id=&page=

Matusitz, J. (2005). Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age? *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy*, *Vol. 27* (2), 137-147. New York, N.Y.: NCAFP. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/10803920590935376#preview

McCarty, B. (2003). The Honeynet Arms Race. *Security and Privacy, IEEE*, 1(6), 79-82. New York, N.Y.: IEEE. Retrieved from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1253575&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F8013%2F28051%2F01253575.pdf%3Farnumber%3D1253575

McQueen, M.A., & Boyer, W.F. (2009, May). Deception used for Cyber Defense of Control Systems. *Idaho National Laboratory*, 1-9. Idaho Falls, ID.: Idaho National Laboratory. Retrieved from http://www.inl.gov/technicalpublications/Documents/4247207.pdf

Porch, D. & Wirtz, J.J. (2002, September 6). "Surprise and Intelligence Failure". *Strategic Insights*, 1-5. Monterey, CA.: Center for Contemporary Conflict, US Naval Postgraduate School. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA485164

Post, J.V. (1983). Cybernetic War. In O. Davies (Ed.), *The Omni Book of Computers & Robots*, 44-104. New York, N.Y.: Zebra Books Publishing

Proctor, P. E. (2001). Intrusion Detection Myths. *Practical intrusion detection handbook (6)*,100-130. Upper Saddle River, NJ: Prentice-Hall PTR. Retrieved from http://www.pearsonhighered.com/educator/product/Practical-Intrusion-Detection-Handbook-The/9780130259608.page

PRWeb (2013). Online Deception and Cyber Narcissism Paper. *PRWeb Newswire*. Retrieved from http://bi.galegroup.com.ezproxy.umuc.edu/essentials/article/GALE|A334678836/8a654bcf13a19c3b2c04609b3f2fd456?u=umd_umuc

Public Intelligence (2012). Executive Summary, Commander's Overview. Principles of MILDEC. *Joint Publication 3-13.4, Military Deception*, Vii-Ix. Retrieved from https://info.publicintelligence.net/JCS-MILDEC.pdf

Ragsdale, D. (2011). Scalable Cyber Deception. *DARPA*, 1-8. Retrieved from Defense Advanced Research Projects Agency (DARPA). Arlington, VA: Information Innovation Office. Retrieved June 12, 2014 from http://www.dtic.mil/dtic/tr/fulltext/u2/a551951.pdf

Roberts, E. (2012). Deception and the art of cyber security. *SC Magazine Awards Blog*, (para. 19). Retrieved from http://www.scmagazine.com/deception-and-the-art-of-cyber-security/article/229685/

Rowe, N. (n.d). Defensive Lies. *Deception in defense of computer systems from cyber-attack*. Paras. 1-13. Anapolis, MD.: U.S. Naval Postgraduate School. Retrieved from http://faculty.nps.edu/ncrowe/wardefdec.htm

Sophos (2004). Anti-spam specialist maps the spam world, Sophos outs 'dirty dozen' spam producing countries. *Sophos.com*, (para. 1-2). Retrieved from http://www.sophos.com/en-us/press-office/press-releases/2004/02/sa_dirtydozen.aspx

Stech, F., Heckman, K.E., Hillard, P., Ballo, J.R. (2011). Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space. *PsychNology Journal*. *Vol. 9,* 2, 79-122. Retrieved from http://eds.b.ebscohost.com.ezproxy.umuc.edu/eds/pdfviewer/pdfviewer?vid=3&sid=80f98d82-8003-4e74-93dc-4101162f1572%40sessionmgr110&hid=101

Taipale, K. A. (2007). Seeking Symmetry on the Information Front: Confronting Global Jihad on the Internet. *National Strategy Forum Review*, *Vol.16*, 1-8. New York, N.Y.: Center for Advanced Studies in Science and Technology Policy. Retrieved from http://ssrn.com/abstract=987040

Thompson, R. (2005). Why spyware poses multiple threats to security. *Communications of the ACM*, 48 (8), 41-43. New York, N.Y.: Association for Computing Machinery (ACM).

Yuill, J., Denning, D. & Feer, F. (2007). Introduction. *Psychological Vulnerabilities to Deception, for Use in Computer Security*, 1-14. DoD Cyber Crime Conference 2007. Retrieved from http://faculty.nps.edu/dedennin/publications/Psychological-Vulnerabilities-to-Deception--Yuill-et-al.pdf

Yuill, J., Zappe, M., Denning, D. & Feer, F. (2004). Honeyfiles: Deceptive Files for Intrusion Detection. In *Calhoun, Instutional Archive of the Naval Postgraduate School*, 1-8.

Monterey, CA: Dudley Knox Library. Retrieved from http://calhoun.nps.edu/public/bitstream/handle/10945/37180/honeyfiles.pdf?sequence=1