Defense in Depth: Perspectives on utility security from a military intelligence viewpoint

Albert H. Carlson
Senior Project Engineer
POWER Engineers, Inc.

Abstract: Electrical utility security and national security are closely related, sharing many of the same characteristics and needs. Effective critical asset protection and proactive defense against a variety of threats are high among these common needs. Military Intelligence has more than a 225-year history of protecting critical national assets. The Intelligence Community pioneered the concept of "Defense in Depth" and directly shaped modern security practices. Until the 9/11 attacks, an assault against a utility facility was considered a possibility only during a time of declared war. Various groups now consider themselves permanently at war with the United States and its allies, prompting the U.S. government to mandate extensive security measures for critical infrastructure protection (CIP). This paper explores what can be learned from the Intelligence Community to facilitate securing utility facilities. Beginning with the "Defense in Depth" strategy, followed by a discussion of Intercept, Destroy, Disrupt, and Takeover (IDDT) analysis – a method that identifies and classifies threats – and using classic historical examples, this paper makes practical suggestions about how to evaluate and strengthen the defense of a utility facility against intelligence gathering, intrusion, and disruption of utility operations.

1.0 Introduction

On Nov. 28, 2008 a single intruder scaled two electrified ten-foot-high razor wire protected fences at the Kingsnorth coal-powered generation station in Kent, England [1]. After bypassing the £12M perimeter defenses, and in full view of CCTV cameras, the man entered through an unlocked door and manually shut down a 500MW generator. The intruder, dubbed the "green Banksy," then exited the station in the same manner he entered. The note left by the man indicated that his motivations were political and that he wished to reduce carbon emissions from "dirty" coal. Despite the expensive protection mechanisms, no lock was placed on the door to the critical and sensitive asset. Defenses were concentrated at the perimeter. Once breached, there were no further barriers to prevent the intruder from carrying out his plans. There was no, in military terms, "Defense in Depth."

This paper explores what can be learned from the Intelligence Community to facilitate securing utility facilities. Beginning with a detailed discussion of the "Defense in Depth" strategy and then exploring the concept of IDDT analysis, practical suggestions are made to evaluate and strengthen the defense of a utility facility against intelligence gathering, intrusion, and disruption of utility operations. The paper will examine historic cases where military organizations both used and ignored defense in depth strategies with predictably varying results.

2.0 Background

Information Assurance (IA), a term used synonymously with information security, is concerned with the management of risks to information. IA seeks to identify and control risks to the confidentiality, integrity, availability, and non-repudiation of information [2]. Rather than concentrating on the mechanisms and tools needed to implement protection, IA focuses on the policies, procedures and governance necessary to minimize risk and provide for the restoration of information.

The primary goals of IA include Confidentiality, Integrity, Availability and Non-repudiation. Confidentiality seeks to keep information secret from unauthorized individuals. Integrity seeks to ensure that information is not changed. Availability seeks to ensure the access to information at all times for authorized users. Non-repudiation seeks to be able to identify users at all times. At times these goals may conflict, so priorities must be set with respect to each goal. For IA, Confidentiality of information is the primary goal, with the Integrity of the information next in importance, and Availability of computing asset or information is least important.

Military Intelligence (MI) is the process of gathering information [3] to gain a tactical or strategic advantage over an enemy, to deny the enemy the ability to gather tactical or strategic information against friendly forces, and to protect resources vital to the military operations of friendly forces. Although practiced since ancient times during periods of national conflict, MI has not been a full-time pursuit until relatively recently [4].

Traditionally, intelligence work was coordinated by individual unit commanders, but met with mixed results [4] when operating independently of national oversight and direction. Coordinated intelligence gathering, analysis of the data, and actions based on the information collected by individual sources was impossible until a centralized intelligence authority was established and supported at the national level. Duplication of effort and an incomplete picture of the situation often resulted. The U.S. did not possess such an intelligence structure until the mid to late 1880s, and then only sporadically maintained an intelligence apparatus until a permanent Military Intelligence Corps was established in 1967 [4]. The prevailing opinion during the period preceding the establishment of the permanent MI Corps was, according to U.S. Secretary of State Henry Stimson, that "gentlemen do not read other gentlemen's mail" [5].

Prior to World War I, the role of MI was largely restricted to gaining tactical advantage on the battlefield. Gathering sensitive information required defeating the enemy's security to gather documents or gleaning information from enemy personnel (Human Intelligence) [3]. Advances in communication and transportation technology made the interception of signals increasingly important. Codes and ciphers (Signal Intelligence) [3], previously restricted to strategic concerns became tactically important as well. Auguste Kerckhoffs [6] laid out the principles of the use of cryptography in MI, firmly placing electronic intelligence [3] in the realm of MI in 1883. Tactical communications also became an MI concern with the advent of portable wireless communications for battlefield units. When data began to be produced, stored, consumed, and transmitted using computers, IA and MI interests intersected. Digital control of weaponry and digital data transmission triggered the inclusion of network communications under the umbrella of MI concerns. The proliferation of technology in weaponry and the focus of interdicting the delivery and use of key resources also shifted the role of intelligence services toward the protection of vital resources, manufacturing, and support services.

Now, MI organizations are typically responsible for the physical security of sensitive facilities, the physical security of sensitive documents, interception and analysis of enemy signals, protection of the confidentiality of friendly signals, signal encryption for friendly signals, signal decryption of both friendly and enemy signals, photo analysis of enemy positions, interrogations of enemy personnel, investigation of security breaches, intelligence gathering, and counter intelligence. Each area of responsibility gathers (intercepts) information about the enemy, takes over enemy assets, disrupts the use of enemy assets, denies the enemy use of their own assets, or denies the enemy information or access to friendly assets, following IDDT principles, which this paper will discuss later.

MI tasks are both offensive and defensive in nature. The Intelligence function of MI is offensive, seeking to gain intelligence from the enemy. Counter intelligence (CI) [3] is defensive and is primarily concerned with defending friendly information, persons, and facilities from enemy exploitation. At the same time, the job of CI is to discover and eliminate enemy personnel involved in intelligence functions against friendly forces.

2.1 Defense in Depth

"Defense in Depth" was a term coined in the military and then borrowed by the discipline of Information Assurance to describe a method of protecting a computing network [7]. As part of the CI effort, MI uses the "Defense in Depth" [8] concept – layering defensive measures and checks in order to increase the difficulty for an enemy to penetrate those defenses. In general, a "Defense in Depth" is a coordinated line of defensive measures meant to coordinate with each other in removing one type of attack at each position, slowing and blunting an attack until it is defeated. Many different types of defenses are employed, making it difficult for an attacker to be successful using a single tactic.

While the definitions from the two fields differ slightly in meaning and application, the IA and military terms share many of the same motivations and goals. The military practices information security in a variety of environments world-wide as part of its regular operations. Intelligence provides a practical laboratory to develop and assess security practices applicable to utility assets.

2.1.1 The Military Intelligence Term "Defense in Depth"

The military concept of Defense in Depth arises from the need to defend a broad Forward Edge of the Battle Area (FEBA, or front line) as well as a substantial undefended area behind the lines, which is susceptible from attack and recapture by enemy forces. The greater the area behind and wider the front exposed to enemy attack, the greater the chance a breakthrough may succeed. A wide front line means that defending units must be spread thinly to repulse an attack that can occur anywhere on the FEBA. If all the defending troops are concentrated on the front lines, a successful attack through the FEBA gives the attacker the opportunity to flank the defenders or make a sustained drive into the undefended rear of the line. Rather than risk the damage that comes with flanking or envelopment, layers of defensive positions and units are deployed. Each layer is designed to blunt an attack and inflict as many casualties as possible before being broken or overrun. If possible, each defensive layer seeks to target one key element of the attack and destroy it. Since the attack on each layer takes time and reduces the attacking force, the defender can then commit his reserves to the right place in strength to repulse the attack.

Military units are placed in positions that take advantage of terrain to multiply the defensive strength, maintain flexibility in deployment, direct the attacking force to the next defensive layer, and retain fresh reserves. An attacker meets the first layer of defense and may break through after sustaining losses. While the attacker is engaged with the defensive position, that position reports the attack and allows the commander to allocate resources to help repulse the attack. Backup units are either sent up in support of the first line position or to the next defensive position in anticipation of a breakthrough.

2.1.2 The IA Concept of "Defense in Depth"

The concept of Defense in Depth for IA is defined by attempts to defend a network against attacks from unauthorized users. Attacks may include passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through IT providers. The results of attacks are to either gather information, deny the legitimate user access to data or services, or to use network assets for a purpose other than what the owner of the network intends. Since the *results* of human-caused attacks are similar to the results of fire, flood, power outages, and user errors, the latter are often included in the same category as "attacks."

The primary goals of IA are to ensure the availability of data and data-processing equipment, maintain the integrity of information, maintain confidentiality of data, and assure non-repudiation [9] of a data source. With a successful IA program, data is protected, attacks are detected, and the system reacts to any detected threats. The primary factors for achieving successful IA goals are people, technology, and operations. The primary considerations for each include:

- *People* – Includes the training of personnel, personal security awareness, physical security awareness, facilities countermeasures, security of personnel, and the administration of personnel having access to sensitive information.
- *Technology* –Includes the architecture of the network and computing system; system risk assessments; and the evaluation, acquisition and integration of products into the computing environment.
- *Operations* - Includes the development and deployment of policies, procedures, and security policies; readiness assessments; incident recognition and recovery; network reconstitution; and the management of operations.

In order to achieve its desired goals, IA deploys a layered defense with selected detection and protection mechanisms in each layer. Each layer is designed to blunt one type of attack. For instance, a firewall is set at the perimeter of the network to trap and eliminate communications coming from sites determined to be dangerous. Inside the firewall, but before access to the network, a challenge/authentication mechanism filters out many unauthorized users from entering the network using an approved IP address. Each layer is also monitored to detect attacks and the results recorded for forensic analysis. Any attacks detected are dealt with according to a predetermined security policy by assets held in reserve for the prescribed defensive action. In order for an attacker to enter the network, the attacker must first successfully defeat the barrier(s) at each layer.

2.1.3 Comparing and Contrasting Military and IA Defense in Depth

In both definitions of "defense in depth," a defense is layered. Layering the defenses allows the detection of an attack, coordinating the resources, and directing the defenses against specific targets (filtering). However, the IA definition of defense in depth includes the monitoring, logging, and eventual forensic analysis of the attack, where such recordings may not be possible in a military environment. The types of units involved in the defense are also divergent. IA employs relatively stationary resources whose attack vector comes from known, and limited, sources while military defenses are fluid and relatively mobile. Attacks on a front can come at any point on the front.

The priorities of the military and IA also differ. The military is primarily concerned with the availability of their defensive assets, since an asset cannot be used if it is not available. The next concern is the integrity of the asset – whether the asset is totally functional and works as anticipated. Finally, the confidentiality of information from the asset is considered. The order of importance—Availability (A), Integrity (I), and Confidentiality (C), or AIC—is completely the opposite of the priorities of IA. IA organizations may, to keep confidentiality, restrict availability or information integrity (CIA or CAI, depending on the organization).

The military and IA concepts of defense in depth are alike in many ways. Both defensive strategies attempt to protect an open and vulnerable set of resources vital to the operation of the protecting forces. For the military, resources include recruits, food, fuel, ammunition and spare parts. For an IA staff, resources include a network, data, and computing equipment essential to communications and the effective utilization of information.

Both the military and IA face attacks meant to meet the goals of their attackers, which are meant to gain some advantage for the attacker. The attack may seek information, attempt to deny the commander, or user, the legitimate use of assets, or may attempt to convert the enemy's units to serve the attacker's goals. While Defense in Depth is the strategic method, IDDT analysis determines what defenses are implemented and how the defenses are ordered.

2.2 Intercept, Destroy, Disrupt, and Takeover Analysis (IDDT)

IDDT is a system that seeks to classify attacks by their purpose. Attacks fit into one of four categories:

1. *Intercept (information)* – Attacks are considerably more likely to succeed with increased information about a defensive position, equipment, or strategy. Efforts to increase tactical and strategic information can include intercepting transmitted information (Signal Intelligence), intruding into a network in an effort to convince the enemy/user to reveal sensitive information that they would not normally reveal (social engineering, or human intelligence), or gathering data on the technical specifications or operation (or electronic intelligence) of equipment.
2. *Destroy* – Destruction of an asset permanently renders the defender less able to fend off subsequent attacks. Assets may not be immediately replaceable, thus giving the attacker an advantage during subsequent attacks.
3. *Disrupt (or Deny)* – Disrupting or denying the use of an asset temporarily renders the defender unable to employ the asset for defensive purposes. Disrupting the use of the asset may be much easier than attempting to destroy the asset, requiring less effort and resources to accomplish than simply destroying the unit. Disruption can be accomplished using social engineering methods, as well as by direct intervention.
4. *Takeover* – Seizing control of an enemy asset and using it in the attack denies the defender a unit and forces the defender to assign units to detail other defending units to deal with the rogue unit. A unit acting as an agent of the attacker doubly reduces the defending force. A takeover attack is often accomplished using social engineering.

The selection of one type of attack versus another rests on the goals of the attacks, enemy preparation and readiness, equipment, methods, and the talents of the personnel available to accomplish the attack. All of the attacks must be evaluated in terms of the cost of the action. If the cost to accomplish the attack is too great, the attacker may compromise his own resources

and be unable to press an attack. IDDT analysis is a method that evaluates possible actions available to an attack in each category. By exploring possible attacks, the defender is able to identify vulnerabilities and take the necessary steps to avoid exploitation by an attacker. As we will see later, IDDT analysis can be applied not only to MI, but also to IA in a utility setting.

2.3 Utility Security

In 1965 a major blackout struck the New York/New England area. As a result, reliability of the bulk power system (BPS) became an industry priority [10]. The federal government responded to the blackout by enacting regulations meant to encourage and ensure reliable transmission and delivery of electrical power. More than a full generation of electrical utility professionals labored to ensure power availability and enact measures preventing power disruption from vegetation, poor maintenance, and lack of redundancy. Part of the process of making the Bulk Power System more reliable was the addition of control technology, in terms of Supervisory Control and Data Acquisition (SCADA) and protective relays. Adding the new technology improved reliability, but also added remote communications and a control network that allowed experience operators to react more quickly and accurately to dynamic conditions on the power grid.

The attacks of September 11, 2002 [11] revealed a new reliability threat – intentional human destruction of a building, facility, or asset. Destruction of bulk power assets disrupts power generation and distribution without prior warning, and therefore renders the power system unreliable. In an assessment of the state of the nation's vulnerabilities [12], the U.S. government identified critical infrastructure sectors. Among the sectors was the Electrical Production and Distribution, or BPS. Electrical power is now considered key to effective operation of the U.S. and is used in many of the other critical infrastructure sectors.

Shortly after the 9/11 attacks a demonstration at the Idaho National Labs (INL) brought the Aurora Vulnerability [13] to the attention of Congress and the American public. The demonstration raised the question of whether or not it was possible to affect the operation of utilities using cyber attacks. Of particular interest was the possibility of remote strikes from individuals, or nations, to vital national assets. The response to the attacks and testimony in front of Congress was the Critical Infrastructure Protection standards [14] administered and enforced by the National Electric Reliability Council (NERC) and the Federal Electric Reliability Council (FERC). The CIP requirements cover physical, electronic, and communications security, as well as personnel, training, and systems management. Most reliability standards directly address maintenance, power equipment operation, generation, transmission, or distribution. CIP standards deal with the supporting communications and automated control systems. Despite the differences, both standards are concerned with different aspects of total system reliability. More specifically, CIP standards directly address increasing reliability by dealing with problems that are intentionally introduced by human agents (See **Figure 1 CIP and Reliability**).

Rather than addressing cyber security as a monolithic subject, different facets of cyber security are treated separately. The CIP standards consider a layer of physical security (CIP 006), a layer of electronic security (CIP 005), personnel considerations (CIP 004 and CIP 007), personnel training for security (CIP 004), electronic systems security (CIP 003), security incident reporting (CIP 008), and recovery plans in the event of a security incident (CIP 009). Thus, CIP standards essentially constitute a defense in depth arrangement.

Utility security has the task of ensuring that equipment and personnel remain safe to perform their jobs reliably and to prevent events that would endanger the operation of the BPS. Utility

security covers threats to physical facilities, assets, and personnel from any source. CIP is essential to utility security and reliability.

Utility security and MI are both responsible for protecting vital national resources. Each integrates cross-functional security measures, coordinating information and actions from multiple sources. The long history of MI provides many examples that serve to illustrate lessons that can be learned from the techniques employed by the MI community.

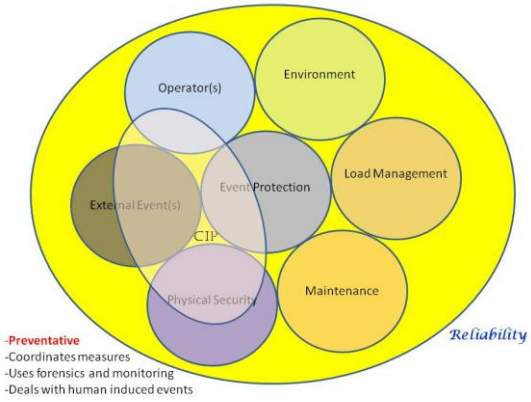

Figure 1 CIP and Reliability

3.0 IDDT Analysis

Every attack has strengths and weaknesses. A defender must know what those strengths and weaknesses are in order to defeat the attacker. Inappropriate defenses are ineffective. Knowing the vulnerabilities of the attacker and countermeasures that exploit the vulnerabilities allow the defender to design a defense incorporating that knowledge into a barrier against the attack. Defending a communications or control network against a cracker employs the same methodology. The approach is described in the military as, "Know your enemy."

Just as a military commander employs intelligence assets to prepare a defense, a similar IDDT analysis can be used to protect utility assets. The steps to applying IDDT are:

1. *Select an asset to defend.* The asset defines the physical and network terrain that must be protected. Each asset has operational needs that must be examined for possible avenues of attack by an enemy. This includes the parts making up the asset: fuel, lubrication and routine maintenance needs, control systems, communications media, and interface requirements.
2. *Compile list of asset vulnerabilities using IDDT.* A list is then compiled of all the ways the asset is susceptible to Intrusion, Destruction, have service Denied or Disrupted, or be Taken Over by an outside agent. This step in the analysis is not meant to be a detailed attack, but rather how the asset is Disrupted, Denied to users, etc.
3. *Compile a list of threats based on vulnerabilities.* For each item in step two, list all of the ways to realize the item on the list. Each implementation that causes the action is an attack. Do not limit the attacks to those which are "probable" or are presently technically feasible. Technology has a way of changing unexpectedly.
4. *List countermeasures to threats.* For each attack, list the countermeasures that prevent the attack from occurring.

5. *Rank order countermeasures.* Rank order by ease of running the attack, then by the cost countermeasures to the attack. This list will help design the defenses for the system.
6. *Find countermeasures stopping multiple attacks.* Correlate which measures can prevent multiple attacks. If a defense prevents multiple attacks, and the cost of using the measure is less than that of implementing separate measures for each of the attacks, use that defense.
7. *Select defenses.* Select the defenses to be implemented. The time and cost involved in putting defenses in place dictate that only a subset of the possible defenses will ever be used. And, because new attacks are created constantly, it is impossible to defend every attack. The choice of defenses should be made to cover as many credible attacks, starting with the most credible, for the allocated budget.

Once IDDT analysis is completed, the list of attacks should be retained for future review and periodic adjustments should be made to cyber defenses based on those reviews.

An effective IDDT analysis must also consider the risks inherent to attacks. Risk analysis means assigning two measures to each attack threat: probability of the attack taking place and the cost of a successful attack. The probability of an attack varies between zero and one, while the cost of an attack is in the local currency and should include the cost of replacing components, labor associated with addressing the attack and its aftermath, lost revenue, personnel costs, and also account for the lead time for procuring replacement parts. Multiplying the risk probability and the cost gives a relative measure that may be used to rank order attacks for the purpose of planning defensive measures.

It is worth noting that the U.S. government uses a consequence-based assessment rather than risk assessment in CIP. A consequence-based assessment sets the probability to one, effectively ranking ordering attacks by their potential costs. By making the probability one for all threats, the government is asserting that, over time, all attacks will be tried. It is just a matter of time [15]. IDDT considers all attacks without regard to probability. Based on lessons from history, consequence-based analysis has proven effective in predicting attacks dismissed by other approaches.

4.0 Examples and Lessons Learned

Even though risks are correctly identified, defenses can fail to fully protect an asset. Numerous examples can be found in the history of the military where security failed. In each case, MI was integrally involved in the action. Through each of the selected examples below, the principles of IDDT are applied and lessons are drawn.

4.1 The Maginot Line (Construction begun 1930, invasion May 10 – 24, 1940)

Background: At the end of World War I (WWI) the French Government, based on its experiences of the war, especially static trench warfare, built a defensive line on the borders of Germany and Italy [16]. The line, which became known as the "Maginot Line" – named after the French Minister of Defense who was successful at getting approval for the project – was actually a series of positions which together constituted a defense in depth. The line was intended to slow, or stop, the advance of an attacking army with a small defense force manning concrete and steel fortresses backing up infantry barriers and machine gun emplacements. Supply depots, with narrow gauge rail lines, were located for quick and secure delivery of material and personnel. The line was manned by a minimal contingent of men. The

opinion of most military and political leaders in France, and in the remainder of the world, was that the Maginot Line was impregnable.

MI Involvement: Nazi leaders planning the invasion of France faced a strong defense in depth along their mutual border. The assessment of the Abwer (Nazi MI) was that an attack along the line would result in massive casualties and slow the invasion down long enough to allow significant reinforcements to arrive. Their analysis showed that the defenses behind the Maginot Line were minimal. The recommendation was to place a diversionary force along the line and send the main invasion around the northern border of the Maginot Line through the Netherlands and Belgium to flank the line and then attack it from the rear.

Result: The attack on the Maginot Line was highly successful. Since the French had not fortified the Franco-Belgian border, the Nazis were able to quickly come in behind the line and isolate it from the invasion. Fourteen days from the initial invasion, German forces were digging in for the attack at Dunkirk. About five weeks after the invasion, France surrendered and French forces were ordered to surrender the Maginot Line. Germany had isolated the line without having to attack it directly. The result was the Maginot Line was effectively eliminated from any defensive relevance, although it probably could not have been defeated by the Germans in a direct attack.

Lessons Learned:

1. *While defense in depth will work, the defense must also be flexible enough to face any attack.* Static defenses can be pointed in the wrong direction and be bypassed.
2. *Defenses can be flanked.* This is especially true if the defenders do not evaluate the possible avenues of attack (IDDT analysis).
3. *A flanked defense is a useless defense.* A defensive measure that cannot be used in the defense is a waste of resources and is has no effect on an attack.
4. *Attackers would rather flank a defense than face it head on.* If a defense can be bypassed, less effort needs to be expended. Hackers, like attackers, prefer to expend the least amount of energy necessary to accomplish their goals.

Applying the Lessons to the Utility:

Several lessons learned from the Maginot Line can be applied to the defense of utility assets. The Maginot Line was a static defense that assumed that the only attack possible on the line was a frontal attack. While the assumption was true when the line was designed and first built, technology advanced between construction and the German flanking attack. Tanks, originally clumsy, slow, and relatively lightly armored, benefited from improvements that greatly enhanced speed and maneuverability. Airborne troops became a part of the attack force, allowing men and material to be delivered behind the line without having to assault positions. Unable to reposition the guns of the line, the line became a fixed position that could be bypassed during an attack. Several military commanders in France, including Charles de Gaulle, warned of the vulnerability, but their opinions were dismissed by government planners and administrators. Defenses deployed to protect an asset must not remain static. Technology constantly improves the tools of an attacker. If the defenses are not altered to keep up with new attack capabilities, the defense is likely to be bypassed.

Static defenses were not the only serious flaw in the design of the line. The Maginot line only protected the Franco-German border. No such defenses were placed on the borders of France and the Netherlands and Belgium. Germany shared borders with both countries and invaded the lightly-defended countries. German forces could then enter France at a point the Maginot Line

was not built to defend. Defending only one portion of the perimeter is ineffectual. Unless the entire perimeter is defended, the enemy will find a way to enter and attack.

Defending a utility has similar difficulties. Dealing with the need to protect the perimeter of the facility and assets can take the form of the following actions:

1. Make sure a written policy, approved by management, is in place for identified threats. When a threat is identified and evaluated the IA/IT department can then immediately take action to deal with the threat without having to wait for management approval.
2. Inventory the network topology for all physical and logical ports. Accurate records on the state of the network topology help to analyze and implement changes to the present state of defenses. Attacks are constantly evolving—so should the network response.
3. Physically disconnect media from any unused port on hubs, switches, and routers. External attacks require an entry point. Eliminating, or reducing, the possible entry points substantially reduces the risk of external attack.
4. Run a port scan on all computers that communicate outside of the Electronic Security Perimeter. Note those ports that are active. Knowing which ports are active allows a faster response. Not all active ports are reported by vendors, leaving an entry point that may be overlooked.
5. Access points include logical ports on computers for application service. Each computer has up to 65,536 logical ports. Disable all ports that are not used for applications on the computer. Each open port is a potential attack vector for hackers.
6. Regularly run the inventory on ports. At the same time as taking port inventory, assess all applications on computers. Remove any applications that are no longer needed and disable the associated logical ports.
7. On at least an annual basis, inventory the network security measures in place. Rerun IDDT analysis to catch new attacks developed since the last inventory and reprioritize the defensive measures to the likelihood of threats. Threats are evaluated according to the cost of a successful breach and the likelihood of such a breach occurring. Ensure that the software is up to date (latest known good revision) and still efficient at preventing the breaches for which they were selected. Replace software as required. A review should also take place after every successful breach of the network.
8. Place a summary of the review, signed by the person(s) conducting the review and the manager certifying the review, in permanent records. Managers are responsible for being able to explain the results to senior management. Senior management should ensure that regular reviews take place.

4.2 Pearl Harbor (December 7, 1941)

Background: The Japanese signed the Tripartite Pact of 1940, signaling their desire to control the destiny of the Asian and western Pacific [17]. In response to this, and other subsequent actions on the part of the Empire of Japan, the U.S. restricted exports to Japan. The Japanese responded by carrying out an attack on the U.S. Navy Pacific Fleet at Pearl Harbor, Hawaii, in December of 1941. The Japanese, inspired by the successful British attack at Taranto, Italy [18] in 1940, conceived of a plan to eliminate the U.S. Navy Pacific Fleet. Although the attack at Pearl Harbor is often called an "intelligence failure," many indicators were noted, and sufficient analysis offered, that refute the assertion.

MI Involvement: Intelligence played a large, but eventually ineffectual, role in the attack on Pearl Harbor. The Japanese diplomatic and military codes had been broken, allowing the U.S. to

see the preparation for the attack. Col. Rufus Bratton, head of Army Signal Intelligence for the Far East at the Pentagon, led an effort to convince high-level commanders that an attack in the Pacific was imminent, although it was generally thought that the target would be the Philippines. Officers in charge of Pearl Harbor, and its defenses, believed that it was physically impossible to attack the fleet because of the shallow depth of the harbor compared to Taranto (35 feet versus 85 feet). Officers favored the conventional view that the local ethnic Japanese population was the greatest threat to security.

Many clues about the impending attack were ignored at various levels of command and control. Radar data (Electronic Intelligence) on incoming aircraft was mistakenly ignored, reports of submarine activity were delayed for confirmation, and increased levels of signal traffic were also ignored.

Results: On December 7, 1941 the Imperial Japanese Navy (IJN) successfully attacked the U.S. Pacific Fleet and inflicted serious damage. The main targets of the attack, the aircraft carriers, were not in the harbor at the time

Lessons Learned:

1. *Technical changes make new attacks and variants of old attacks possible.* Technology must be closely watched to indicate when attack conditions change.
2. *Never underestimate the enemy*. Biases about the ability of the Japanese caused commanders and defenders to discount warnings of an attack because the commanders found the warning not "credible" due to preconceived notions about ability.
3. *Respond quickly.* Delays in decision making cost valuable time in warning about the attack. By the time the decision makers responded the attack was underway. Written response plans allow faster response.
4. *Think outside of the box.* The Japanese developed novel approaches for reaching their goals. Defenders relied on conventional thinking and were surprised by the type and focus of the attack.
5. *Treat all information as vital to understanding an attack and creating a defense.* Discounting information as "irrelevant" before an attack can result in defending against the wrong attack.

Applying the Lessons to the Utility: One of the more interesting lessons from Pearl Harbor has to do with technology and innovation. Change to the status quo is a rule. In response to new problems, new solutions are developed. The mindset needed to develop radically new approaches ("disruptive" technology or ideas) begins with denying the idea that something is "impossible" because it has not previously been done. Change happens when impediments to keep something from happening are systematically identified and then removed. Conventional thinking only leads to conventional solutions. When the Japanese identified the problem with torpedoes delivered by aircraft needing more depth to level off than was available in Pearl Harbor, they developed a way to deliver torpedoes with a wood stabilizer that acted as a water parachute and allowed torpedoes to operate at shallower depths.

U.S. commanders also relied on their biases about the ability of Japanese engineers and manufacturing. Conventional analysis at the time proclaimed it impossible that such innovation could come from Japan. As a result, U.S. command personnel dismissed all gathered evidence that an attack was planned on Pearl Harbor. Any evidence contrary to conventional thought was dismissed as irrelevant and fanciful. The result was nearly the destruction of the Pacific Fleet and complete domination of the Pacific by the IJN.

The U.S. was also slow to respond to the information indicating an attack was imminent. The command structure evaluated all information and then issued warnings, but the warnings came far too late to be of use.

1. Encourage "disruptive" ideas and analysis by security personnel. Ideas that are unconventional should be investigated and tried. Not all ideas will work, but those ideas that prove effective should be adopted. Allowing security personnel to try ideas will also improve moral.
2. Set aside time for security personnel to investigate technological changes and approaches to security. If possible, allow security personnel to attend conferences, such as Defcon, and training related to securing information. Untrained, or poorly trained and uninformed security personnel, will be "surprised" by innovation in attacks. The result is an increased number of security breaches and damage resulting from attacks.
3. Set up policies, plans, and procedures ahead of time to address potential road blocks in responding to security breaches. Each policy, plan, or procedure should address a single area, be brief as possible, and empower action at the lowest practical level for decision making. All policies should be reviewed on a regular basis to keep them current and be easily accessible.

4.3 Midway (June 4 – 7, 1942)

Background: Six months after Pearl Harbor the Japanese attempted to capture the atoll of Midway in the Pacific Ocean. The goals of the operation were to deny the U.S. a base from which to launch air attacks against Japan, provide a forward base for operations in the Solomon Islands, and to lure U.S. aircraft carriers into an ambush.

MI Involvement: U.S. Naval Intelligence had broken the JN-25 [19] Code of the Japanese prior to World War II and had been intercepting enemy naval traffic. In analyzing the traffic, CDR John Rochefort (in command of the code-breaking effort) was able to determine the target of the attack by using a false (spoofed) message. Chester Nimitz, in command of the Pacific Fleet, was also given the Japanese order of battle and an approximate date of the attack. Although the Japanese changed their code prior to the Battle of Midway, Rochefort's crew was able to partially break the new code. Rochefort could read about one in fifteen words [20] encrypted by the Japanese.

The IJN suffered from incorrect data and intelligence analysis following the Battle of Coral Sea one month earlier. The Japanese believed that the Lexington was either sunk or could not be repaired rapidly if still afloat. The Lexington had returned to Pearl Harbor and was repaired sufficiently to allow it to participate in limited offensive action within 72 hours of docking. The ship provided a vital air platform for the operation. Intelligence gathering assets also missed the deployment of U.S. Navy aircraft carriers near Midway.

Result: The U.S. Navy set up its own ambush and delivered a decisive blow against the IJN. The Japanese lost four carriers and a heavy cruiser against the loss of one aircraft carrier and destroyer for the U.S. Navy. The IJN never recovered from the loss.

Lessons Learned:

1. *Intercepted information has value.* Even small, seemingly unimportant, and infrequently revealed pieces of information can be used against an organization. Hackers often collect information from a variety of sources that is used to help target an organization. Some information is used directly in the final attack, while other information is used as a way to collect more sensitive information.

2. *Know your enemy.* The more knowledge that you have about an enemy, the more effective the defense. Assumptions made about the attack or the attacker can overestimate—or underestimate—the situation. Overestimating the attack(er) leads an overly aggressive, and costly, response, while underestimating the attack(er) leaves vulnerabilities and exposure to exploitation.
3. *Knowledge is a defense multiplier.* Even with a parity of force the U.S. Navy achieved approximately a 10:1 ratio of damage.

Applying the Lessons to the Utility: Midway is an example of the power of information and intelligence analysis. Information was gathered by U.S. Naval Intelligence and assembled in the analysis phase to allow a tactical reversal. The information gathered, though small and facilitated by lax key changes, was enough to change the course of the war.

1. Utilities should check their public information exposure to reduce the amount of information that a potential attacker can gain through open source collection. Employees should also be trained not to give the names, positions, or other information to unknown, unauthorized persons.
2. Use encryption on communications and change the key often. The IJN believed their cipher to be unbreakable and were lax about changing the key. Frequent key changes deny an attacker information until the cipher is again broken. Statistical analysis of the time required to break a key is the guide for how long a key should be employed for encryption prior to change.
3. When planning or responding, gather as much information about the attack(er) as is possible and err on the side of caution. Gather intelligence on the attack(er) the same way that the attacker would on your facility. Make data collection and analysis part of your defensive plan.

4.4 The Korean Invasion (beginning June 25, 1950)

Background: After World War II the Korean peninsula was administered by the Soviet Union north of the 38th Parallel and the U.S. south of the same line. Under the influence of both nations separate governments reflecting the political ideology of their respective administrators developed. Both governments desired unification under their own direction. By 1946 [21] the Democratic People's Republic of Korea (DPRK, North Korea) had begun regular border skirmishes into the Republic of Korea (ROK, South Korea). In early 1950 the DPRK began massing troops along the border with the ROK, evacuating civilians out of the area, and began to station Russian T-34 tanks [21] at the border. Other indications of impending invasion were a lull in cross-border incursions and an increase in the propaganda coming from North Korea.

On June 25, 1950 a massive force of North Korean soldiers left forward positions and invaded the ROK. Both the U.S. and ROK were caught by surprise.

MI Involvement: An active intelligence detail was stationed in Korea prior to the eruption of the conflict. The detachment correctly analyzed the ample intelligence and predicted an invasion in the spring of 1950. More than 1,200 reports were issued in support of the prediction. However, the command structure in Korea were desensitized to the border incursions due to their frequency, believed that the ROK forces were far superior to DPRK forces, and misjudged the ability of T-34's to negotiate rice paddies and the terrain of South Korea. The command structure actively disagreed with intelligence analysis and forwarded reports indicating their analysis. Announcements of Korea-wide elections made by Kim Il Sung for August 1950 were also dismissed as propaganda.

Result: The surprise attack caught an under prepared and equipped force of the ROK, overrunning defenses and pushing the ROK Army back to the Pusan area. The situation was not stabilized until United Nations (UN) forces entered the conflict. Superior UN forces pushed the DPRK forces back into North Korea. Once UN forces crossed the 38th Parallel, Chinese forces joined the action. The invasion ended at a stalemate with the border approximately where it was prior to the invasion.

Lessons Learned:

1. *Do not regard probing attacks as a routine occurrence.* Probing attacks often means a potential attacker is searching for a weakness to exploit and will continue until a vulnerability is found. Upper echelon command structure came to regard the action at the borders as routine, dismissing it as an indication of further action. This is similar to attacking an Intrusion Detection System (IDS) by making the unusual common and then using the action as an attack vector.
2. *Avoid biases.* The command structure chose to believe a small body of contradictory indicators over a massive body of evidence indicating invasion and the analysis of their intelligence/security specialists.
3. *Listen to the experts***.** Senior commanders dismissed the analysis of experts in their field because the analysis did not fit their biases. Intelligence personnel were marginalized as "not credible" because of a view that intelligence/security personnel could not make it in other mainstream job functions.

Applying the Lessons to the Utility: The invasion of South Korea teaches lessons about the interaction of senior management and security staff.

1. Designate a senior management member to be in charge of security. The manager tasked with security must have the authority to act on threats and react to incidents. The security function requires the credibility and partnership that come from senior management backing.
2. Hire qualified security professionals to design and run security functions. Make sure all security positions are staffed at least two deep. Remember that security personnel need constant training in order to stay current with new developments in the field.
3. Make it a practice to consider and list all possible biases during analysis. Awareness of biases is the first step to overcoming them.

4.5 The Trojan Horse (circa 1200 BC)

Background: According to legend [22] Paris of Troy was promised the hand of the Helen of Greece by Aphrodite in exchange for choosing her as the fairest among her, Hera, and Athena. After visiting Helen's husband, Menelaus, Paris kidnapped Helen and took her back to Troy. Menelaus rallied his allies and, after exhausting diplomatic avenues, entered into a decade-long war against Paris and Troy. The Greeks began by cutting supply lines to Troy and had to defeat Troy's neighboring kingdoms in order to lay siege to the heavily fortified city. Despite several years of siege and intermittent attacks, the Greeks were never able to breach the defensive walls and only rarely able to enter the city on other missions.

In an attempt to bring a successful conclusion to the war, the Greeks resorted to subterfuge rather than direct confrontation. They built a large, hollow sculpture in the shape of a wooden horse large enough to hide a small force. The Greeks loaded their main force onto ships and sailed out of sight to give credibility to the feint, leaving one man behind to tell the Trojans that the Greeks had fled, leaving the magnificent wooden horse for the Trojans. Upon finding the

Greeks gone, the Trojans readily accepted the story and sculpture as a war trophy, dragging it inside the walls that the Greeks were previously unable to penetrate.

MI Involvement: The Greeks ran at least two main intelligence operations at the conclusion of the war. The first was infiltrating Troy to capture the Palladium. The Palladium was a statue of Athena, patron Goddess of Troy. Capturing the Palladium created a morale swing for the Greeks – emboldening them for further war and lowering the Trojan morale. The oracles indicated that capture of the Palladium was necessary for Greek victory. The second action was disseminating disinformation to the Trojans by creating a "defector." Sinon [23], a Greek, was allowed to stay with the Trojan Horse and tell his "story." Sinon gained credibility because he was supposedly left behind by the Greeks and had every reason to tell the Trojans the truth. Instead, he bolstered Trojan biases and encouraged the Trojans to drag the Horse inside the city.

Result: After the Trojan "victory" celebration the Greek force exited the horse, surprised and killed the guards, and opened the city doors to the main Greek force that had sailed back to Troy and landed out of sight. Troy was sacked, many of the citizens slaughtered, and the remaining citizens were divided among the victorious Greek force. Some Trojans escaped, but Troy never returned to its former glory.

Lessons Learned:

1. *Social Engineering works.* Social Engineering attempts to elicit an action from a person, or group, that they would not normally allow to take place. The brazenness of the action leads to it being accepted at face value as truth. Social Engineering also depends on the desire of people to believe each other.
2. *Always use common sense and be suspicious***.** Check everything that is out of the ordinary. Ask the question, why? Often a simple check or verification is sufficient to detect and defeat a Social Engineering attack.
3. *Thoroughly check everything.* A simple check would have revealed that the sculpture was hollow, resulting in the discovery of the attack force. Outnumbered, the small attack force would have been easily defeated and Troy would not have been sacked.

Applying the Lessons to the Utility: Social engineering is one of the most effective cyber attacks. Often no technical knowledge is required to accomplish a successful penetration of defenses or to gather intelligence. However, social engineering can usually be defeated with simple, common sense measures practiced by all employees.

1. Foster the feeling that security is everyone's responsibility. Many social engineering attacks are aimed at low-level employees. A plan of education and the support of upper management is invaluable in implementing simple, effective security measures. Training should focus on detection of unauthorized personnel, protection of information, and recognition of vulnerabilities.
2. Appoint a member of upper management to coordinate security. The active support of upper management establishes the priority of security. The higher to designated Security Officer is in management, the stronger the support will be from employees. The management member may designate functions to others, but must take an active role in promoting security.
3. Decide what information is critical and should be protected. Include information from which critical information can be derived or constructed. For instance, user IDs and how the ID is created, are not thought to be critical. But, combined with a password, the user ID greatly facilitates hacking. List identified data and train employees to protect data on that list.

4. Train personnel about security and how to defeat social engineering. Hire security consultants to use social engineering penetration techniques to test security. Use lessons learned to improve training and defenses.
5. Make it easy to check information. Provide mechanisms that allow any employee to report suspicious activities and receive instructions on how to deal with the situation. Pay attention to the reports, treat them as possible early warnings of an attack. Log and monitor reports as part of detecting a pattern of intrusions and/or attacks.

5.0 Conclusions

Security is one facet of reliability. Both a preventative and reactive action, security focuses on human intentionally induced threats. Utility security is related to the intelligence function of MI, preventing attacks on critical assets and reacting to attacks. Many attacks are thwarted using the concept of defense in depth.

Defense in depth describes a methodology of protecting critical assets for an operational mission from enemy attack. The asset is protected by multiple layers of defenses meant to wear down an attack until it is defeated. The defender designs the defenses by analyzing the attacker and his abilities then selects the most efficient mix of responses. Using IDDT methodology allows a defender to consider the various modes of attack and prepare responses.

Several of the examples above showed how past military organizations have used defense in depth effectively in major conflicts. Others showed how past military organizations failed to utilize defense in depth concepts. Based on examples gleaned from the history of MI, lessons applicable to utility asset security have been cited. The specific suggestions are contingent upon the support of upper management. As with most "intelligence failures," the indicators of an impending attack, and its direction, are normally observed well ahead of the actual attack [21]. Indeed, warnings are issued by the security team but are often ignored because of the biases of the managers. The frequency of the warnings are often interpreted by commanders as the intelligence community "crying wolf" rather than seen as a strong consensus from intelligence personnel. Biases range from a belief that an attack is technically "impossible," that the enemy is not capable of making, to thinking the enemy is not motivated to make such an attack. Major disasters often follow.

Intelligence and security personnel may be perceived as "alarmists" or manufacturing threats to justify their existence. Outright dismissal of security personnel opinions can be risky. Security personnel are highly trained and skilled. Because the focus of most organizations is not security there can be a tendency to view intelligence and security personnel as junior to other advisors or as substandard because the skill sets do not directly produce revenue. Senior management must create a culture in which security expertise is valued and regularly consulted if utility attacks are to be avoided.

Attacks evolve and change with available resources. Protecting against traditional attacks is prudent, but thinking outside the box will also prevent novel attacks. New security vulnerabilities are identified regularly, making it important to anticipate an attacker's intentions. Most attacks, however, are not technologically complicated [24]. A hacker will use the most efficient, least cost-intensive attack to accomplish his goals. The simplest—and most effective—attacks target physical intrusion and social engineering. By implementing simple, low-cost measures, many attacks can be prevented. Training personnel to be aware and take common sense measures to protect information and access have a similar effect. The layers of protection should include:

1. Physical protection of an asset. Keep unauthorized people from getting access to sensitive equipment. Once an attacker has access a successful attack is only a matter of time.
2. Train personnel to protect information and be aware of intrusion.
3. Protect information flow into, and out of, an asset. This means protecting the access points and media. Encryption and signal security become extremely important.
4. Protect the asset from "inside jobs." Once unauthorized personnel are denied access, look to an insider that may be corrupted or have a reason to cause damage.
5. Monitor and log everything. Forensic evidence allows security to check for subtle attacks in progress or to reconstruct an attack.
6. Set up a program to continually research new attacks and develop defenses. Train security personnel in new techniques. Then apply IDDT analysis to search for new system vulnerabilities.

Works Cited

[1] No new coal - the calling card of the 'green Banksy' who breached fortress Kingsnorth. 11 Dec., 2008 The Guardian. "No new coal - the calling card of the 'green Banksy' who breached fortress Kingsnorth" 20 Feb. 2009 http://www.guardian.co.uk/environment/2008/dec/11/kingsnorth-green-banksy-saboteur

[2] CNSS Instruction No. 4009 Committee on National Security Systems "National Information Assurance (IA) Glossary" Jun. 2006 http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf 24 Feb. 2009

[3] Field Manual 2-0, Intelligence. Washington, DC: Department of the Army, 2004

[4] Finnegan, John Patrick. Military Intelligence. Washington, DC: U.S. Government Printing Office, 1997

[5] Bauer, Craig and Burkholder, Joel. "Reading Stimson's Mail." Cryptologia 31.2 (2007):179 – 184

[6] Kerkhoffs, Auguste. "La Cryptographie Militaire." Journal des sciences militaries, IX (1883):5 – 83, 161 – 191

[7] Security Configuration Guides. National Security Agency. "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments" 2 Jan., 2009 http://www.nsa.gov/snac/support/defenseindepth.pdf.

[8] Field Manual 3-06, Urban Operations. Washington, DC: Department of the Army, 2006.

[9] Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition. New York:John Wiley and Sons, 1996

[10] Hordeski, Michael Frank, Emergency and Backup Power Sources: Preparing for Blackouts and Brownouts. Lilburn:The Fairmont Press, 2005

[11] National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. New York:W. W. Norton, 2004

[12] DHS|National Infrastructure Protection Plan. Department of Homeland Security. "National Infrastructure Protection Plan" 2 Jan. 2009 http://www/dhs.gov/xprevprot/programs/editorial_0827.shtm

[13] Cano, Craig and Larson, Kathy. "FERC Proposes New Cybersecurity Authority as House Panel Pummels NERC on the Issue." Electric Utility Week 26 May 2008: 2

[14] FERC: Electric Reliability: CIP Reliability Standards. Federal Energy Regulatory Commission. "CIP Reliability Standards" 2 Jan., 2009 http://www.ferc.gov/industries/electric/indus-act/reliability/cip.asp

[15] "Winning a Cyber War" The Wall Street Journal 21 Feb. 2009 Weekend Edition: A11.

[16] Kaufman, J. E, Kaufman, H. W, and Idzikowski, Tomasz, Fortress France: The Maginot Line and French Defenses in World War II. Mechanicsburg:Stackpole Books, 2006

[17] Prange, Gordon W. At Dawn We Slept: The Untold Story of Pearl Harbor. New York:Penguin Books 1981

[18] Horn, Steven. The Second Attack on Pearl Harbor, Operation K and Other Attempts to Bomb the United States in World War II. Annapolis:Naval Institute Press, 2005

[19] Donovan, Peter, "The Flaw in the JN25 Series of Ciphers." Cryptologia 28.4 (2004):325 – 340

[20] Wells, Richard B., Applied Coding and Information Theory for Engineers. Upper Saddle River:Prentice-Hall 1998

[21] The Uncertain Oracle, Some Intelligence Failures Revisited. 25 Dec. 2008 http://huachuca-www.army.mil/HISTORY/SiteMapReferences/uncertain.html
[22] Coolidge, Olivia, The Trojan War. New York:Houghton Mifflin, 1980
[23] Strauss, Barry, The Trojan War: A New History. New York:Simon and Shuster, 2006
[24] Long, John. No Tech Hacking, Burlington: Syngress Publishing Co., 2008