LEVERAGING TRADITIONAL BATTLE DAMAGE ASSESSMENT PROCEDURES TO MEASURE EFFECTS FROM A COMPUTER NETWORK ATTACK

GRADUATE RESEARCH PROJECT

Richard A. Martino, Major, USAF

AFIT/ICW/ENG/11-08

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ICW/ENG/11-08

Leveraging Traditional Battle Damage Assessment Procedures to Measure Effects From A Computer Network Attack

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Richard A. Martino

Major, USAF

June 2011

AFIT/ICW/ENG/11-08

Leveraging Traditional Battle Damage Assessment Procedures to Measure Effects From A Computer Network Attack

Richard A. Martino
Major, USAF

Approved:

Robert F. Mills, PhD (Chairman)	date
David J. Robinson, Lt Col, PhD (Member)	date
Jonathan W. Butts, Capt, PhD (Member)	date

Abstract

The art of warfare in cyberspace is evolving. Cyberspace, as the newest warfighting domain, requires the tools to synchronize effects from the cyber domain with those of the traditional land, maritime, space, and air domains. Cyberspace can compliment a commander's theater strategy supporting strategic, operational, and tactical objectives. To be effective, or provide an effect, commanders must have a mechanism that allows them to understand if a desired cyber effect was successful which requires a comprehensive cyber battle damage assessment capability.

The purpose of this research is to analyze how traditional kinetic battle damage assessment is conducted and apply those concepts in cyberspace. This requires in-depth nodal analysis of the cyberspace target as well as what second and third order effects can be measured to determine if the cyber-attack was successful. This is necessary to measure the impact of the cyber-attack which can be used to increase or decrease the risk level to personnel operating in traditional domains.

AFIT/ICW/ENG/11-08

To My Wife

Acknowledgements

I would like to thank my incredible family for their constant love and support. I am especially grateful to my beautiful wife who has supported me through every deployment, TDY, extended workday, and move to a new assignment for the past 26 years. Without you none of this would have been possible, or worth it.

This work would not have been possible without the patience and guidance from my committee. I am especially grateful to Dr. Bob Mills for not only helping to scope this research to a manageable task, but particularly working my application to accept me into the AFIT Cyber Warfare program. I am also in debt to Lt Col (Dr.) Robinson and Capt (Dr.) Butts for the mid course and final corrections that helped me fully understand the art of cyber warfare. Thank you for giving me an appreciation for that which you have devoted your careers to.

Without a doubt I would still be on page one of this research if it hadn't been for the intelligence professionals at U.S. Cyber Command and the National Air and Space Intelligence Center. While your efforts in this unclassified research remain anonymous what you have taught me about cyber warfare and intelligence was instrumental in the final product. I truly appreciate you taking the time to edit and comment on my research despite your busy schedules.

There were a few others that took the time to help push this rock a little further; LT Dane Johnson from Joint Forces Command's Joint Targeting School, Maj Bo Birdwell from Air Mobility Command's Air Intelligence Squadron, and Mr. Juan Lopez from the Center for Cyberspace Research. Your thoughts and advise early in the development of this research helped guide my ideas.

Finally, it has been an incredible honor to share this journey with my classmates; eleven of the Air Force's finest. It was your mutual support and camaraderie this past year that helped me endure the seemingly endless papers, labs, and exams.

Richard A. Martino

Table of Contents

Page

List of Figures

List of Tables

Leveraging Traditional Battle Damage Assessment Procedures to Measure Effects From A Computer Network Attack

I. Introduction

> "The success or failure of this one F-117 mission, this one bomb, would tell a lot about how our air campaign would fare. If Iraqi telecommunication were destroyed, the air superiority battle became manageable: blind the enemy air defense system, and isolate the elements from the brain, and it is no longer a "system" but individual weapons operating in the dark. ..CNN just went off the air. That was it. The "AT&T" building had taken a mortal blow." [6] – General Chuck Horner

During the start of Operation DESERT STORM, U.S. Air Force F-117's loaded with GBU-27s struck key nodes in and around Baghdad, Iraq to isolate Iraqi commanders from their units in the field. Although the start of the Gulf War would be Special Operations forces taking out Iraqi border positions, the world witnessed the start of the Gulf War as a kinetic strike against key Iraqi targets around Baghdad as a live CNN feed showed Iraqi anti-aircraft artillery firing into the dark night. The success of these first strikes into the heart of Baghdad were easy, as General Chuck Horner recalled how their CNN feed in the air operations center went to static – no battle damage assessment of that target would be required.

The wave of F-117s braved what was thought to be a formidable Iraqi integrated air defense system (IADS). The strikes on day one of the war met tactical objectives (destroyed the Iraqi telecommunications center), operational objectives (degraded the Iraqi IADS), and strategic objectives (isolated Iraq from the world and demonstrated Coalition domination early to gain an advantage in world opinion). Battle damage assessment (BDA) was critical for these first strikes.

Today, the United States and other countries are faced with the possibilities of how to use computer network attack (CNA) to achieve strategic, operational and tac-

tical effects. To grow a capability that accepts a "first" strike cyber-attack capable of targeting the same targets as F-117s delivering GBU-27s did at the onset of DESERT STORM, the United States will require more than just a live CNN feed to conduct battle damage assessment.

The probability exists that future military conflicts will continue to involve some sort of preemptive cyberspace effect that could target telecommunications, space-based sensors and relays, automated aids to financial and banking networks, power production and distribution, and media to share public perceptions. [29] The Israeli strike against Syria in 2007 with an integrated cyber component, coupled with the cyber-attack of Estonia[1] (May 4 – 8 2007) and the invasion of Georgia by Russia (August 7, 2008), demonstrate a willingness and capability to leverage cyber-attacks against nations. [7] [37] [29]

1.1 Background

BDA is both an art and a science. The art of BDA is applied through years, if not a lifetime, of applying judgments of the success, failure and/or percentage of either success or failure to provide an assessment through the observation of one or more indicators. The science of BDA is based on the known quantities of the target and capabilities of the weapon used against the target to render the target destroyed or unusable. Analysts apply both the art and science of BDA to provide an assessment that drives other decisions; some more obvious than others. If the target is not "adequately" destroyed, then the commander can require a re-strike. Less obvious is the impact to the battle by destroying the target. Is the SA-10 destroyed and no longer a threat to aircrew flying in the vicinity of where it was once positioned?

How BDA is conducted requires a host of technical and non-technical means. The quickest means to receive BDA is from a Joint Terminal Attack Controller (JTAC) on the ground that witnessed the GBU-12 strike the target. Alternatively, there may

[1] "While the common belief is that the Russians did it [conducted the attack], no one has ever been able to perform any digital forensics linking the attacks to the Russian government." [29]

be an MQ-9 Reaper over the target area with an electro-optical/infrared (EO/IR) camera watching the AGM-114 Hellfire missile impact the cave complex with secondary explosions (and with a live feed to the Air and Space Operations Centers (AOC)). There could also be other airborne and space based sensors that receive indications of the attack that must be carefully analyzed before BDA can be properly assessed.

Kinetic BDA has a long history that has allowed its methodology to evolve as technology has evolved. But how can attacks in cyberspace be analyzed if the attack does nothing more than shut-down power to an enemy's command post? Do the lights going out in the area indicate that the cyber-attack was successful, or did an operator recognize a fault in the power system that caused them to shut down the power to the command post before permanent damage could take place? An inherent problem with the cyberspace domain is that the very existence resides in a space that is neither visible to JTACS on the ground, visible to EO/IO sensors, nor visible to other airborne or space based sensors. The problem is not much different from the BDA problem in the traditional domain such as targeting underground facilities.

1.2 Motivation

A methodology for Cyber BDA is required that is rooted in science yet exploits the art of seasoned analysts that a commander can rely on with the same certainty that traditional kinetic BDA uses. As cyber operations synchronize with traditional domains (air, land, maritime and space), commanders will require a means to gauge the effectiveness of offensive cyber operations. The promise of an effect requires evidence of success or some degree of proof that the effect yields the required results. In the original example, if a pilot is notified that the SA-10 is confirmed destroyed, the level of risk to the pilot is decreased and improves the freedom of action of the pilot. If, however, the SA-10 is not destroyed, the risk to the pilot increases as their freedom of action in vicinity of the SA-10s missile engagement zone is reduced.

As cyberspace operations integrate with other domains their impact to risk in the battlespace can have a more profound effect to aircrew flying in enemy territory. On September 6, 2007, Israeli fighters slipped through a robust Syrian IADS undetected to strike a suspected weapons of mass destruction facility. Three possibilities surround how Israel was able to fly through Syrian airspace undetected by the IADS: [7]

– Input of false data into the IADS radar by an unmanned aerial vehicle.

– A "trapdoor" embedded in the IADS air defense algorithm.

– Splicing a fiber optic cable to gain access to the air defense system.

Regardless of the method used it is clear that the use of cyber operations was successful to reduce the risk to an offensive counter-air package.

1.3 Purpose

The purpose of this research is to demonstrate how the physical components of a system attacked through cyberspace can utilize the current methodology of kinetic BDA to provide commanders with the necessary feedback to judge the success or failure the attack. This research will look at the current Joint doctrine for BDA and propose solutions for bridging cyberspace with traditional intelligence, surveillance, and reconnaissance (ISR) in a non-traditional environment. The proposed techniques could be used by planners to conduct nodal analysis of the target of offensive cyber operations identifying both direct and indirect sub-systems that can be used for BDA.

The intended audience of this research consists of operational planners that are integrating cyber operations into traditional domains as well as intelligence professionals tasked with conducting nodal analysis of a cyber target for the purpose of exploiting targets that can leverage cyber or kinetic effects, as well as building an ISR collection plan to measure the effects of a cyber attack.

1.4 Scope

This research will focus on determining if there are effects that can be measured in the traditional physical domains as a result of a cyber-attack. To demonstrate this, supervisory control and data acquisition (SCADA) systems will be used as a vignette "target" system to demonstrate how nodal analysis outside of the targeted system can be used to provide a degree of certainty of a successful cyber-attack. While techniques currently exist within cyberspace through the use of computer network exploitation, little research has been conducted to demonstrate if it is faster to measure the physical effects that result from a cyber-attack. The methodology researched readily extends to any cyber-attack scenario.

1.5 Organization

Chapter II of this research examines the current battle damage assessment methodology as defined in Joint Publication 2-0, Joint Intelligence, JP 3-60, Joint Targeting, and JP 5-0, Joint Operations Planning. The intent is to highlight what current processes are in place to conduct battle damage assessment. This includes a brief background of BDA and the inherent problems associated with receiving timely and accurate BDA. Next, Chapter II provides a background of situational awareness (SA) and the impact of the different levels of SA as defined by Dr. Micah Endsley. Cyber intelligence, surveillance, and reconnaissance (ISR) are explored with a focus on what current work has been, or is being undertaken to define how cyber ISR are achieved. Although cyberspace is unique in some way from the traditional domains (air, land, sea, and space), Chapter II highlights how electronic warfare is in some ways similar in terms of providing BDA assessments. Finally, as a vignette for future chapters, supervisory control and data acquisition (SCADA) systems are defined.

The purpose of Chapter III is to outline and describe why cyber BDA needs to be researched and steps that can be used to conduct a nodal analysis of a cyber physical system, specifically SCADA systems as an example. The goal of Chapter III is to demonstrate that with careful analysis of the targeted system in cyberspace,

interdependencies can be identified that will help bridge the effects that happen as a result of a computer network attack (CNA) to those physical effects that can be measured outside of cyberspace. This is particularly important as limited ISR resources are tasked to look at areas with the greatest chance of detection to measure the effects of a CNA. Finally, the chapter concludes with a brief introduction to how providing commanders with the results of a successful cyber-attack can impact the risk in the battlespace.

Chapter IV concludes with the research results, recommended future research areas, and the application of the research to the warfighter. This chapter highlights that deliberate nodal analysis of a cyber target with an emphasis on identifying critical nodes outside of cyberspace can result in measurable results that can assist in cyber BDA. This is important in understanding that as cyberspace operations become more synchronized with the traditional domains, effective utilization of limited ISR resources can directly impact warfighters and the ability of commanders to wage war.

II. Considerations for Cyber Battle Damage Assessment

> "The less physical the attack, the less the certainty that there is that it did harm." [26] – Dr. Martin Libicki

2.1 Background of Battle Damage Assessment

There was a time in history that commanders could observe BDA for themselves, watching from either the front line, or within visual range as their forces maneuvered and engaged the enemy. Because battles were confined in space and time, the advantage to the commander to make their own assessment was based on the ability to observe all developments of the battle. [16]

BDA has always suffered from limited reports and observations of the primary and secondary effects of munitions. During World War II photo reconnaissance was restricted to "reporting only what could be seen by another interpreter" through a physical damage assessment. [22] Despite advances in technology, the Vietnam War continued to be plagued by BDA problems. Colonel Burton S. Barrett, Seventh Air Force Director of Targets and Deputy Chief of Staff for Intelligence noted in his Project CORONA HARVEST[1] end-of-tour report that"all intelligence sources, analytical formulas and analysis judgments have been applied to the BDA problem, but it still remains an enigma." [22]

Modern weapons have increased the ability to hit targets from greater range and with more accuracy. Additionally, the age of high technology systems that provide real time, to near-real time updates of the battlespace has increased the demand for faster, more accurate BDA. During Operation DESERT STORM it was noted that the use of precision weapons reduced the size of a weapon's impact area into a building, but masked the effects of the weapons inside the building where the target was located, reducing the ability for analysts to determine the success or failure of the mission. [9]

[1]Project CORONA HARVEST was an effort by Air University at Maxwell AFB, AL to study and develop lessons learned from the Vietnam War while the war was in progress.

The tempo of a fast-moving fight, coupled with limited intelligence, surveillance and reconnaissance (ISR) capabilities with conflicting/competing priorities further complicates collecting raw data that can be used for BDA. As recent as Operation IRAQI FREEDOM, Diehl and Sloan stated that BDA was "overrun by the rapid operations tempo and endured much of the same criticism it received in the previous decade" which was reported during Operation DESERT STORM as "*slow and inadequate*". [16] Furthermore, in some situations, the political desire to minimize physical damage has complicated efforts to perform effective BDA, forcing commanders to take either additional risks, such as assuming that the target is down based on initial BDA, or assuming that the target is still operational and retarget or restrict operations that required that target to be destroyed. [2]

Joint Publication 2-0, *Joint Intelligence*, states that "the JFC should provide a comprehensive plan, together with an intelligence architecture, to support BDA. This plan must synchronize ISR resources and reporting to effectively/efficiently support timely BDA." [11]

BDA is in high demand. From the initial weapons release from a fighter or bomber aircraft, or the launching of Tomahawk Land Attack Missile (TLAM) or High Mobility Artillery Rocket System (HIMARS) against a target through the collection of imagery, signals intelligence (SIGINT), human intelligence (HUMINT), and other all-source capabilities, commanders are driven by an information technology age that has the capability to collect data at a rapid rate. However, although there is an abundance of ISR assets available to commanders, BDA is still confined and tempered by the availability of "wet ware" or analyst's brain power to make judgments based on individual expertise, intelligence preparation of the operations environment (IPOE), and post-strike effects by direct and indirect means. [2]

The drive for more sensors (data) is best stated by Lt Gen David A. Deptula, former Air Force Deputy Chief of Staff for ISR who stated "We're going to find ourselves in the not too distant future swimming in sensors and drowning in data." [28]

Having an unblinking eye in cyberspace results in an increase in data for analysts but does not equate to greater situational awareness. Rogers et al. stated that "our cyber sensors have also been dramatically improved, increasing the volume of continuous data by orders of magnitude, when we really have not figured out how to handle all the data we produced before persistent sensing." [35] The problem of large amounts of data is essential to identifying the best source of where to focus limited ISR resources (analysts and sensors).

The need for BDA in cyberspace is no different, yet there are two extremes on how cyberspace BDA can be viewed. On one extreme, the traditional operators may have little understanding on how CNA is conducted let alone understand little of the physical components of the domain and how information is stored, transmitted, and processed.

On the other extreme is the belief that the capability to conduct BDA in cyberspace is limited. Libicki stated that "battle damage assessment on C2 [Command and Control] warfare is so difficult (consisting of both what was hit and what difference the hit made) that field commanders understandably want to see visible craters to ensure they had any effect at all." [25] BDA is futher complicated if you eliminate a crater from a kinetic strike and target a cyber physical system "somewhere" that controls processes miles from the target that still will not produce a crater.

The attacker's insight of the target system is based on what is observed operating through computer network exploitation (CNE) and other all-source reporting. Once an attack commences, fail safe devices may not result in a manner predicted by the attackers (Table 1). [27] Since recovering from a cyber-attack has not been observed, there is no timeline on how long system administrators will take to recover from a cyber-attack, and as Dr. Martin Libicki stated in a presentation to Johns Hopkins University's Applied Physics Laboratory, "cyber-war will be a series of surprises." It can be the series of surprises that impacts the ability to conduct accurate BDA. [27]

Table 1: Dr. Libicki briefing,"Predicting Battle Damage is Also Hard" [27]

Far in Advance	**Systems change with every software update**
In the near term	What can be observed about systems may say little about how they respond to attack: (1) May have crisis reserve modes (2) May have processes that kick in only when systems threaten to go awry
All the time	Damage roughly proportional to downtime or persistence of corruption, but even system administrators don't know how fast they can reverse effects

2.2 Current BDA Methodology

The roots of BDA rests in the Joint Targeting Cycle where targets are nominated based on the commander's intent. Joint Publication (JP) 3-60, *Joint Targeting*, defines a target as an entity or object considered for possible engagement or action, and describes the target itself as an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior. [12] A cyber target can have an effect in one of these target descriptions either directly or indirectly, and therefore JP 3-60 provides a solid framework for developing cyber BDA techniques.

2.2.1 Target Characteristics. For the purposes of targeting and target analysis, planners must understand the target's intrinsic or acquired characteristics. JP 3-60 categorizes these as physical, functional, cognitive, and environmental which are the basis for target detection, location, identification, and classification for surveillance, analysis, strike, and assessment. [12]

Traditionally, the *physical* characteristics of a target are more appealing to a commander. Imagery of a target provides a "before and after" comparison to gauge the effect of a strike. Explosions at the target area can be observed at the time-over-target (TOT) indicating that the designated weapons platform delivered their munitions to the target, but does not indicate if the munition hit the correct target. Likewise, a radars electronic signature can be detected by multiple sources

that provide an indication that the attack was not successful if electronic emissions are still detected after the designated TOT.

Knowledge of the *functional* characteristics of the target are more complicated than determining the physical characteristics of a target. Understanding what the target does within the system requires complete understanding of all of the components of a system and how the system operates.

The *cognitive* characteristics of a target describe how information is processed within the target, the decision cycle of the target, and how the target stores information. The sociology aspect of understanding the target is more difficult to apply towards target analysis and is better confined to the study of influence operations, which may be able to contribute towards BDA data.

The *environment* can not only affect the target, but can also affect the ability to conduct BDA. Also loosely included in this characteristic is the target's reliance on resources such as energy, water, and command and control.

The impact of time-sensitivity, regardless of the target's physical characteristics, affects the relative priority of the target. Although this research does not look at the targeting process, time sensitivity is important in understanding the limited opportunity to target a system through cyberspace and conduct BDA against that target.

2.2.2 Application of Measures of Effectiveness to Targets. Targets are (or should be) linked to the commander's end-state and goals. Measuring the success of attacking those targets is essential to provide feedback so commanders at all levels can understand the effectiveness of their targeting. *Measures of effectiveness* (MOE) are "tools used to measure results achieved in the overall mission and execution of assigned tasks." [12] MOEs also link the target to the actual requirement for intelligence collection. Without MOEs, intelligence could be collected, but the data collected could remain unreported to analysts resulting in failing to correctly report BDA.

The desired effects are key to understanding the target. When planners select targets they take into consideration the direct and indirect effects of hitting the target. Direct effects are immediate and easily recognized. Attacking a bridge with the purpose to collapse the bridge so that it is not usable by enemy forces can be immediately viewed through a fighter aircraft's targeting pod, visual observation, or through the EO/IR camera on a Remotely Piloted Aircraft (RPA).

Indirect effects are normally referred to as delayed or displaced effects (second, third, or higher-order consequences of action) created through intermediate effects or mechanisms. Indirect effects are usually more difficult to recognize. For example, if targeting an oil pipeline, shutting off the flow of oil to an airbase may result in more tanker trucks arriving at the base, indicating that the pipeline was successfully shutoff.

2.2.3 The Joint Targeting Cycle. The Joint Targeting Cycle provides the framework needed to successful conduct joint targeting (Figure 1). The Joint Targeting Cycle consists of six phases: (i) End-State and Commander's Objectives, (ii) Target Development and Prioritization, (iii) Capabilities Analysis, (iv) Commander's Decision and Force Assignment, (v) Mission Planning and Force Execution, and (vi)Assessment. [12] This research focus specifically on steps (ii) and (vi).

During target development, target system analysis (TSA) is conducted to identify critical components or nodes of a target system. [12] From the traditional kinetic view, TSA provides a view from the macro level to the micro level based on all-source, fused data that allows planners to focus on both the physical and functional components of the target and the relationship to other targets within an operational system. TSA is therefore important in not just target selection, but also understanding what direct and indirect effects can be measured after a strike.

The assessment phase provides analysis of the target through the collection of information from multiple sources. Analysis is the fusion of multiple sources of information to provide an estimate as to the effect of the strike which results in an

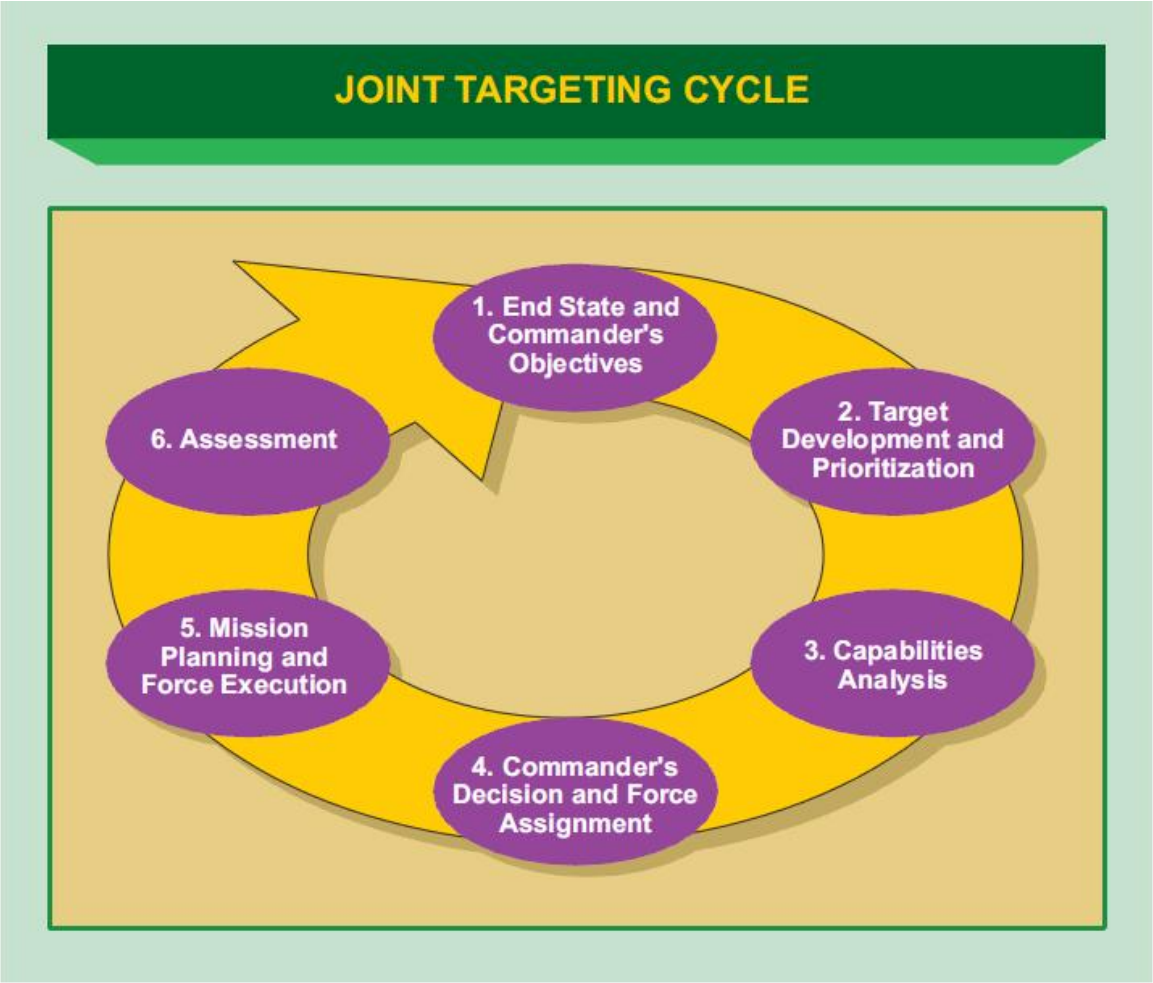

Figure 1: Joint Targeting Cycle [12]

estimate as to the success of the strike and the achievement of the commander's goals. It is the analysis that takes the raw intelligence data and transforms the data into meaning that can be used to assess the strike.

Operational and strategic level assessment provides the Joint Force Commander (JFC) the ability to adjust planning and current operations through the use of MOEs. Since targeting can impact any level of warfare, the JFC requires the ability to conduct BDA at these levels. Some targets could have an immediate impact to the operational and strategic levels of war.

Operational and strategic assessment focuses more on the broader goals and progress towards the commander's end-state while tactical assessment is more concerned with individual tasks that contribute to the campaign. Individual tactical objectives contribute to operation level goals which in turn contribute to the overall strategic goal(s).

Combat assessment provides results of an engagement against a target with three elements: BDA, munitions effectiveness, and re-attack recommendations and future targeting. BDA can be conducted through geospatial intelligence (GEOINT), in-flight reports and mission reports, aircraft video and weapons system video, signal intelligence (SIGINT), human intelligence (HUMINT), open source intelligence, end of mission reports for surface-to-surface fires, and indigo reports for cruise missiles. [12]

The complexity of relying on multiple sources is based not just on capabilities of each system, but collection time and methods to conduct analysis, classification levels of collection, and reporting requirements. As outlined in Table 2, traditional BDA is conducted in three phases; Phase 1 BDA (Physical Damage), Phase 2 BDA (Functional Damage), and Phase 3 BDA (Target System Damage). This, combined with 18 basic target categories provides a framework for conducting BDA.

Within the realm of conducting BDA, each Phase of the BDA process provides an estimate of success. The estimates are assigned according to the following guidelines:

– Phase 1, confidence levels are applied as;

- Greater than 95% - Virtually certain

- Greater than 50% - Likelihood, little inference

- Less than 50% - Likelihood, considerable inference

– Phase 2 Functional Damage Assessment

- Destroyed

- Greater than 45% - Severe

- 15 – 45% - Moderate

- Less than 15% - Light

- No Functional Damage

- Unknown Functional Damage

- Abandoned

– Phase 3 Target System Assessment

- Completed assessment of the target system based on all source reporting

The traditional BDA methodology provides a solid foundation to help address the cyberspace BDA requirements and the impact it can have in the battlespace. However, unlike a traditional kinetic strike where the effect of the strike is directly on the location where the desired effect is required, a cyberspace attack's physical location may only provide nothing more than a medium to continue the attack through other means far removed from the actual target location.

2.3 The Impact of Situational Awareness and Cyber Battle Damage Assessment

Research has been conducted on the impact of situational awareness (SA) and the cognitive process of humans interacting in their environment. SA is an important

Table 2: Battle Damage Assessment Quick Guide, DI-2820-03 [12]

Assessment Type	**Physical Damage or Change Assessment**	**Functional Damage or Change Assessment**	**Target System Change Assessment**
Initial Assessment	Initial physical damage or change assessment of aimpoint(s) and target due to direct and unintended weapon effects.	When possible, an initial functional damage assessment of target element(s) and target is accomplished. When possible, re-attack recommendation is also included.	Not performed
Supplemental Assessment	Detailed physical damage or change assessment of aimpoint(s) and target element due to cumulative weapon effects.	Detailed functional damage assessment of target element(s) and target. When possible, inputs to the Target System Change Assessment, MEA, or re-attack recommendation are also included.	Not performed.
Target System	Not performed	Not performed	Detailed assessment of change to target system(s) due to cumulative attacks on targets.

concept to understand as it relates to cyber BDA because the majority of effects analyzed may result in a physical effect far removed from a target that does not have before and after imagery to compare. Therefore, SA must be considered in all aspects of looking at second and third order effects. A definition of SA that best fits as it relates to BDA is as follows: [17]

> "Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."

In this context SA is not the sum of a person's entire knowledge, but only pertains to the dynamic environment and is separate from decision making and performance. [17] High SA does not guarantee the correct decision, nor does low SA equate or demonstrate to poor performance.

2.3.1 Endsley's Situational Awareness Model. No pure research was found on the impact of cyber-attack on an adversary's decision process, but some work has been accomplished on how disruptions, interruptions, and other forms of information attack can affect situational awareness and decision making. [18] An understanding of this model is essential as commanders could receive data from a CNA the same way that the operator at the receiving end of a computer network attack interprets data to make a decision on what is happening and the impact it has on the target system.

Endsley and Jones state that "the decision-maker must determine whether the cues represent something abnormal, or are part of a known class of typical problems that exist within daily operations." [18] CNA may target a system far removed from the actual location where an effect needs to be achieved. Physical damage assessment and/or direct effects will probably not be discernible using traditional sensors. For example, a command in the form of a computer network packet could travel in milliseconds from the attacker to the target with no direct feedback as to the success or failure of the packet reaching its destination and executing the command in the correct sequence.

Likewise, BDA through cyber means (Computer Network Exploitation) may be denied due to accesses closing via the cyber route the attacker used denying the ability to exploit the system once the attack sequence has started. With no physical evidence at the point of the attack, BDA would be based on a functional understanding of the system. In the cyber domain, environments would have limited impact on the ability of the attacker to understand how the attack proceeded. An understanding of the reliance on external sources such as power could provide indications, but no conclusive results for BDA.

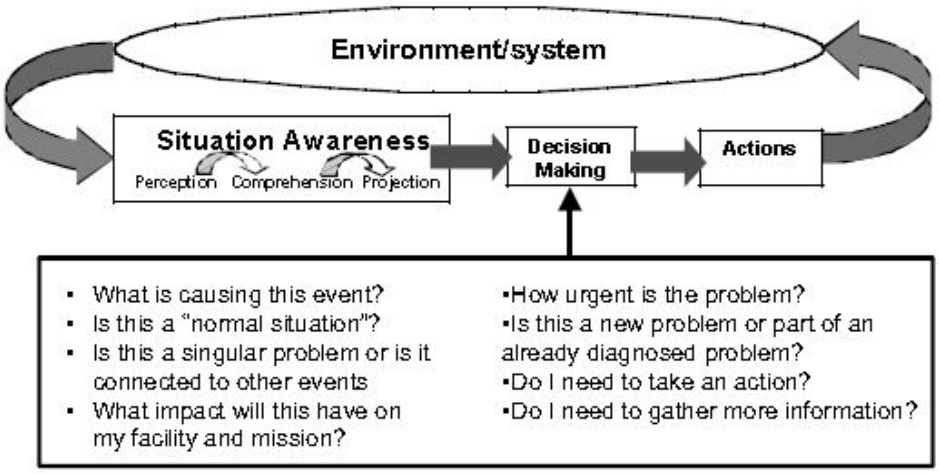

Figure 2: Decision Context for Detection and Diagnosing Information Attacks [18]

From a cognition approach, Figure 2 is useful in understanding what is happening to situational awareness during an information (cyber) attack. Similar to the operator at the receiving end of the attack who builds SA from what is happening, analysts rely on the same cognition of information from what is observed about the system during IPOE and to some degree, measuring second and third order effects. The similarities of a traditional kinetic attack and an CNA is best illustrated in two regards:

1. In a kinetic attack, the physical application of force against a target could be readily detected through defensive systems such early warning radars, sensors,

scouts, or other indications and warnings absent of the use of low observable technology. In cyberspace, intrusion detection systems (IDS) provide a capability to detect an attack based on established rules.

2. The result of a kinetic attack is immediate in the physical destruction of a target. In cyberspace, the attack can take the form of manipulating data that produces no physical destruction or manipulating a system that does result in the physical destruction of the target system or a system removed from the location of the attack. A cyber-attack that results in physical destruction may or may not result in visible physical damage (destroying a generator versus corrupting a hard drive making the hard drive unusable).

To complicate SA in cyberspace, indications of a cyber-attack can be viewed as a normal part of the system and very difficult to detect: [18] (i) The results of a cyberspace attack may result in too much information that can be correctly observed by the operator, information flow that is input too fast into a database, disorganized information content, dissonant information (where information from different sources disagree), and delayed information all impact the cognition of decision makers. (ii) From the perspective of conducting BDA for a cyber-attack, these same problems can face commanders in gauging the success of an attack.

The role of SA in BDA is directly related to applying the Observe, Orient, Decide, Act model proposed by Boyd and enhanced by Endsley (Figure 3) and provides a venue for understanding the cognition of information at all levels of war. [17] However, with cyberspace, the missing component that commanders have relied on for centuries (physical destruction) further complicates the ability to observe, orient and decide, thus having the potential of paralyzing an action.

2.3.2 Elements of Endsley's Situational Awareness Model. Endsley's model focuses on three levels of SA. Level 1 SA, perception of the elements in the environment, describes the perception of the status, attributes, and dynamics of relevant

elements in the environment. From a BDA perspective, this would be the raw data that is viewed by an analyst.

Level 2 SA, comprehension of the current situation, applies the knowledge of level 1 SA and adds the understanding of the significance of those elements as it relates to the goals of the person. For example, an analyst views raw BDA data and recognizes that one of the data points is relevant to potentially identifying the significance of the data towards understanding the impact of the data towards making a decision.

Level 3 SA, projection of future status, identifies the ability to take the knowledge of the status and dynamics of the elements and comprehension of the situation and predict a course of action. This can best be summed up as comprehending the meaning of that information in an integrated form, comparing it with operator goals, and providing the projected future states of the environment that are valuable for decision making. [17] Level 3 results in the final analysis that accompanies BDA, especially BDA that requires high cognition that requires the observer to make assumptions.

Elements are the things that the operator needs to perceive and understand. Elements change depending on the SA level. For example, when describing the elements for air-to-air fighter aircraft: [17]

– Level 1 SA: location, altitude, and heading of ownship and other aircraft; current target; detections; system status; location of ground threats and obstacles.

– Level 2 SA: mission timing and status; impact of system degrades; time and distance available on fuel; tactical status of threat aircraft (offensive/defensive/neutral).

– Level 3 SA: projected aircraft tactics and maneuvers, firing position and timing.

The concept of elements can be applied to BDA with the knowledge that as an analyst observes different elements of raw data and increases their SA, their under-

standing of the data will change and impact their understanding of the BDA as it relates to the target and if that data is directly related to the attack.

Although SA will change over the course of time, SA is affected by both the past and the future. Initial raw data may not be immediately known as relevant to the target, but as more data is received that appears to be related to the target, or the data changes, the analyst could recognize the changes as being related to the target. This not only increases their level of SA level, but also helps analysts apply future data sets to the same target based on patterns. Endsley states that while SA is "highly spatial", functional relationships of system components and aspects of the environment are very important for SA. [17]

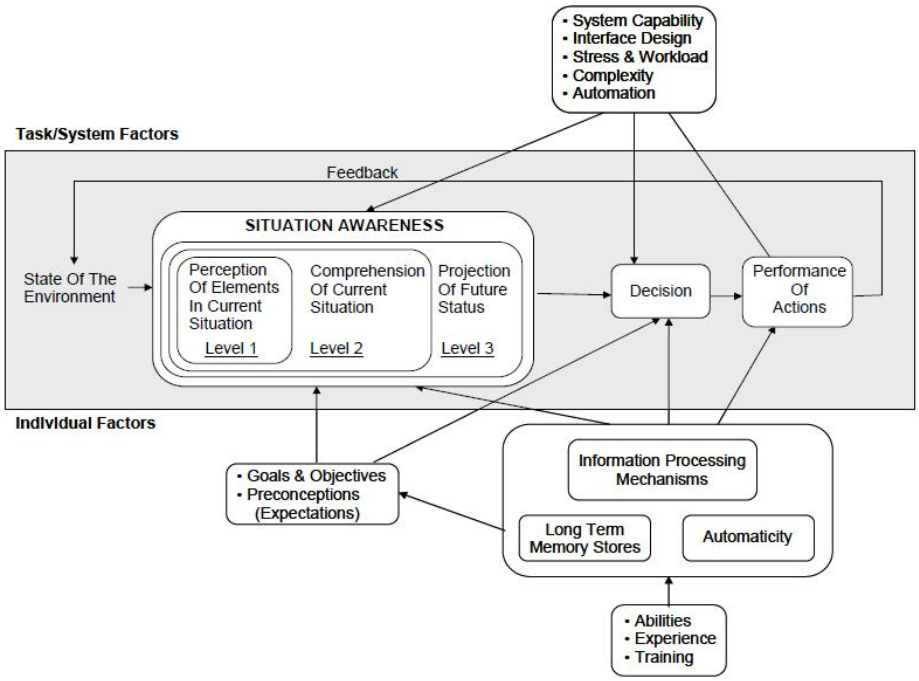

Figure 3: Endsley's Model of Situational Awareness in Dynamic Decision Making [17]

If BDA is designed to provide commanders an assessment of the success or failure of the strike against a target, then situational awareness becomes critical as different layers of personnel interpret data streaming into their consoles. With physical destruction, the ability for information to be quantified is easier than in a cyber-attack

that yields little to no physical indications, instead relying solely on a functional assessment may not necessarily have all of the complete details.

Confidence in the attack is just as paramount as how well a cyber attack tool will work. Although the developers of cyber attack tools have undoubtedly tested their tools through simulations of a known target network, and even through CNE have acquired a level of confidence of their abilities to penetrate the target at a time and place of the commander's choosing, there are still a lot of unknowns. Richard Clarke stated that "What cyber warriors cannot know, however, is whether the nation they are targeting will surprise them with a significantly improved array of defenses in a crisis." [7] The importance of BDA when synchronizing CNA with the traditional domains is therefore important, and if it is planned for, the CNA effect must be counted on and reportable.

2.4 Cyber Intelligence, Surveillance, and Reconnaissance

From a Joint perspective, JP 3-13, *Information Operations*, provides a framework for Information Operations to include computer network operations. Computer network exploitation (CNE) is the equivalent of traditional ISR in the cyber domain. It is defined as the enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. [13] CNE by itself allows IPOE and post-strike intelligence collection in cyberspace. A limitation with CNE, by itself, is that CNE requires continued access into the targeted system and may not account for effects that can be measured outside of the targeted domain.

2.4.1 Major Functions of Cyber Intelligence, Surveillance, and Reconnaissance.

In an attempt to understand the requirements for cyber ISR, Convertino, DeMattei and Knierim identified five major functions of cyber ISR. [8] These major functions include:

1. Identifying potential target systems through all-source intelligence, data specifically collected to access the target, and "social engineering" - the process of obtaining information on systems from people inside the organization.
2. Obtaining access through direct penetration of the adversary network or through installation of trap-doors, backdoors, and multi-role, customizable mobile code called cyber craft.
3. Exfiltrating data about the target-system configuration.
4. Analyzing data and build a network diagram.
5. Creating a model of the adversary's target-system.

These requirements highlight the IPOE phase of intelligence collection. Steps 4 and 5 are useful in understanding that a network diagram is beneficial to understanding the key components of a network by accessing data and creating a model of the system. This accounts for the "before" understanding of the target system (or establishing a baseline) and can be useful in comparing data from a post-strike CNA.

2.4.2 Cyber Effects-Based Assessment. The concept of a cyber effects-based assessment (EBA) best accounts for a drive towards conducting BDA of cyber operations real-time or near real-time. [21] It is suggested that cyber EBA is accomplished by combining multiple sensors and combining multiple means of measuring effects. Cyber EBA is assessed in three ways: (i) effects on systems, (ii) effects on users, (iii) and cyber effects assessment of kinetic operations.

The first-level requirement for cyber EBA is effects on systems. Effects on systems determines the effects of a cyber operation on a target-system such as computers, network infrastructure, intelligent weapons systems, and critical infrastructure. Achieving an understanding on the effects on systems can yield information on potential cyber targets which, coupled with the correct MOEs, could assess "higher-order" effects of cyber operations.

In addition to determining effects on systems, effects on users constitute the second application of cyber EBA. This area focuses on assessing the impact of cyber operations on the behavior of the users. Information on the humans, organization, cultural, and societal structures and behavior are all elements of this application.

Finally, the cyber effects assessment of kinetic operations leverages cyber means to measure the effects of cyber operations. Having this capability would enable an understanding of changes in network operations using pre-attack analysis as a baseline and measuring changes after a kinetic strike. Included in this area is the use of both traditional ISR and cyber ISR.

Initial research indicates that cyber EBA is based on a distributed cyber sensor network that can provide SA on changes to network status, system performance, and adversary behavior. Cyber effects assessment of kinetic operations includes the fusion of both cyber and traditional ISR capabilities. Cyber EBA can provide relevant BDA information to commanders. However, cyber BDA should also focus outside of the cyber domain to be effective in providing commanders with relevant feedback on the effect of a CNA against at cyber-target.

2.5 Electronic Warfare and the Relevance to Understanding Cyber Battle Damage Assessment

Cyber BDA is still a great unknown outside of the CNE process. A peer effect that could be used to help understand cyber BDA is best illustrated by electronic warfare (EW). EW suffers from the same inherent problems of CNA, namely the lack of visible physical destruction. The actual application of electronic attack (EA) depends on the effect that the attacker is trying to produce. For example, jamming an early warning radar serves two purposes:

– Disguise / mask the true air picture.

– Force the operator interpreting the data to not trust the information that is being displayed resulting in delayed or inaccurate reporting that may not be trusted.

EW relies on the attacker using simulated evidence such as modeling or simulation based on the known physics of the target radar and the attacker's system to provide proof of capability. [26] It also relies on more indirect evidence of the effectiveness in terms of real time analysis by pilots over the battlespace (e.g., fewer spikes[2] from target tracking radars), as well as fewer emissions observed by ISR aircraft. The more "spike" calls received by EW crews and/or increase or consistent emissions from targeted SAM radars provide indications that EA is not effective. The key is that there is no physical destruction of a radar system that will provide pilots with proof of the effect of EW.

It is acceptable practice for aircrew to "trust" the effects of EW, but no research was uncovered that explains the methodology for how EW is an acceptable practice to deny or degrade radar acquisition without observable BDA. Volumes of references exist in Air Force Tactics, Techniques and Procedures (AFTTPs) that explain how to employ EW assets based on the capabilities of the EW platforms versus the targeted radar systems, but no explanation exists as to how to measure the success of an EW system in combat. However, historical examples provide a venue to evaluate what specific actions were taken that has led to the full acceptance of EW aircraft.

The crux of integrating EW without actual BDA appears to hinge on training and tactics development as well as the integration of EW assets during major exercises. During the Vietnam War, F-100F Super Sabre aircraft were modified with electronic receiving equipment to detect and locate North Vietnam's SA-2 surface to air missile radars. During testing at Eglin AFB, Florida, these new "Wild Weasel" aircraft flew about three hundred runs against an emitter range. Test engineers had no way of evaluating from the ground the ability of the aircraft's receiving equipment to locate

[2]A spike is a radar warning receiver indication of an airborne intercept threat in track or launch (AFTTP 3-1, General Planning, Attachment 1)

the target radar. The real results would be measured in the aircraft cockpit. To overcome this problem of determining if the aircraft was detecting the target radar, engineers had to rig "a system to monitor our own signals, so we knew what had gone out. That way, if a Wild Weasel crew failed to pick up our signals, we knew what they should have received and when." [32] This form of evaluating an "effect" proved invaluable. The comparison of known data points versus what was displayed to the aircrew proved the capability of the system as well as provided confidence to the aircrew that would fly the Wild Weasel missions over North Vietnam.

As early as 1975, Exercise RED FLAG, conducted at Nellis AFB, Nevada, integrated EW assets with other combat aircraft. These exercises helped educate aircrew on the capabilities and limitations of EW systems against a realistic threat representation despite no physical damage produced by the EW effects. [19] Today, capabilities exist with the Joint Information Operations Range (JIOR) that can provide aircrew the same level of confidence in integrating cyber effects with traditional missions that have been realized with EW. [19]

2.6 Cyber Physical Systems and SCADA Design and Operation

"Cyber-Physical Systems (CPS) are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa." [23] At the heart of CPS is the need to make hardware and software interactions more predictable allowing more precise control of a system.

Supervisory Control and Data Acquisition (SCADA) systems, as a subset of a CPS, are a complex system used to control industrial processes through the use of computers, networks, and sensors (Figure 4). [30] SCADA is defined as an industrial measurement and control system consisting of central host or master (usually called a master station, master terminal unit or MTU); one or more field data gathering units (usually called remote stations, remote terminal units , or RTUs); and a collection of

standard and/or custom software used to monitor and control remotely located field data elements. [24]

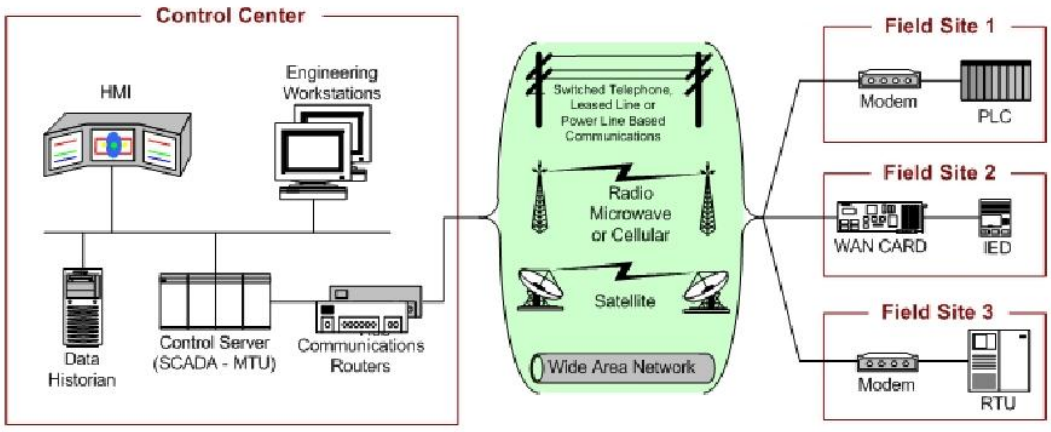

Figure 4: Typical SCADA Design from NIST 800-82 [30]

The Operations Control Center (OCC) consists of computers, networks, and databases. The sensors and control actuators are directly connected to remote terminal units (RTUs). [24] A human machine interface (HMI) provides the status to the operator on the state of the system, to include settings of sensors and actuators.

Commands from the OCC to the field units are sent via a communication link. A Master Terminal Unit (MTU) communicates with the RTUs. The MTU acts as the system controller (also referred to as host computer, host controller, or server). [4] Each network is different, but because of the distributed nature of SCADA systems, the network must be robust and capable of not just sending commands, but receiving data from RTUs. The MTU provides a capability to monitor and control processes.

Most SCADA systems employ redundancy to decrease the risk associated with lost or degraded services. The benefit of a SCADA system is the ability to increase the amount of automation. However, this attribute increases the susceptibility to attacks against the system. [24]

Lewis identified seven"wicked problems"[3] related to critical infrastructure protection (CIP): vastness, command, information sharing, knowledge, interdependencies, inadequate tools, and asymmetric conflict. [24] The problem of interdependencies are defined by Lewis as, "infinitely complex because of subtle interdependencies that mirror the organizations that created and operate them in addition to inherent technical interdependencies that exist." [24] By analyzing the problem from the defender's point-of-view, CIP can be used to look at system vulnerabilities and apply them to BDA. At first glance this risks mirror-imaging vulnerabilities to that of an adversary, but SCADA systems regardless of which country has them, contain the same general components.

Directly related to SCADA and the wicked problems is the notion of interdependencies caused by connecting, overlapping, and contradictory organizational structures resulting in complex and poorly understood interdependencies in various sectors. This is demonstrated in Figure 5. Not all of these critical infrastructures are operated with SCADA systems, but the interdependence of this critical infrastructures highlight that at some point, a SCADA system impacts the infrastructures operation.

These dependencies are further linked by networks. Regardless of the attack location, there are areas outside of the attack location that could be affected by the attack. Power and Energy is linked to every other major industry. There may be a time lag before some industries experience an impact caused by an attack, but the probability still exists for an effect to be measured.

The interdependencies of networked systems can be further illustrated as shown in Figure 6. Reigel contended that understanding critical infrastructures and their dependencies was critical due to the interoperability dependencies on other basic infrastructure services such as electricity, water, information and telecommunications. [34]

[3]A wicked problem, coined by Horst Rittel, results because the problem evolves as new possible solutions are considered.

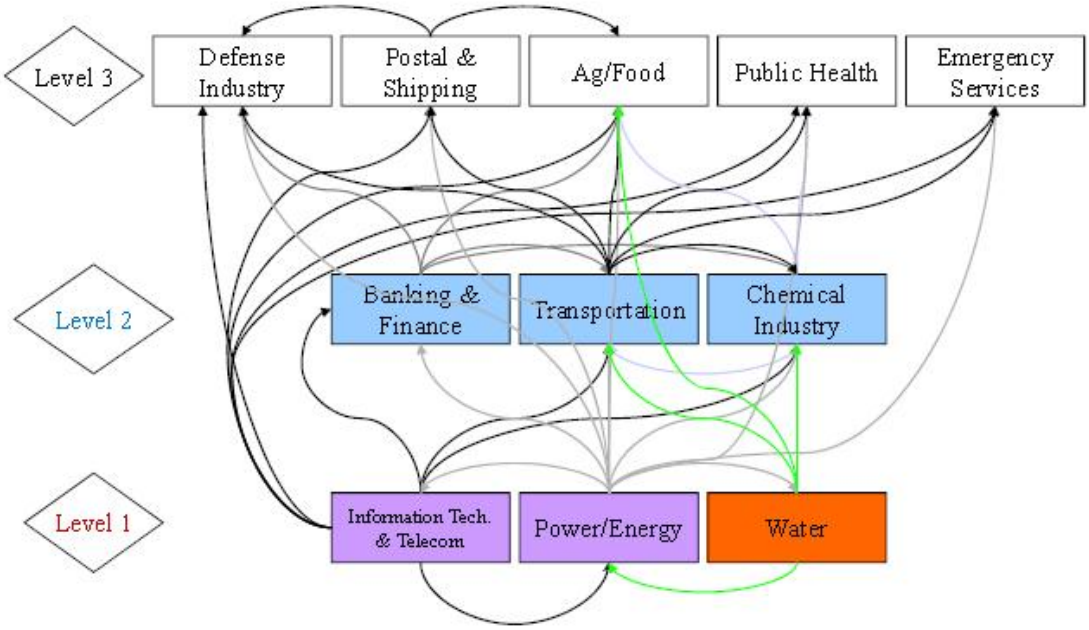

Figure 5: Levels and Dependencies of Various Sectors [24]

Because SCADA systems exist in these critical systems (water, power, telecommunications, etc.), nodes outside of a target SCADA system exist that can be observed and measured, either directly or indirectly. The nodes may or not present a quicker, more efficient way to measure the effects of an attack (BDA).

2.7 Conclusion

Cyber BDA presents unique challenges in cross-domain integration. However, applying Joint doctrine to cyber BDA provides a foundation that can be applied to most cyber BDA problems and is clearly understood in the joint community across all domains. CNE and traditional ISR provide the avenue for collecting relevant data that can be applied towards a strike analysis. The key component is the need to understand where data can be collected and ensure that the correct MOE is applied that will enable collection of relevant data.

Understanding how SA is obtained in cyberspace could enable a better understanding of how to recognize and report second and third order effects in the bat-

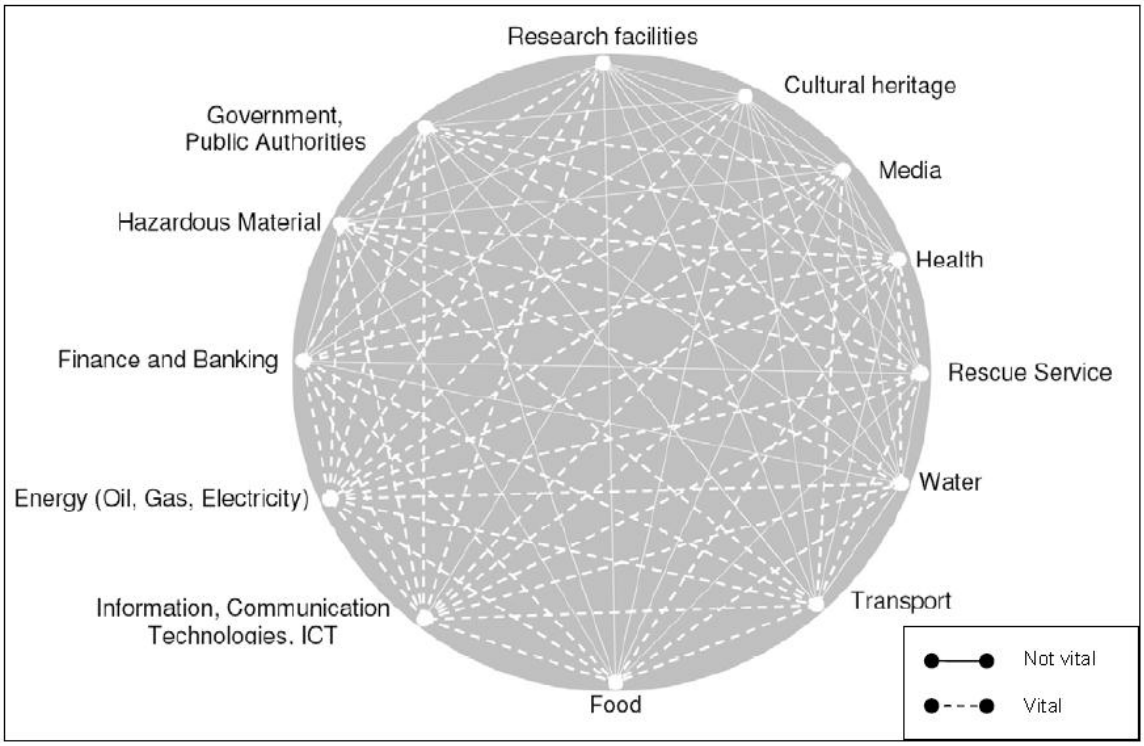

Figure 6: Dependencies in Health Care [34]

tlespace that are relevant to a cyber-attack. Personnel at all levels must apply clearly defined MOEs, allow for the collection of data through CNE and ISR, and look for connections outside of cyberspace to understand if the effect that is being measured is a correlated with a cyber-attack. The drive to identify the functions of cyber ISR is a critical component of this effort. By carefully modeling a network through deliberate IPOE, cyber operators can fully understand and exploit their understanding of a network providing a baseline before and after a cyber-attack. Through continued research and development, efforts such as cyber EBA can truly provide real time, to near-real time assessment before, during and after a cyber-attack.

As cyber BDA matures it is critical to understand that other effects suffer the same problems as cyberspace. EW relies on the known physics of the attacking system and the system being attacked to provide users an understanding on the effects that EW can provide. The absence of BDA has not stopped the use of EW in the battlespace.

The nature of cyberspace effects can result in effects far removed from the cyber target. An opportunity may exist to measure cross domain effects through an understanding of the physical components of a target system. SCADA systems are one such opportunity to exploit the physical effects of a cyber attack outside of cyberspace. The interdependence of critical systems highlights how an effect in one sector can impact and produce effects in other sectors. While not every sector is controlled by SCADA, the interdependence of all systems is central to understanding where second and third order effects can be measured.

III. Cyber Battle Damage Assessment Recommendations

> "We have moved past the civilities in the cyberspace domain." – General Kevin Chilton

The interdependencies that cyberspace shares in the physical domain can result in effects that can be measured outside of cyberspace. A method is required to conduct BDA outside of cyberspace and in the physical domains that leverage the capabilities of CNE with traditional ISR. This method must recognize the unique nature of cyberspace as well as the physical effects outside of cyberspace that can be measured. By carefully modeling a system that resides in cyberspace and identifying linkages that reside outside of cyberspace, planners can correctly apply MOEs that will capitalize on limited ISR resources which may result in quicker BDA.

3.1 Why Analyze Cyber Battle Damage Assessment?

JP 3-60, *Joint Targeting*, addresses the need for BDA to be conducted, but current doctrine does not clearly separate the physical from the non-physical and falls short of providing a foundation for total BDA. In an effort to focus joint terminology, General Cartwright, Vice Chairman of the Joint Chiefs of Staff, issued the Joint Terminology for Cyberspace Operations. New to the lexicon is a definition for *effects assessment*; [5] [13]

> "The timely and accurate evaluation of effects resulting from the application of lethal or non-lethal capabilities against a military objective. Effects assessment is composed of physical effect assessment, functional effect assessment, and target system assessment."

This definition is in line (word-for-word) with JP 1-02 for battle damage assessment except for the note at the end of the definition which states,"BDA is a specific type of effects assessment for damage effects." [13]

The integration of cyberspace with the traditional domains is currently centrally controlled by U.S. Cyber Command (USCC) and the service's cyber components. Under the USCC construct cyber operations are centrally controlled from USCC with direct support provided to Combatant Commanders (COCOM). [15] COCOMs

are still in the process of establishing staffs that can fully integrate cyberspace into full spectrum operations, and even when fully completed, USCC and the service components will still control the ability plan and execute cyberspace missions.

USCC identified three scenarios for conducting BDA reporting: (i) USCC conducts autonomous Computer Network Operations (CNO) and is the supported commander, (ii) USCC is the lead organization for CNO conducted in conjunction with other mission partners operations and is the supported commander, (iii) and USCC is not the lead operational organization and is the supporting commander. [38] The difference in these three scenarios is the nature of the support relationship. If the supported commander is USCC, then BDA will be analyzed within USCC in which processes exist for the purpose of cyber BDA. The target audience is the USCC leadership who are familiar with cyber effects and how cyber effects are measured. If the supported commander is one of the traditional Combatant Commander (COCOM) (CENTCOM, PACOM, EUCOM, AFRICOM), then the supported commander's staff would be responsbile for the final analysis of cyber and traditional BDA. These staffs may not be familiar with cyber BDA or the effects that can be achieved in cyberspace. The fusing of BDA data would become critical as USCC would send their cyber BDA results to the supported commanders staff for final analysis.

3.2 Nodal Analysis of a SCADA Attack

The purpose of identifying nodes and critical nodes is an important part of TSA. JP 5-0 defines a *system* as "a functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements; that group of elements forming a unified whole." [10] *System nodes* are defined as the tangible elements within a system that can be "targeted" for action, such as people, materiel, and facilities. *Key nodes* are a node that is critical to the functioning of a system.

For the purpose of this research, a *node* is defined as "A point within a network where a number of communications media intersect at a given location, facility, or equipment device. The identification of a node indicates that some sort of measure-

ment of the operation of the node is capable. Critical nodes generally result in a relationship with other important entities within the government, military or civilian population that can impact critical operations." [2] Figure 7 illustrates how military centers of gravity, nodes and links have interdependence with Social, Information, Infrastructure, Economic and Political environments.

AFDD 3-12, *Cyberspace Operations*, states that "Cyberspace links operations in other domains, thus facilitating interdependent defensive, exploitative, and offensive operations to achieve situational advantage". [15] While this statement focuses on cyberspace operations as a whole, the concept of interdependencies of cyberspace with other domains provides relevance in the basic understanding that whatever effect is accomplished in cyberspace could have an effect outside of cyberspace.

Any infrastructure automation system can be threatened by a CNA. [3] SCADA, as one such automation system, provides a good venue for nodal analysis for several reasons. First, the convergence the internet and all associated protocols to move information adds nodes that can either be affected or measured. Moving data through the Internet is causing convergence of other telecommunications systems such as TV, radio, and cellular phone as these systems rely on and use the same major nodes to transmit data. This is particularly true if the SCADA system relies on wireless technology that can be intercepted and inspected to determine what commands are being transmitted which may indicate a fault or alarm condition.

Second, a SCADA system isolated from other processes is an exception, not the norm. [31] SCADA, by its nature, requires interconnectivity with other processes, all of which can have their own connection to other systems. Even systems that use obscure protocols can be affected by reverse engineering to gain an understanding of how the system operates.

Nodal analysis of a SCADA system must be accomplished during target planning. Planners intimately familiar with the target through exploitation must help

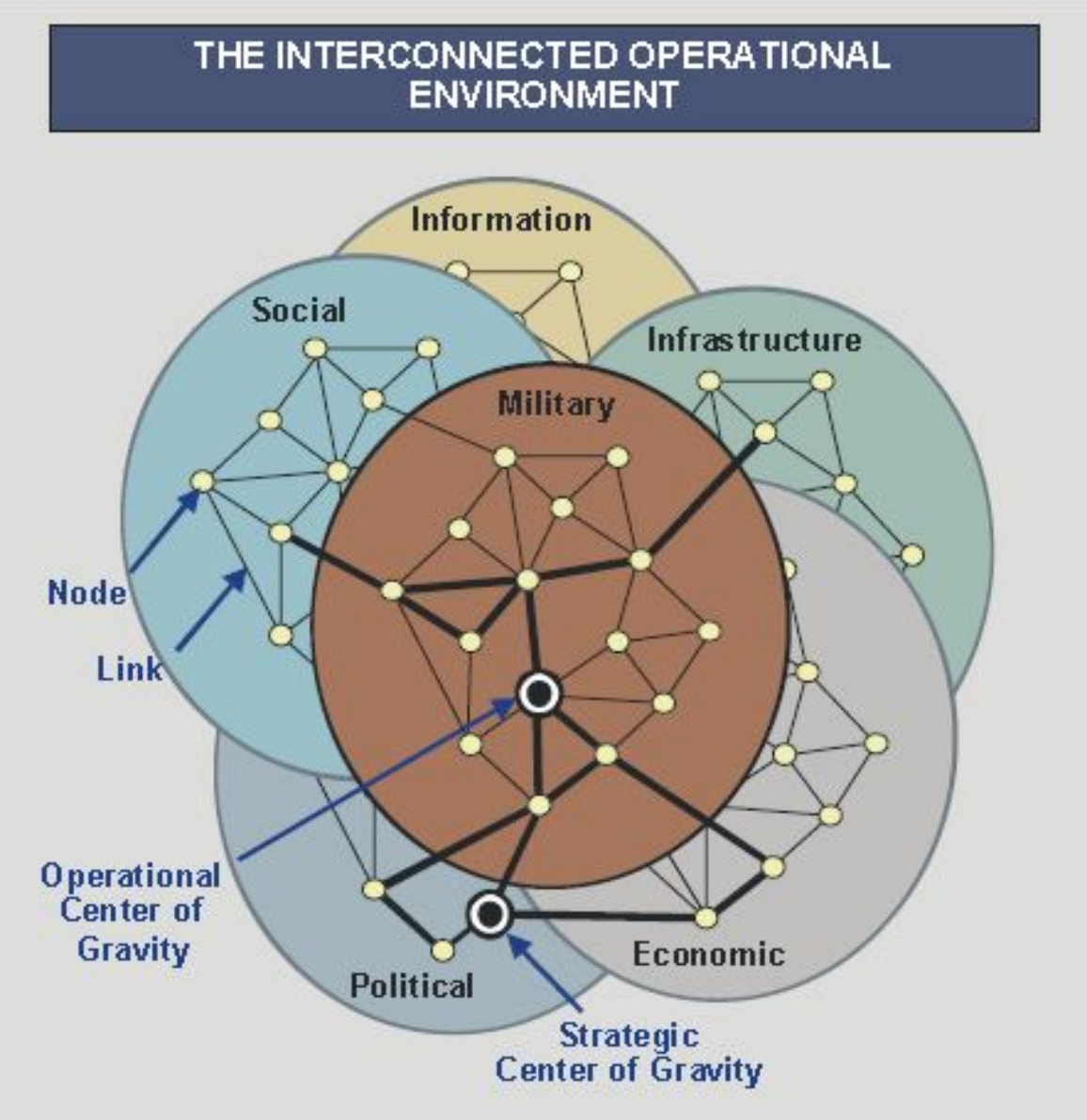

Figure 7: The Interconnected Operational Environment [14]

identify where all of the nodes of the SCADA system are, and help determine what indications can be measured once the attack takes place.

The type of attack will determine what direct and indirect impacts can be measured. A disruption of service attack may yield direct results that can be measured by physical means. Deliberately causing a mechanical system to fail through injection of a command could produce effects that can be measured by sensors. For example, the Idaho National Laboratory's test on attacking a SCADA system resulted in not just the physical destruction of a generator, but smoke was evident with increased heat that could be detected by EO/IR sensors. [36]

A cyber-attack against a SCADA system with an end result of attempting physical destruction may also result in indirect measures. The problem with measuring indirect effects resides in correlation of observed faults from within the system. [26]

The U.S. Department of Energy commissioned Pacific Northwestern National Laboratories (PNNL) to study the U.S. electric power system to look at future federal research, development and demonstration. [20] The PNNL white paper analyzed eleven major electrical disturbances in the United States from 1965 through 1998, noting that the technical problems are often unique to just that system. Factors such as geography, weather, networked topology, generation and load characteristics, age of equipment, staff resources, maintenance practices, and other issues are all unique to each system, and therefore, must be considered when evaluating any large power system. It is important to note a common theme of most of the power outages was a result of the tripping of circuits which caused a cascading effect, some of which were not fully realized until 59 minutes (New York City blackout, July 13-14, 1977) and 44 minutes (MAPP [now MRO, Midwest Reliability Organization] Breakup, June 25, 1998).

The recurring factors cited in the PNNL white paper were ubiquitous problems including: protective controls (relays and relay coordination), unexpected or unknown circumstances, understanding and awareness of power system phenomena (voltage

collapse), feedback controls (power system stabilizer, high voltage direct current, and automatic generation group), maintenance, and "operator error". [20]

Of these "ubiquitous" problems, the protective controls of the power generation system could possibly be measured outside of a SCADA cyber-target. Cascading effects of a power system could result in adjacent power production facilities in the same grid as the SCADA cyber-target to trip circuits as a result of the failures.

The target determines what nodal analysis should be conducted. For example, a typical power grid can consist of four components: generation, transmission and distribution, load, and SCADA. Within the U.S., it is estimated that there are 10,000 generating units powered by coal, nuclear, natural gas, hydroelectric, and petroleum that contribute to the overall U.S. and Canadian power grid. [24] The design of power grids are shaped by the regulations, economics of generation and technical design limits.

Attacking a SCADA system can produce effects that can be measured in either the generation and transmission and distribution. Since the load (consumer) drives the demand, the effects measured by the load should not be measurable unless baseline data is available that correlates the usage factors where unexplained drops or spikes in demand can be accounted for. Analysis of the area control error (ACE) (which determines the demand versus the capacity) and the RTU (which is responsible for transmitting data from the SCADA database to the control switches and receives inputs form the control switches) is one such way where effects can be measured.

Since power is on a grid, attacking one area of the grid may show results that other generation sources have increased their requirements by monitoring the SCADA database. An increased load from one ore more generators during non-peak times may be an indication that the SCADA database is sending commands to RTUs to compensate for a loss of generation capability at the target location. Measuring effects through this means is a concept of looking at the indirect, second, third and higher order effects.

When the SQLSlammer worm hit the Ohio Davis-Besse nuclear power plant in January 2003, the effects disabled a safety monitoring system for 5 hours and shut down a control network. [1] Although this cyber-attack didn't affect the control of the nuclear power plant, it demonstrates the susceptibility of the SCADA system. However, on August 14, 2003, a blackout hit the eastern United States when transmission lines had gone down, but were not detected by the control room alarm system. [20] The blackout escalated once the power degradation started and the SCADA/EMS alarm software failed to detect the fault. A series of lines "tripping" resulted in cascading line failures in eight states that started in Ohio. Although the failure started in Ohio, the effects were seen in seven other states.

When looking back at Figure 5, for example, everything is dependent on power, and therefore, there are more opportunities to look at second and third order effects when attacking the SCADA system of a power distribution center.

Power is but one example of a system that uses a SCADA system. Pipelines are also controlled by SCADA systems which monitor the pipelines and its contents, control pumps, valves, pressure, density and temperature. Successfully attacking a SCADA system that controls, for example, an oil pipeline may require planners to observe the end users (or customers). An increase in tanker trucks to a location serviced by the pipeline could be one indication that the attack was successful, but there are other second and third order effects that could be measured such as the indirect impact into all areas that the pipeline either serviced directly or indirectly.

A telecommunications system also offers another example of how attacking one system can have effects in other areas that are measurable. Since telecommunications are usually designed as redundant systems (landlines, cellular service, and satellite communication) different services can be used to reroute data as other services lose availability. Telecommunication services are tied together by nodes that ensure redundancy and availability. With thousands of nodes, the critical nodes are the ones that require special attention. Since data travels along copper and fiber lines at near

the speed of light, and switching stations are capable or rerouting communications in milliseconds, the overall effect is not obvious. However, since telecommunications do provide redundant services, attacking landlines via cyber may force an adversary to change the communications service that can be exploitable by other means, and therefore provide a second order effect when the secondary medium is used more frequently.

3.3 Pre-Attack Target Analysis

Computer network exploitation (CNE) serves as the baseline for cyber intelligence preparation of the operating environment (IPOE). IPOE has long served the traditional domains of land, sea, air and space so commanders could fully realize the adversary's posture, identify targets, and make a risk determination. Likewise, CNE maps out the adversary network identifying the known and unknown for commanders.

During interviews with subject matter experts from the National Air and Space Intelligence Center (NASIC) on how to conduct traditional nodal analysis (or TSA) important issues were discovered: [2]

– No classified or unclassified manual on how to conduct nodal analysis was available. As stated earlier, nodal analysis is more an art of how to combine several nodes and demonstrate relationships among the nodes.

– Limited data exists on the inclusion of the cyber domain with traditional domains for nodal analysis.

However, subject matter experts were able to provide an overarching methodology on how nodal analysis is conducted which is beneficial to this research. Specifically, there are several avenues that should be pursued as nodal analysis is conducted: [2]

1. Research existing databases. Information may already exist on identified nodes. For example, if conducting nodal analysis of a power generation plant with a SCADA system, intelligence may already be available on the location of the

main facility where the MTU is located, communications nodes that connect the main facility, as well as the remote locations where the RTUs are located. This data enables a perfect starting location and provides the known variables. Because multiple databases may exist, planners should not assume that the data in these databases are complete or absolute, but the mere presence of data allows planners to reference an existing location against other databases.

2. Research national standards. Most infrastructures are designed and developed based on national standards. Understanding what the national standards are may assist planners in searching for requirements that are not yet identified. For example, if there are national standards for telecommunications systems that can be physically identified and planners have yet to identify certain aspects of the telecommunications system, then searching imagery may result in an unknown physical structure that has the appearance of the required telecommunications system. Planners can then submit a request for information (RFI) through the appropriate channels to determine if the structure is the location they are looking for. Once that structure is identified, then collection activities can be requested.

3. Research existing records that were built as a result of the target facility. There may be public records of the facility to include who built the facility. Further records searches may yield what equipment was used inside the facility. For example, the power requirements for a facility may yield results of who built the power system. This data may in turn produce records of the equipment purchased for the facility which may yield a better understanding of how the power is distributed to the facility and if it is networked to outside sources for monitoring.

4. Search open source materials. Open source materials continue to provide a wealth of information. From Google Earth to newspaper articles, open source reporting is yet another key component to conducting good nodal analysis.

5. Develop baselines. Although it is important to fully understand how each node is connected to the overall system, a baseline is required to understand what is normal, below normal and above normal. Communication rates may vary at specific times of the day which may help the analyst identify not only the demand on the node, but the overall relevance of the node with the functioning of the overall system and how the node connects to other nodes. Developing patterns of operation or behavior is critical to fully understand the node.
6. All source reporting. There are other sources that can still contribute to nodal analysis that may not be organic to the planner's organization. Planners must have knowledge of, and access to all sources of intelligence if for nothing else but to ask a specific question (Request for Information (RFI)) to other organizations.
7. Finally, look for the obvious. Some information on nodes may not be readily available, but planners must look for the obvious. For example, lines of communications (roads, railways, bridges) may also be where communications and power lines were laid for convenience. Cell phone towers could also be used for other antennas due to their height above other terrain and obstacles.

Once the major nodes of the target system are found, RFIs can be submitted to look for the missing information. These RFIs are naturally prioritized first within the organization, and then at higher levels where multiple agencies compete for limited resources.

Increased data on specific nodes can be used as an input in other tools. CascadeNet "demonstrates the behavior of a cascade failure in an arbitrary network, and provides tools for studying the effects of network structure on its ability to resist cascade failure." [24] While this tool may appear to be network centric, the mere existence of a tool that can identify major nodes within a network can assist planners in looking at the critical nodes and looking for dependencies outside of the network. For example, in Figure 8, if Node 19 were a telecommunications node that was also connected outside of the SCADA system facility, then planners could search for the

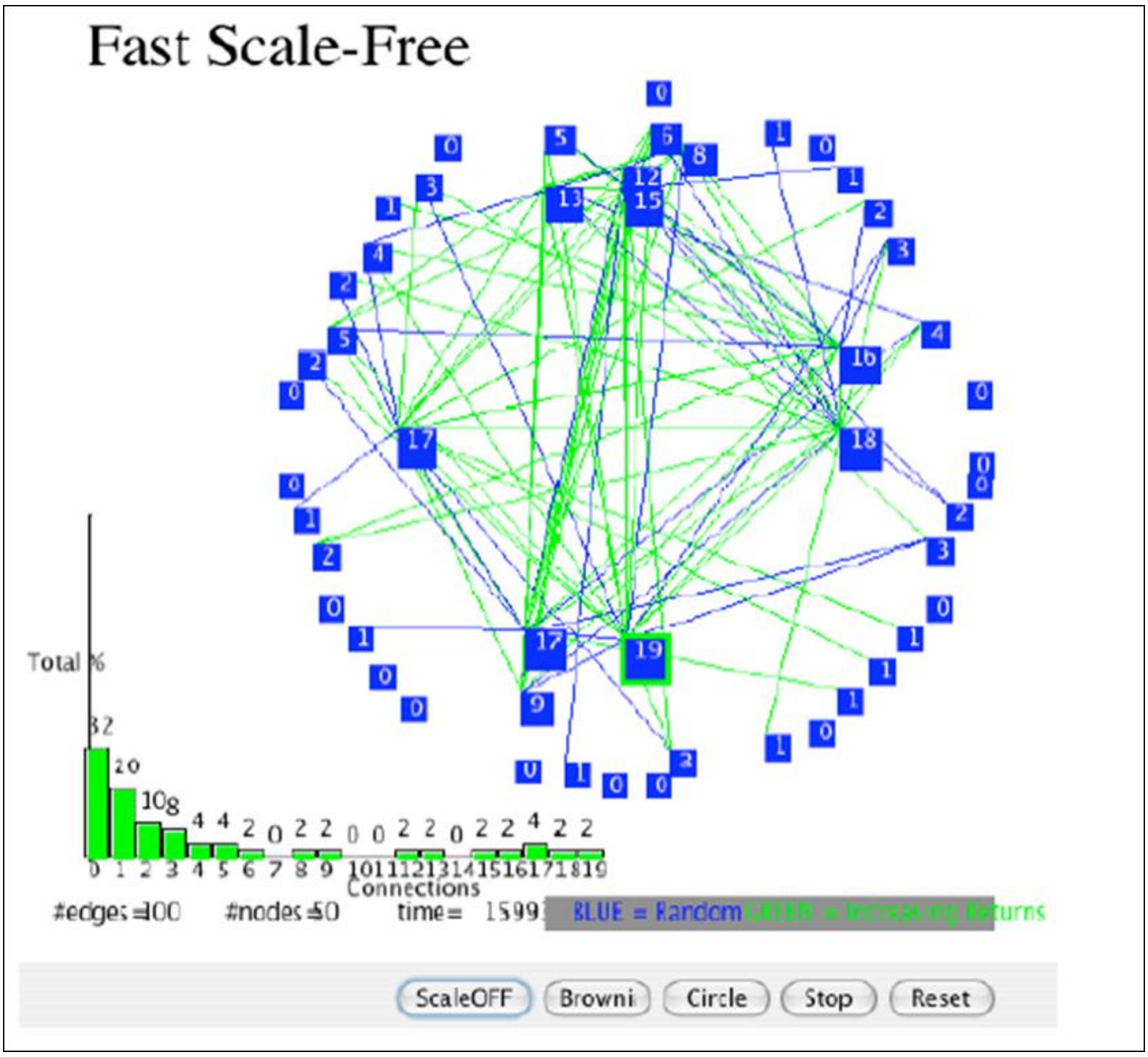

Figure 8: CascadeNet Tool Used to Determine Major Nodes within a System [24]

node that is connected to node 19 from the outside. If found, this new node could then be included in the overall nodal analysis and be assigned a MOE for the ISR collection plan.

As cyber targets are nominated, IPOE must include the primary cyber target as well as take into account what other effects will be achieved, whether intended or unintended. Vast knowledge may already exist of an adversary's infrastructure. The convergence of technologies demonstrates that at some point commands from the MTU to the RTU will travel on a path common to other systems. Likewise, the

RTU will control a device or sensor that will yield a change in way it was intended, producing a result that may yield a physical component that can be measured, perhaps more quickly than CNE.

The dependencies within most infrastructures require analyzing more than the network that is being attacked. In a report for the U.S. Department of Energy, Hauer and Dagle studied eleven cascading power failures, most of which were traced back to a single trigger. [20] This is significant in terms of pre-attack target analysis based on the need to determine what effects outside of the cyber attack can be measured. Assuming that most power systems are controlled by some SCADA system, an attack on that SCADA system will produce measurable effects outside of the attacked network.

The use of modeling is another avenue for determining relationships and dependencies within a SCADA system. Object modeling can identify the roles that exist between one object to another which can yield information on security vulnerabilities. [34] Identified vulnerabilities may yield information on vulnerable nodes that can be measured for BDA once a CNA is completed. Since power SCADA systems are so prevalent, the relationships that must exist for the SCADA system to operate effectively are well understood.

With sufficient data, modeling of networks can yield sufficient knowledge of significant nodes. [33] Models provide more than just nodes. Models also provide a means towards quantifying and qualifying the assumptions associated with building the model and therefore are valuable at looking at the input and output of each node.

As each node is identified, the model can be further expanded to nodes that are outside of the system thereby building a model of a system of systems resulting in the model that can be used for phase 3 BDA or assessing targeting system change.

Nodes can be looked at from the targeting perspective and early decisions can be made if the existence of the node results in an avenue to measure effects. For example, some nodes may be internal to the network with no capability to measure if the node is functioning correctly. Other nodes, such as a transmission device, may

be capable of measuring traffic which could produce results of an increase, no change or decrease in traffic once the CNA event takes place.

Once all nodes are identified, MOEs can be assigned to each node for inclusion into the ISR Collection Plan. This is critical since nothing will be reported unless there is a requirement to actually collect the data. Without an MOE data could remain in a database unused.

3.4 Sensor Cueing and Fusion of 2nd and 3rd Order Effected Nodes

The identification of nodes outside of the network (or cyberspace domain) opens up new venues for traditional ISR to collect data that can be used to make a determination as to the success or failure of a CNA. The ISR Collection Plan is the baseline for identifying which sensors can contribute to the collection for BDA. This can also be used to help identify probabilities of detection by each sensor which can contribute to the overall CA probability associated with the CNA.

A major assumption is that with a SCADA system the CNA location (where the CNA is targeting the payload) may not always produce measurable results at the location of the attack. For example, if the plan is to corrupt the MTU of a SCADA system in order to alter the command message to the RTU, then the result of the attack could yield results at the following locations:

1. At the MTU (can the command message to the RTU be inspected to determine if the CNA did alter the message).
2. At the communication nodes (can the command message be inspected at the communication node to determine if the CNA did alter the message).
3. At the Field Unit (RTU, sensors, etc) (can the results of the corrupted command message be measured through a change in how the sensor, valve, or other processes react).
4. At a node connected to the targeted system but separated by a different SCADA system such as a different power station (can the results be measured by de-

termining if a different power station increased power generation to supplement lower (or no) power generation from the targeted system).

5. At a node that receives inputs from the targeted system (is there an increase in telephone calls to a customer service center).

As data is collected for BDA from nodes outside of the targeted system, analysts must then determine if the data collected is a result of the CNA or a random event. The importance of understanding second and third order effects as it relates to cyber BDA increases in importance. The level of situational awareness cannot be measured directly in terms of collection systems (sensors) but rather the analyst looking at the raw data. As the raw data is evaluated and compared with the stated MOEs, level 1 SA as defined by Endsley is achieved (perception of elements). If not, the raw data will reside in a database either properly or improperly tagged.

As the raw data is then collected and the pieces of the data are applied towards a possible result from the BDA, level 2 SA (comprehension of current situation) is achieved. The pieces of second and third order effects are building towards a sight picture of determining if the collected data are a result of the CNA or some other event. However, it is important to note that because the MOEs helped define the requirements for collection the data, the data now resides outside of a database and should be included in the initial assessment.

Finally, the resulting BDA report is presented to the analyst that will make the final determination if the data collected is part of the CNA. The immediate effects of the CNA (measuring results inside the SCADA network) as well as the data from other nodes outside of the SCADA system can now provide a more comprehensive view of the intended effect against the targeted system resulting in Level 3 SA (projection of future status).

The overall impact for using nodal analysis helps shape the ISR Collection Plan, which contributes to identifying traditional sensors that can measure effects outside

of the SCADA network, as well as assists in ensure that relevant raw data is collected for consideration towards making a BDA decision.

3.5 Confidence of a Successful Cyber Attack and the Impact to Air Operations

Cyberspace will face the same challenges of incomplete and/or slow reporting that traditional BDA has suffered from. For cyber operations to be effective, CNA must yield measurable results that commanders can use at all levels of war (strategic, operational, and tactical). It is also important for mission planners that need additional options outside of a traditional kinetic attack.

If cyber operations transition to a supporting role, the supported commander must expect that a CNA can be measured satisfactorily that it meets the commander's intent. Furthermore, as the initial chapter illustrated, if cyber can replace traditional kinetic attacks, then BDA will be critical, and in some situations, the quicker the BDA is produced, the quicker additional measures can be implemented to include reducing the risk in the battlespace. If the BDA timeline for the F-117 strike against the Iraqi communications center in Bahgdad is used, the attack was critical for the air superiority battle.

At the heart of air operations is the air operations center (AOC). Since collection of multiple nodes may be required, the intelligence, surveillance, and reconnaissance division (ISRD) has a critical role in reviewing BDA reports and making recommendations to the Joint Forces Air Component Commander (JFACC). The ISRD will require the means to collect analysis from multiple sources and locations with sufficient subject matter experts to formulate a BDA decision. This BDA decision can result in a decrease to the risk in the battlespace which could result in more freedom of movement and increase the options to planners for sustained operations. Because so much is hinging on a BDA assessment, timely BDA decisions are critical to maintaining operations.

3.6 Conclusion

Cyberspace is unique yet the same principles that have applied to the traditional BDA problem is still relevant to how to conduct cyberspace BDA. The uniqueness of cyberspace demands a fresh look at how BDA is conducted to ensure every venue is pursued towards bridging CNE and traditional ISR. Each capability, when combined with other sources, produces better data for analysts to provide feedback to the commander.

SCADA, as a cyberspace attack vector, provides a way to understand how cross domain effects can be measured both in cyberspace and the physical domains. Not everything attacked through cyberspace can, or should be measured in cyberspace. The need for fast and accurate BDA resulting from a CNA can hinge on enabling other missions and/or reducing the risk in the battlespace.

By carefully conducting nodal analysis of a cyber physical system and reaching out beyond the borders of cyberspace, planners can look for opportunities to exploit effects, provide well defined MOEs, cue sensors, and reduce the timeline needed to conduct BDA. The results of which are critical to all forces operating in and around the battlespace.

As cyberspace operations become synchronized with operations in the traditional domains, commanders will require a means to measure the success of a CNA, or risk choosing a kinetic option that has a higher chance of timely and more certain feedback. Maturing cyberspace BDA procedures is one way to guarantee effects that can be achieved more quickly and efficiently in cyberspace are not discounted for kinetic options.

IV. Conclusion

> "While the time-tested principles of war will ultimately apply in cyberspace, its characteristics are so radically different that they demand significant innovation and changes to the way we organize and conduct military operations and tactics in this domain." [3]– General Keith Alexander

4.1 Research Results

It is possible to measure BDA of a CNA against a SCADA system through physical means outside of the cyber domain. Success relies on deliberate planning and extending the nodal analysis of the cyber target outside of the cyber domain. Significant work has already been accomplished in nodal analysis that may yield significantly more capabilities to measure effects than trying to distinguish the effects in cyberspace.

Limited ISR resources demand that only the best nodes be used to measure effects. Senior leadership advocacy and smart resource allocation is essential due to the nature of limited ISR resources. If properly prioritized with the correct MOEs, nodes outside of the cyber target system can contribute to evaluating second and third order effects that may ultimately provide analysts with a determination as to the success or failure of the cyber attack.

Historical events and experiments provide an initial starting point towards understanding what physical effects can be measured outside of the cyberspace. Although each system may be unique in terms of how it could respond to a CNA, each system will produce some effect that, if properly accounted for, could be measured in the physical realm. Nodal analysis of the target system beyond the cyber domain could help bridge cyberspace with the traditional domains.

Experience is already available with intelligence professionals that are trained in the art and science of BDA and nodal analysis. The challenge is not necessarily more sensors or better algorithms, but instead working towards a complete understanding of the target system beyond the traditional borders that define the system's processes.

4.2 Recommended Research

The information presented in this research was presented as a way to advocate the synchronization of the traditional warfighting domains of air, land, maritime and space with cyberspace towards improving nodal analysis for BDA. In an attempt to demonstrate how the convergence of technologies has inseparably linked the traditional domains with cyberspace, more research areas were found that were outside of the scope of this research.

1. The capability exists to model cyberspace effects as well as provide percentages of successful detection of an effect. Significant work is being conducted by U.S. Strategic Command to model cyber attack tools which would provide probability of success, or stated differently, a probability of kill (pK). This effort would further increase the ability of cyber operators to communicate to commanders and mission planners the value of using CNA versus traditional kinetic strikes against a target.
2. Research has already been conducted on breaking down models further to show weights of importance on each indicator. Additional research in this area could show which critical nodes are more likely to yield specific BDA results which can help address the limited intelligence resources towards better prioritizing which nodes would be measured. This is particularly important for developing an ISR collection plan that does not waste limited resources.
3. As part of this research, a classified thesis was reviewed. In this thesis, the author analyzed several CNA operations and found that limited baseline data was available for cyber operations. Without good baseline data, analysis of raw data is difficult. BDA still requires a "before" and "after" view of the target systems. This is not to say it is not already accomplished, rather, physical damage assessment is already difficult under the best circumstances from a kinetic attack. Adding non-kinetic attack (CNA) into the equation can further

complicate the process. More research is required to fully understand what physical effects outside of the cyber domain can be measured.

4.3 Application to the Warfighter

Planning for cyber effects with the traditional domains is difficult due to several factors[1]:

1. Lack of understanding from operators in the traditional domains (air, land, sea and space) on what cyberspace capabilities can and cannot achieve. This includes the access and authorities required to attack through cyberspace, time-lines of attacking and assessing, and command and control of cyber forces.
2. Lack of understanding from cyber operators on how the traditional domains synchronize effects and the time-lines needed to fully utilize an effect (which may include the required BDA to validate a successful strike against a target that may be required for access).
3. The speed and uncertainty of war which happens at the detection of the first adversary or the first engagement of the adversary (also referred to the fog and friction of war).

For warfighters in every domain, cyberspace holds the keys to some areas that have been difficult in previous operations. The ultimate goal of every commander is usually to attempt to decrease the risk to friendly forces as quickly as possible to gain an advantage over their enemy. This is especially true to reduce attrition of one's own forces while inflicting as much attrition on the enemy. Operations in cyberspace may not solve every problem, but inclusion with the traditional domains will certainly improve overall joint operations.

Understanding how to synchronize BDA in all domains is important. If an attack cannot be measured towards accomplishing a commander's goals, then additional

[1]These views are based on the author's personal experiences in planning exercises and deliberate planning.

resources may be needlessly expended to service an additional attack so the effects can be better measured. Just as intelligence resources are not infinite, neither are weapons and munitions in an AOR. Efficiencies can be realized at all levels of war when cyberspace is fully integrated into all operations.

Warfighters tasked with synchronizing cyber operations must understand and be capable of asking some basic questions about the cyber target:

1. What is the time-line required to gain access into the target-system and determine if a cyber effect can be achieved?
2. Can the effect be measured?
3. How long will it take to measure?
4. What is the certainty that, if the effect can be measured, the attack was successful?

By conducting nodal analysis, planners may identify targets that can be attacked both kinetically and non-kinetically. For example, if the desired effect is to shut down a power generation facility, planners may determine that it is easier to sever the communications node between the MTU and RTU kinetically versus attempting to use CNA to change the command from the MTU to the RTU. Likewise, planners may find a way to use CNA to disrupt the power supply to a facility that supports surface to air missiles, denying the use of a primary communications nodes to target friendly aircraft.

The ultimate goal of any operation is the meet the needs of the commander's goals and priorities. It should not matter how it is done, just that it gets done as expeditiously as possible with minimum risk to friendly forces.

Bibliography

1. SQL Slammer Worm Lessons Learned for Consideration by the Electricity Sector. Technical report, North American Electric Reliability Council, 2003. `http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf`.

2. Interview with Subject Matter Experts, 2011. Several SMEs from NASIC and USCYBERCOM were interviewed for this research, but due to the classification of this research they preferred to remain anonymous.

3. General Keith B. Alexander. Warfighting in Cyberspace. *Joint Forces Quarterly*, pages 58–61, 2007.

4. Stuat A. Boyer. *SCADA Supervisory Control and Data Acquisition 4th Ed.* ISA, 2010.

5. General James W. Cartwright. Joint Terminology for Cyberspace Operations. JCS Memorandum, Nov 2010.

6. Tom Clancey and Chuck Horner. *Every Man a Tiger*. G.P. Putnam's & Sons, 1999.

7. Richard A. Clark and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About It*. HarperCollins, 2010.

8. Sebastian M. Convertino, Lou Ann DeMattei, and Tammy M. Knierim. Flying and Fighting in Cyberspace. Technical report, Air University, 2007.

9. Department of Defense. *Conduct of the Persian Gulf War*, Apr 1992. `http://www.dod.gov/pubs/foi/reading_room/404.pdf`.

10. Department of Defense. *Joint Publication 5-0, Joint Operations Planning*, 2006.

11. Department of Defense. *Joint Publication 2-0, Joint Intelligence*, 2007.

12. Department of Defense. *Joint Publication 3-60, Joint Targeting*, 2007.

13. Department of Defense. *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, 2010.

14. Department of Defense. *Joint Publication 3-0, Joint Operations*, 2010.

15. Department of the Air Force. *Air Force Doctrine Document 3-12, Cyberspace Operations*, 2010.

16. James G. Diehl and Charles E. Sloan. Battle Damage Assessment, The Ground Truth. *Joint Forces Quarterly*, 46:59–64, Jul 2010.

17. Mica R. Endsley. Toward a Theory of Situational Awareness in Dynamic Systems. *Human Factors*, pages 32–64, 1995.

18. Mica R. Endsley and Debra G. Jones. Disruptions, Interruptions and Information Attack: Impact on Situational Awareness and Decision Making. *Human Factors and Ergonomics Society*, pages 63–67, 2001.

19. Andrew P. Hansen. Cyber Flag, A Realistic Cyberspace Training Construct. AFIT Thesis, March 2008.

20. John F. Hauer and Jeff E. Dagle. White Paper on Review of Recent Reliability Issues and System Events. Technical report, Pacific Northwest National Laboratory, 1999.

21. Kammal Jabbour. The Science and Technology of Cyber Operations. Technical report, Air Force Research Lab, Rome NY, 2009.

22. John T. Rauch Jr. Assessing Air Power's Effects: Capabilities and Limitations of Real-Time Battle Damage Assessment. Technical report, Air War College, 2002.

23. Edward A. Lee. Cyber Physical Systems: Design Challenges. Technical report, University of California, Berkeley, 2008. `http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html`.

24. Ted G. Lewis. *Critical Infrastructure Protection In Homeland Security.* John Wiley & Sons, 2006.

25. Martin C. Libicki. What is Information Warfare?, 1995. `http://www.iwar.org.uk/iwar/resources/ndu/inforwar/a003ch03.html`.

26. Martin C. Libicki. *Conquest in Cyberspace.* Cambridge Press, 2007.

27. Martin C. Libicki. Cyber Security and Cyber Deterrence, 2011. `http://outerdnn.outer.jhuapl.edu/rethinking/VideoArchives/DrMartinLibickiPresentationVideo.aspx`.

28. Stew Magnuson. Military "Swimming in Sensors and Drowning in Data", 2010. `http://www.nationaldefensemagazine.org/archive/2010/January/Pages/Military%E2%80%98SwimmingInSensorsandDrowninginData%E2%80%99.aspx`.

29. Robert A. Miller and Daniel T. Kuehl. Cyberspace and the "First Battle" in 21st-century War. *Defense Horizons*, 68:1–6, Sept 2009.

30. National Institute of Standards and Technology. *NIST 800-82, Guide to Industrial Control Systems Security*, 2008.

31. Ludovic Pietre-Cambacedes, M. Tritschler, and G.N. Goran. Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs. *IEEE Transactions of Power Delivery*, pages 161–172, 2011.

32. Alfred Price. *The history of US Electronic Warfare vol III.* The Association of Old Crows, 2000.

33. Gregory J. Rattray. An Environmental Approach to Understanding Cyberpower. In *Cyberpower and National Security*, pages 253–274. Potomac Books, Inc., 2009.

34. Christopher Riegel. Risk Assessment and Critical Infrastructure Protection in Health Care Facilities: Reducing Social Vulnerability. http://securitrus.com/documents/CIPhealthcaresectoroverview.pdf.

35. Steven K. Rogers, Richard A. Raines, Matthew Kabrisky, Jeremiah T. Rogers, Adam Rogers, Thomas Burns, Mark Oxley, Mark M. Derriso, Paul D. Williams, Bobby D. Birrer, Gilbert G. Kuperman, and Kenneth W. Baueri. Beyond OODA Nonsense, 2010. www.academic-conferences.org/ppts/RogersKeynote.ppt.

36. Frank Saxton. The Aurora Power Grid Vulnerability, 2008. http://unix.nocdesigns.com/aurora_white_paper.htm.

37. E. Tikk, K. Kaska, K. Runnimeri, M. Kert, AM Taliharm, and L. Vihul. Cyber Attacks Against Georgia: Legal Lessons Learned. *Presentation at the NATO Cooperative Cyber Defence Centre of Excellence*, 2008.

38. U.S. Strategic Command. *Battle Damage Assessment (BDA) Concept of Operations (CONOP) - Draft*, 2010.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
16–06–2011	Graduate Research Project	28 June 2010 — 16 June 2011

4. TITLE AND SUBTITLE

Leveraging Traditional Battle Damage Assessment Procedures to Measure Effects From A Computer Network Attack

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Richard A. Martino, Maj, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

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

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

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENG/11-08

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

Col Mustafa R. Koprucu
505th Command and Control Wing
138 Hartson Street
Hurlbert Field FL 32544 505ccw.cc@hurlburt.af.mil
DSN 579-5054

10. SPONSOR/MONITOR'S ACRONYM(S)
505 CCW

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approval for public release; distribution unlimited. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The art of warfare in cyberspace is evolving. Cyberspace, as the newest warfighting domain, requires the tools to synchronize effects from the cyber domain with those of the traditional land, maritime, space, and air domains. Cyberspace can compliment a commander's theater strategy supporting strategic, operational, and tactical objectives. To be effective, or provide an effect, commanders must have a mechanism that allows them to understand if a desired cyber effect was successful which requires a comprehensive cyber battle damage assessment capability. The purpose of this research is to analyze how traditional kinetic battle damage assessment is conducted and apply those concepts in cyberspace. This requires in-depth nodal analysis of the cyberspace target as well as what second and third order effects can be measured to determine if the cyber-attack was successful. This is necessary to measure the impact of the cyber-attack which can be used to increase or decrease the risk level to personnel operating in traditional domains.

15. SUBJECT TERMS
BDA, Cyber ISR, Nodal Analysis, CNA, CNE, SCADA

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert F. Mills
U	U	U	UU	66	19b. TELEPHONE NUMBER *(include area code)* (937) 255–3636, ext 4527 robert.mills@afit.edu