Fall 2017

Methodology to Perform Cyber Lethality Assessment

Matthew W. Zurasky
Old Dominion University

Recommended Citation

Zurasky, Matthew W.. "Methodology to Perform Cyber Lethality Assessment" (2017). Doctor of Philosophy (PhD), dissertation, Engineering Management, Old Dominion University, DOI: 10.25777/48r8-ke52
https://digitalcommons.odu.edu/emse_etds/25

METHODOLOGY TO PERFORM CYBER LETHALITY ASSESSMENT

by

Matthew W. Zurasky
BSE May 1983, Duke University
MBA December 2002, Averett University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTORATE OF ENGINEERING

ENGINEERING MANAGEMENT

OLD DOMINION UNIVERSITY
November 2017

Approved by:

____
Dr. C. Ariel Pinto (Director)

____
Dr. Holly Handley (Member)

____
Dr. Pilar Pazos-Lago (Member)

____
Dr. Jang Park (Member)

ABSTRACT

METHODOLOGY TO PERFORM CYBER LETHALITY ASSESSMENT

Matthew W. Zurasky
Old Dominion University, 2017
Director: John Adams

The Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Lethality and Effectiveness Branch is the Navy's subject matter experts (SME) on target vulnerability, weapon lethality, and weapon effectiveness. Branch personnel currently exercise expertise in the kinetic and directed energy weapon domains. When the Navy develops weapons in the kinetic and directed energy domains, there are clear and well established procedures and methodologies for performing target characterization that support weapon-target pairing. Algorithms exist to describe the likelihood of damage effects. It is natural that in the paradigm shift to cyberspace warfare that the Branch provide these same services to the warfighter in the cyber domain. In simplistic terms, cyberspace lethality is the opposite side of the cybersecurity coin. Rather than protecting own-systems, a cyber-offensive capability is applied to an adversary's network to disrupt normal operations. However, there are currently no established procedures or methodologies for performing cyberspace target vulnerability characterization (CTVC) or cyber lethality and effectiveness analyses. Nor is there any organization currently dedicated to performing these tasks. Previous efforts were conducted stand-alone and did not produce a meaningful or accepted methodology. This dissertation is intended to research existing lethality prediction processes for kinetic and directed energy weapons and modify them for the new cyber weapon realm such that the new methodologies will allow analysts to perform effective and efficient CTVC and cyber weapon lethality performance assessments. The methodology will be presented to the Joint Technical Coordinating Group for Munitions Effectiveness for

consideration and adaptation. The cyber lethality research and methodology development has the support of NSWCDD management which has designated cyber warfare engineering to be a thrust within the NSWCDD 2015-2020 Strategic Plan. This thrust includes providing support for offensive cyber operations through the experimentation, development, test and evaluation, training, integration, and certification of combat and weapon systems that will allow the naval commander to project power by the application of force in or through cyberspace.

This thesis is dedicated to the proposition that the quest for knowledge should never end. Learning something outside one’s area of expertise can be especially satisfying.

"One's work may be finished someday, but one's education never."
-- Alexander Dumas

ACKNOWLEDGMENTS

There are many people who have contributed to the successful completion of this dissertation. I extend many thanks to my committee members for their patience and guidance regarding the direction of my research. A special thank you is extended to Dr. Pinto, as my academic advisor, for guiding me across the finish line. Ms. Deanna Kroner, as the ODU Military Program Coordinator in Dahlgren, was instrumental in determining my plan of study and making sure that my courses suited the degree requirements.

I would also like to acknowledge the encouragement I have received from my family. They have been very supportive even as I spent nights and weekends attached to the computer. They have also made it exciting to try to keep ahead of my wife, Amy, and daughter, Katrina, in the number of degrees earned.

NOMENCLATURE

CCB	Configuration Control Board
CTVC	Cyberspace Target Vulnerability Characterization
DMod	Data Modification
DRep	Data Repudiation
DoD	Department of Defense
DoS	Denial of Service
FALT	Failure Analysis Logic Tree
FMEA	Failure Modes and Effects Analysis
HEL-RAPT	High Energy Laser Review Analysis and Process Team
ICS	Industrial Control System
IF	Integrated Fires
JMEM	Joint Munitions Effectiveness Manual
JTCG/ME	Joint Technology Coordinating Group for Munitions Effectiveness
MisI	Misinformation
NSWCDD	Naval Surface Warfare Center, Dahlgren Division
NIDR	Navy Information Dominance Roadmap
$P_{d/h}$	Probability of Damage given a Hit
P_{Deliv}	Probability of Delivery
$P_{Exploit}$	Probability of Exploit
P_h	Probability of Hit
P_{Intel}	Probability of Intelligence
P_K	Probability of Kill

$P_{k/d}$	Probability of a Kill given Damage
$P_{K/H}$	Probability of Kill given a Hit
RCE	Remote Code Execution
SCADA	Supervisory Control And Data Acquisition
SME	Subject Matter Expert
TGM	Target Geometry Model

TABLE OF CONTENTS

Section Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
1. INTRODUCTION

The Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Lethality and Effectiveness Branch is the Navy’s subject matter expert (SME) on threat vulnerability, weapon lethality, and weapon effectiveness. Branch personnel demonstrate expertise in the kinetic and directed energy weapon domains. The Lethality and Effectiveness Branch ensures that warfighters employ effective weapons by providing decision-makers with objective technical assessments of engagement options. The mission is accomplished through the application of four core capabilities:

- The ability to quantify the performance of complex weapon systems,
- The ability to define & exploit the threat,
- The ability to capture the dynamics of weapon/threat interaction in mathematically tractable models, and
- The ability to perform first principles numerical calculations (Zurasky, 2015).

1.1 Purpose

It is natural that in the paradigm shift to cyberspace warfare that the Branch provide these same services to the warfighter in the cyber domain. However, there are currently no established procedures or methodologies for performing cyberspace target vulnerability characterization (CTVC) or cyber lethality and effectiveness analyses. Nor is there any organization currently dedicated to performing these tasks. NSWCDD must close this capability gap to keep pace with new technology development. The Branch finds itself in the same situation that the French Committee of Artillery reported to their Minister of War in 1800: “Ici il n’est pas question de changer, il faut créer [Here there is no question of changing, it is necessary to create]" (Dahlgren, 1852).

1.2 Problem

This dissertation is intended to research and adapt existing lethality prediction processes for kinetic and directed energy weapons to the new cyber weapon realm such that the new methodologies will allow analysts to perform effective and efficient CTVC and cyber weapon lethality performance assessments. This dissertation will propose a methodology to bridge the capability gap while meeting the security and data distribution requirements imposed by the Navy and the Department of Defense.

1.3 Method and Procedure

This dissertation is developed from unclassified public sources and public release information from government sources. This will limit some of the details available to describe the methodology, but it has the benefit of eliminating any concerns relative to security or releasability of the information. Also, this paper refers to a "cyber target" and a "cyber threat" interchangeably. Both of these terms refer to the adversarial system that is to be exploited by the cyber weapon.

CHAPTER 2

2. BACKGROUND / HISTORICAL CONTEXT OF THE STUDY

2.1 Literature Review

Military mission planners rely upon validated weapon and target information to determine the probability of success for mission scenarios. A process exists within the Department of Defense to match kinetic weapons to targets so that an optimum solution can be selected. A similar process for cyber weapons is necessary or the United States military will cede this aspect of warfare to adversarial parties; combatant commanders will not utilize cyber warfare without knowing the effects it will produce or the potential collateral damage that may occur.

There is limited academic or professional literature relating to the assessment of cyber weapon lethality. A few companies have performed studies at the behest of the U.S. Government but these efforts are classified and are not releasable in this forum. Others have documented aspects of the cyber defense perspective.

Joint Publication 3-12(R) (U.S. Department of Defense, 2013) provides the military's doctrine regarding the planning, preparation, execution, and assessment of joint cyberspace operations. This document introduces cyberspace and its integration across the range of military operations. The doctrine describes three layers of cyberspace, as shown in Figure 1: the physical network layer, the logical network layer, and the social (cyber-persona) network layer. The document also discusses roles and responsibilities relating to the planning and coordination of cyberspace operations.

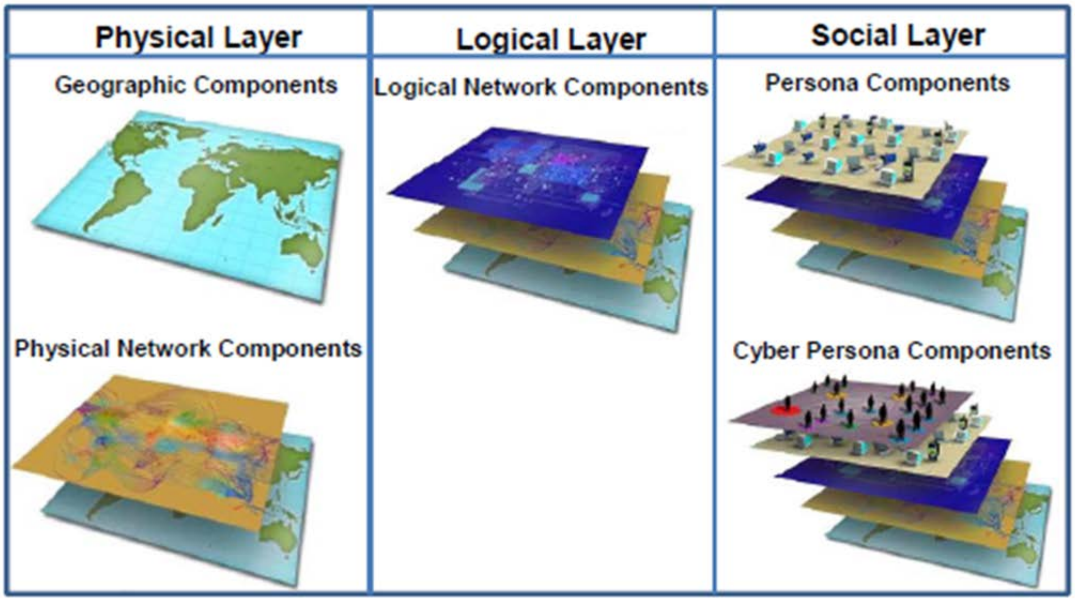

Figure 1 Cyber Domains

Some activities have developed schemas and nomenclature to describe characteristics of malware and other cyber capabilities. The Malware Attribute Enumeration and Characterization (MAEC^{TM}) language developed by the Mitre Corporation is one example of this (Beck, Kirillov, & Chase, 2014). Mitre also developed the Trusted Automated eXchange of Indicator Information (TAXII^{TM}) framework that defines a set of message exchanges and services to share information (Connolly, Davidson, & Schmidt, 2014). Using its kill-chain model, Lockheed Martin describes the phases of intrusions and indicators that may identify patterns of an advanced persistent threat (Hutchins, Cloppert, & Amin, 2014). These authors propose an intelligence feedback loop to decrease an adversary's likelihood of success with each subsequent intrusion attempt. This is a precursor to predicting cyber weapon performance.

The U.S. Army Cyber Command tasked the RAND Corporation to study and develop a strategy for providing cyber support to units at the Army corps level and below (RAND Corporation, 2017). The resulting document describes the overarching goals, objectives, and associated activities for these forces. Part of this strategy describes what the Army needs to do to implement an overall vision for tactical cyber operations. In addition, the report discusses the potential incorporation and use of offensive cyber operations, specifically at the tactical level.

However, without a standardized and accepted methodology to predict cyber weapon performance, cyber capability will not be released to the corps or equivalent level and will remain limited in its applications to strategic targets.

2.2 Development of Weapons and Systematic Analyses

Mankind has developed and utilized weapons since the earliest recorded history. Ancient cave and rock drawings show humans using spears and bows for hunting. Over time, stone and wood were replaced with metals such as copper, bronze, and iron. Eventually gunpowder was invented and kinetic weapons using lead, iron, and steel shot became commonplace. Accordingly, critical scientific methods have been applied to the development of kinetic weapons. Analyses of threat systems characteristics and the calculations of interactions between kinetic weapon systems and threat systems have been conducted for many years. Benjamin Robins published his *New Principles of Gunnery* in 1742. In it he expressed mathematical equations to describe factors such as the effects of air resistance on projectiles. He also noted that the penetration depth achieved by musket balls appeared to be a function of the ratios of the square of their velocities (Collins).

The United States followed European practices and established schools and curriculums for military sciences. At the insistence of President Washington, Congress in 1794 authorized the establishment of a "Corps of Artillerist and Engineers" at West Point, New York. No formal course of study was adopted, so President Thomas Jefferson proposed and signed legislation on 16 March 1802 establishing that a Corps of Engineers "… shall be stationed at West Point and constitute a Military Academy …" to focus on science and engineering (Ambrose, 1999). Likewise, in 1825, President John Quincy Adams asked Congress to establish a Naval Academy "for the formation of scientific and accomplished officers." His proposal, however, was not acted upon until 20 years later when, through the efforts of the Secretary of the Navy George Bancroft, the Naval School was established without Congressional funding. The curriculum for the initial class of 50 midshipmen included mathematics, navigation, gunnery, and steam. In 1850 Congress authorized the Naval School to become the United States Naval Academy (U.S. Navy).

In addition to having separate methods and academies to train officers, up until the post-World War II era and the establishment of the Department of Defense (DoD), the War Department and the Department of the Navy handled their business separately. For the Navy, the Bureau of Ordnance and Hydrography was established by Congress in 1842 to develop new weapons and ordnance materiel, to improve existing items, and, in wartime, to oversee large-scale production and procurement of such equipment. In 1862 the Bureau was divided into separate commands as the Bureau of Ordnance and the Bureau of Navigation. The first Chief of the Bureau of Ordnance, Rear Admiral John A. Dahlgren, played a significant role in the development of naval gunnery. First in the Bureau of Ordnance and Hydrography, and then as the Chief of the Bureau of Ordnance, Admiral Dahlgren applied scientific methods to become the “father of modern naval ordnance” (U.S. Navy). In doing so, Admiral Dahlgren became an ordnance expert, developed a percussion lock, and wrote a number of books, including *The System of Boat Armaments in the United States Navy*, *Shells and Shell Guns*, and *Naval Percussion Locks and Primers*. Under his command, the Navy established its own foundry to manufacture new equipment. Its first product was the boat howitzer, designed for use aboard ships and in landings.

The Naval Surface Warfare Center Dahlgren Division, named for Rear Admiral Dahlgren, has been at the forefront of performing these types of analyses for nearly one hundred years. Figure 2 illustrates an early lethality test performed at Dahlgren in 1922. Test data today is used to develop high fidelity and engineering level models that are engaged to determine probability of occurrences of lethal and non-lethal events.

Eventually, Secretary of Defense Robert MacNamara saw the benefit of standardized practices across all the military services and established the tri-service Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME). Currently, NSWCDD is a leading Navy participant in the JTCG/ME and is actively improving vulnerability, lethality, and effectiveness simulation models.

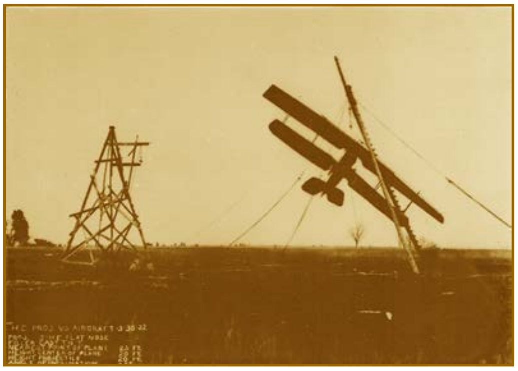

Figure 2 Lethality Test Performed at Naval Proving Grounds Dahlgren in 1922

2.3 Tri-Service Systematic Processes for Kinetic and Directed Energy Weapons

The JTCG/ME was established in 1964 to provide warfighters, operational commanders, DoD targeteers, weaponeers, planners, weapon system designers, and logisticians with the most current and accurate non-nuclear weapons effectiveness data. JTCG/ME is a tri-service organization whose approved data is available to authorized personnel. Since the 1960's the JTCG/ME has governed a standardized process that is accepted by all three services within the DoD. The standardized process outlines common test data collection practices and modeling methodologies. The principal products of the JTCG/ME are known as the Joint Munitions Effectiveness Manuals (JMEMs). The JMEM information includes damage/kill probabilities for specific weapons and threats, physical and functional characteristics of munitions and weapon systems, threat vulnerability, obscuration on weapon effectiveness, and analytical techniques and procedures for assessing munitions effectiveness (U.S. Army Material Systems Analysis Activity, 2016). The JMEMs were developed to provide a set of data developed with known methodologies that would permit a standardized comparison of weapon effectiveness across all three service communities (Driels M.). Combatant commanders and mission planners in the field can use the JMEM information to determine the best combination of weapon ordnance and tactics to attack and render inoperable enemy systems and structures.

The JTCG/ME has recently adapted its standard kinetic energy threat vulnerability characterization process to directed energy weapons through the High Energy Laser Review Analysis and Process Team (HEL-RAPT) efforts. The current JTCG/ME kinetic and laser processes determine the vulnerability of threat platforms, weapons, and infrastructure, predict the ability of an ordnance package to inflict damage to a threat, and measure the ability of a weapon to engage and inflict damage given the performance and environmental conditions. Thus, field commanders have the ability to pair both kinetic and directed energy weapons to threats.

The JTCG/ME process has evolved to reflect the increased capabilities of models and computational systems. However, newer methodologies continue to use foundational principles that are now well established. For example, the following definitions have been established and are accepted in the vulnerability/lethality community (Zurasky, 2015):

- Vulnerability – the characteristic of a threat that causes it to suffer functional degradation as a result of manmade damage (Threat Vulnerability)
- Lethality – the ability of a munition to inflict damage on a threat sufficient to cause functional degradation in its ability to complete its designated mission(s) (Weapon Lethality)
- Effectiveness – the overall ability of a weapon system to engage and inflict damage on a vehicle sufficient to cause functional degradation (Weapon System Effectiveness).

2.4 Systematic Analyses for Electronic Warfare and Psychological Operations

The kinetic and directed energy weapons that physically damage an incoming threat – and thereby destroying/altering its payload/warhead or propulsion in such a way that the intended effect on the threat is severely impeded – are designated as hard-kill measures.

Electronic warfare is the military action that involves the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action that retains friendly use of the electromagnetic spectrum (Frieden, 1985). Psychological operations are "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives" (Naef, 2011). Electronic warfare and psychological operations are designated soft-kill measures. These methods are more dependent upon outside influences than kinetic and directed energy weapons to be effective. They also have a more difficult time predicting and evaluating performance.

Most stakeholders in the military environment (warfighters, acquisition professionals, Congressional staffers) understand the contributions of hard-kill measures against materiel. That is, while they may not be able to quantify the exact tonnage of bombs or missiles to destroy a threat, they certainly understand that bombs and missiles can be used to destroy materiel threats. However, there is a lack of shared knowledge relative to soft-kill methods such as electronic warfare and psychological operations. This leads to pressure to provide more thoughtful and explicit documentation to decision makers. While there is a burden to develop and provide the increased information to decision makers, there can be significant benefits for future soft-kill measures. An improved shared understanding of the return on investment can potentially improve advocacy for these efforts and also improve the efforts themselves by imposing more rigorous assessments (Paul, Yeats, Clarke, Matthews, & Skrabala, 2015).

For electronic warfare, mission planners attempt to qualitatively predict its effectiveness. The electronic warfare contribution is required to be effective at a particular time and location. However, the electronic warfare contribution is currently not very well quantified; instead it is predicted to be non-existent, fair, or potentially likely to be effective. For this reason it is often considered to be an ancillary contributor and so is not counted upon for mission planning purposes.

Psychological operations are often unconstrained by a particular location or time element. Although psychological operations should include a time horizon for their completion, changing behaviors can require significant investments in time and resources. Thus, due to the long-term nature, many psychological operations do not lend themselves to intermediate or periodic progress measurements (Paul, Yeats, Clarke, Matthews, & Skrabala, 2015).

2.5 Required Evolution to Assess Cyber Weapons

In just a few decades, the Navy moved from a fleet of sail and steam-powered ships to a high-tech fleet with nuclear-powered vessels (submarines and surface ships) and supersonic aircrafts. The service is now undergoing another significant change to adopt cyberspace as a new warfighting domain. Others have recognized this situation. Israeli Major General Aviv Kochavi has stated that cyber warfare "will soon be revealed to be the biggest revolution in warfare, more than gunpowder and the utilization of air power in the last century" (United Press International, 2014).

The January 2012 announcement by the DoD that it plans to enable the U.S. military to conduct a "combined arms campaign across all domains – land, air, maritime, space, and cyberspace" makes it clear that we are moving past the time of strictly using kinetic weapons (U.S. Department of Defense, 2012). The Navy Information Dominance Roadmap for 2013-2028 emphasizes that Navy Integrated Fires (IF) will coordinate all elements within the blue kill chain and disrupt adversary kill chains. This will allow U.S. Naval forces to seize and hold the initiative in combat and to limit an enemy's freedom of maneuver and action. The Roadmap states that IF will require new capabilities to fully employ integrated information in warfare by expanding the use of offensive cyber effects to complement existing and planned kinetic weapons within the battlespace (U.S. Navy, 2013).

Cyber lethality finds itself in a situation similar to the soft-kill weapons; most DoD stakeholders do not have an intrinsic understanding of the process or potential outcomes of cyber weapons. Therefore, it is imperative that commanders be given a measure of the predicted performance of cyberspace weapons.   Without this commanders won’t be able to properly weigh the benefit of offensive cyberspace capabilities.

CHAPTER 3

3. METHODOLOGY

3.1 Assigning a Methodology to Cyber Lethality

As reported by The Economist magazine, a senior defense official implied that cyber weapons will be used as an adjunct to conventional weapons and noted that "if a cyber attack is to be used as a military weapon, you want a predictable time and effect" (War in the fifth domain, 2010). More recently, the Defense Science Board presented a new report on cyber deterrence to the U.S. Senate Armed Services Committee. The report proposes the accelerated acquisition of scalable offensive capabilities. These are in line with the desires of U.S. Cyber Command head Admiral Michael Rogers who wants to structure Cyber Command teams much more like special operations forces and give local commanders more license to use offensive cyber weapons (Tucker, 2017). Obviously, a predictable effect necessitates an efficient and appropriate cyber lethality prediction methodology.

As in the case for kinetic weapons, the objectives of a cyber weapon lethality and effectiveness prediction process are to promote consistency and improve weapon system evaluation accuracy across DoD. Without a proper assessment and prediction process, commanders will remain reluctant to employ cyber weapons. Consistency is implemented through a common set of definitions and assumptions that are used by each of the Services to produce weapon system performance estimates. This commonality ensures that significant differences, if any, are attributable to the weapon system and threat characteristics rather than the methods employed by the individual Services. Also, standardization facilitates a common interpretation and meaningful comparison of weapon system performance. Thus, the predictions delivered by a cyber effectiveness analysis are likely to be accepted by the warfighting community.

Given the various effects capable to be enacted by cyber weapons, the lethality and effectiveness prediction methodology must be robust enough to be tailored to suit each particular analysis. That means there must be some common structure that gives the analyst leeway to develop assessments against threats and for kill effects not yet encountered.

3.2 Existing Process to Assess Kinetic Weapons

The process established to assess kinetic weapons has been long established and understood by the tri-service lethality and effectiveness community. The process allows an analyst to assess the physical interactions between ordnance and the threat and to determine if the resulting damage is sufficient to negate the threat’s mission. There are multiple steps to the process.

Once a threat system is identified the analyst must collect intelligence on the threat and identify critical system elements. Using a standardized format, a Threat Geometry Model (TGM) is created to show the physical interconnectivities of components and, if appropriate, the significant crew members. A critical systems analysis is developed to illustrate the functional connections. Once a desired kill level is associated with the threat, a Failure Analysis Logic Tree (FALT) for the system components is developed to indicate which components factor into damage effects. A typical FALT structure is illustrated in Figure 3. A Failure Modes and Effects Analysis (FMEA) follows to link particular damaged components to functional degradations.

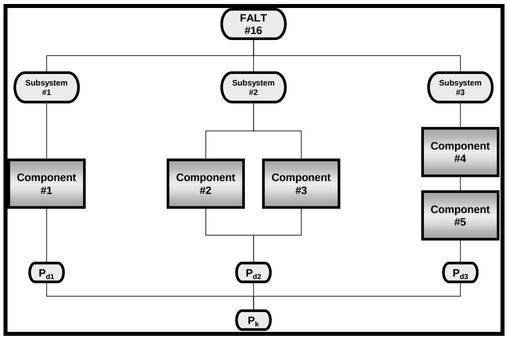

Figure 3 Typical Failure Analysis Logic Tree (FALT)

Component vulnerabilities are estimated based upon test data, computational physics hydrocode analyses, or engineering level analyses. Most component vulnerability inputs are generated using engineering level analysis. Examples include:

- Penetration equations/program with a spreadsheet, and
- Specialized algorithms (e.g., Jacobs-Roslund equation for explosive detonation) (Naval Surface Warfare Center Dahlgren Division, 2014).

An example graph of component fragility curves (also known as probability of damage curves) is shown in Figure 4. It shows that given a force of *x* the component designated with the yellow curve will be damaged with a higher probability than the components designated by the red and blue curves.

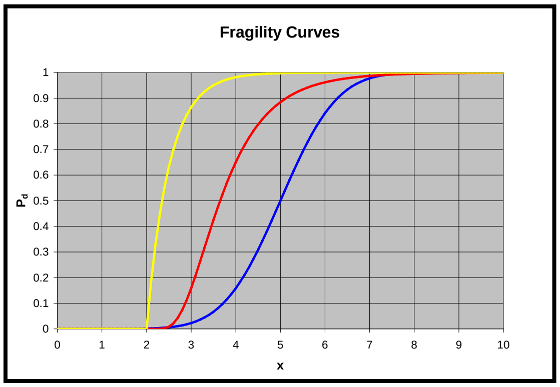

Figure 4 Example Fragility Curves

Once the TGM has been constructed and the fragility of components estimated, the threat vulnerability process is completed. The second part of the JTCG/ME process pertains to characterizing U.S. weapons. This is done using standard data collection methods appropriate to the weapon effects type. For fragmentation weapons, data is collected for fragment masses, shape, velocities, and material. The data is saved in a zonal data (“z-data”) file. For blast weapons, a Comp B or TNT equivalent explosive charge weight is determined. Penetration data is collected for projectiles and shaped charge devices. Lastly, for laser weapons, propagation and irradiance on the threat is calculated using engineering-level simulation codes that utilize the expected engagement geometry and the TGM information.

Given the completed vulnerability assessment and the weapon characteristics, an analyst can pair the threat with a weapon and perform a lethality estimate. This estimate provides a probability of kill given a hit ($P_{K/H}$) on the threat and is dependent upon the munition characteristics, the threat vulnerability, the kill definition criteria, the velocity and orientation at impact. Driels provides examples of kill definitions as shown in Table 1 (Driels M. R., 2013).

Table 1 Examples of Kill Definitions

Target Type	Kill Definitions
Land Vehicles	K – catastrophic kill (not repairable) M0 – mobility kill (cannot move, immediately M40 – mobility kill (cannot move within 40 minutes) F – firepower kill (cannot fire)
Parked Aircraft	PTO – repairs requiring at least 5 minutes PTO_4 – repairs requiring at least 4 hours PTO_{24} – repairs requiring at least 24 hours
Personnel (standing)	Defense (prevent) within 30 seconds Assault (prevent) within 30 seconds Assault (prevent) within 5 minutes Supply (prevent) within 12 hours

For a typical lethality estimate, each point on threat is assigned a single shot $P_{K/H}$. The calculations at each point include penetration, blast, and fragmentation effects. The results are illustrated in an image called a “vulnagram” to highlight the best aimpoints for maximum effects. A sample vulnagram is shown in Figure 5 (Naval Surface Warfare Center Dahlgren Division, 2014).

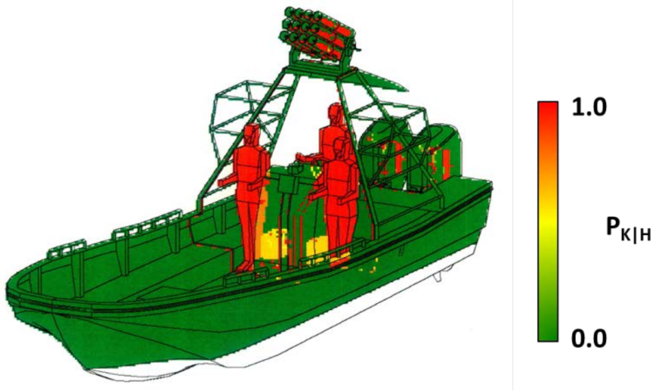

Figure 5 Vulnagram of a Small Boat Threat

The effectiveness of a weapon is defined as the Probability of Kill (P_K) and is the product of many probabilities. Often the equation is truncated to $P_K = P_h * (P_{d/h} * P_{k/d})$ because the analyst assumes that prior events occurred to position the kinetic weapon at the intersect point. P_h is the accuracy term and ($P_{d/h} * P_{k/d}$) is the lethality term (equivalent to $P_{K|H}$ in the previous paragraph. Simulation codes such as *Advanced Joint Effectiveness Model* and *Effectiveness ToolBox* calculate these terms. Figure 6 illustrates a typical effectiveness equation for a missile intercept event (Zurasky, 2015). For the most part, all of the probabilities to the left of the end-game values (P_h, $P_{d/h}$, and $P_{k/d}$) are nearly equivalent to one. The true variability is associated with the warhead interactions.

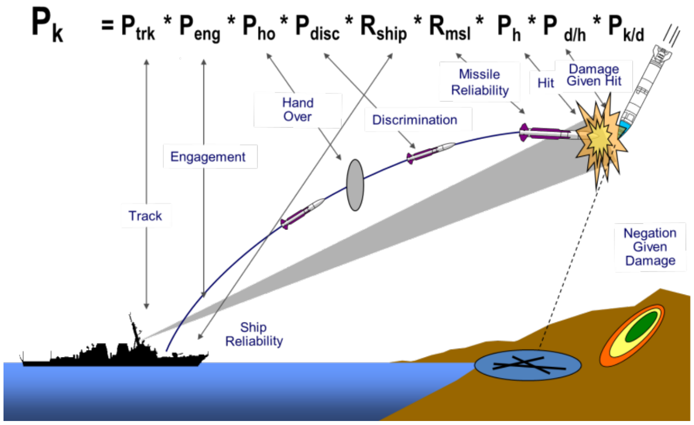

Figure 6 Kinetic System Effectiveness Kill Chain

3.3 Inherent Differences Between Cyber Weapons and Kinetic Weapons

Weapons can impart damage to threats in several ways. Kinetic weapons cause damage through physical means such as blast, fragment penetration, and heat effects. Kinetic weapons are effective when the damage caused to the threat results in the failure of critical components. Cyber weapons do not interact physically with threats; rather, they manipulate software to achieve effects.

A high explosive blast warhead is designed to achieve damage through overpressure effects. Upon detonation, the high explosive material converts to a gas at extremely high pressure and temperature. The pressure of the expanding gas fractures the weapon case and allows the gas to escape. The air surrounding the case is then compressed and a blast (shock) wave is transmitted through it. Blast weapons are particularly effective against buildings and personnel in the open. This is because when a threat is exposed to a blast wave, it will experience the overpressure and under-pressure effects. The internal cavities on insufficiently reinforced bodies reflect and amplify the blast wave. This causes injuries in the lungs, gastrointestinal tract, and ears in humans and damage in equipment compartments and manned spaces in buildings and vehicles.

Fragmenting weapons and projectiles both operate on the same premise: masses accelerated to great velocities impacting and penetrating materials. In the case of a fragmenting warhead, hundreds of naturally-forming or scored fragments are ejected from the explosion in the path or proximity of the threat. A certain number of the fragments intersect and penetrate the body of the threat. The depth and volume of the penetration is dependent upon the mass of the fragment and its impact velocity. Similarly, a projectile penetrates material by exerting extreme force on a point-like small area on the threat. Its depth of penetration is again dependent upon the mass of the projectile. The effectiveness of a fragmenting or projectile weapon depends upon its ability to penetrate and damage a critical component.

Laser weapons focus a concentrated beam of visible or invisible light at a point on a threat. This light energy is absorbed by the intercepting body and converted to heat. The temperature increase of the material causes its weakening and deformations. Given enough heating, material may melt away and expose internal components. Burning occurs if the temperature exceeds the material's ignition point.

Kinetic weapons interact physically with threats in accordance with the laws of physics. For example, as shown in Figure 7, a blast wave appears as a rapid rise from ambient to a peak pressure point which is followed by an exponential decay to a value below ambient. It then returns to the ambient condition. The penetration of fragments or projectiles follow Newton's Second Law of Motion and requires the weapon to overcome the resistive force of the threat material (Zook, 1977). Lastly, the irradiance of a laser on a threat is dependent upon the output power, atmospheric attenuation, and beam quality characteristics such as beam width and divergence.

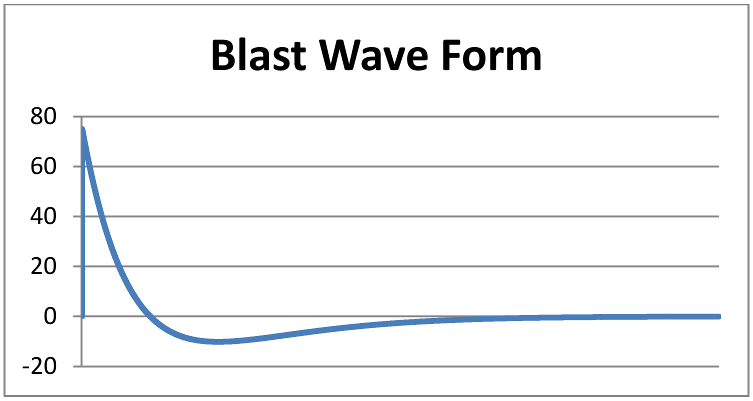

Figure 7 Pressure-Time Profile of a Blast Wave

Cyber weapons allow practitioners to compromise computers and processors by identifying important data to manipulate, steal, or destroy. Cyber weapon penetration into a system is not achieved physically. Instead, cyber weapons leverage inter-computer protocols to gain access to threat computers. Some cyber weapons engage networking and administrative tools to probe and map networks and to conduct lateral movements across networks. Other cyber weapons actually manipulate the computer code to alter the output of algorithms. These cyber weapons, however, do not directly rely upon the laws of physics to inflict damage. That is, weaponized code does not come with an explosive charge. Potential physical damage must be created by the targeted system itself through stopping or altering ongoing processes (Rid & McBurney, Cyber-Weapons, 2012).

3.4 Initial Proposed Process to Assess Cyber Weapons

Similar to kinetic weapon assessments, a cyber lethality methodology must include the following:

- Identification and definition of cyber kill effects,
- Cyber threat vulnerability assessment,
- Cyber weapon characterization, and
- Cyber lethality estimate generation.

Identification and Definition of Cyber Kill Effects

The first element of the common structure is a common set of kill criteria. In some cases, a cyber weapon may enact effects that cause physical damage similar to a kinetic weapon. For example, a cyber weapon that causes a servo controller to turn off will induce the same failures to a flight system as those caused by a penetrating projectile damaging the same servo controller.

The existing definitions for mobility kill and firepower kill still apply to cyber weapons for those effects that cause physical damage. Mobility kills are those where the damage or effect is sufficient to render a platform incapable of executing controlled movement within the time interval being assessed. Firepower kills are those where the damage or effect is sufficient to render the threat immediately incapable of engaging its weapon. On the other hand, cyber weapons do not appear to contribute to Crew kills. Crew kills are those where injury or effects to the crew are such that they are incapacitated and enough crewmembers are incapacitated such that the threat's mission cannot be accomplished.

However, the added variation in cyber effects makes the prediction of cyber weapon effectiveness problematic. The outcomes of some of these effects do not directly correspond to existing kinetic weapon kill definitions. Cyber-specific kill effects include:

- Denial of Service – computer or network resources are made unavailable to intended users by temporarily or indefinitely disrupting services of a host connected to the Internet
- Misinformation – false or incorrect information is spread intentionally
- Data Modification – data is inserted, deleted, or altered in a manner that is intended to appear genuine to the user
- Data Repudiation – data or information is made to appear to be invalid or misleading
- Spoofing – an attempt to masquerade as someone else
- Network Enumeration – usernames and info on groups, shares, and services of networked computers are retrieved

These need to have quantifiable metrics associated with them. They need to have a time associated with the initial effect and they need to have an associated duration period. The following are initial proposals; completed definitions will have to be reviewed and accepted at the tri-service level. Note that some cyber effects have a lasting effect. That is, the effect continues to exist until a corrective action is taken by the adversary.

- Denial of Service –
    - Kill/Effect: damage or effect to the threat system resulting in its disruption of service
    - Time Start: immediate
    - Time Duration: 5 minutes (DoS), four hours (DoS4), or 24 hours (DoS24)

- Misinformation –
  - Kill/Effect: false or incorrect information is spread intentionally
  - Time Start: immediate
  - Time Duration: 5 minutes (MisI), four hours (MisI4), or 24 hours (MisI24)
- Data Modification –
  - Kill/Effect: data is successfully inserted, deleted, or altered in a manner that is intended to appear genuine to the adversary
  - Time Start: immediate
  - Time Duration: 5 minutes (DMod), four hours (DMod 4), or 24 hours (DMod 24)
- Data Repudiation –
  - Kill/Effect: data or information is successfully made to appear to be invalid or misleading
  - Time Start: immediate
  - Time Duration: 5 minutes (DRep), four hours (DRep 4), or 24 hours (DRep 24)
- Spoofing –
  - Kill/Effect: successfully masquerading as someone else
  - Time Start: immediate
  - Time Duration: indeterminate
- Network Enumeration –
  - Kill/Effect: successfully retrieving usernames and info on groups, shares, and services of networked computers

- Time Start: immediate
- Time Duration: indeterminate

It is important to note that Misinformation and Repudiation must provide the adversary with the proper balance of belief and disbelief. Libicki writes that prior beliefs or opinions drive how users interpret information. Users are more likely to believe something to be true if it supports their prior thoughts. This is especially true when they rely upon their beliefs and fail to research the information that is presented (Libicki, 2007).

Other cyber effects are likely to be added in the future. However, these are sufficient to develop a general methodology.

Cyber Threat Vulnerability Assessment

Similar to kinetic weapon assessments, a multi-phase cyber lethality threat vulnerability assessment must include the following: (1) selection of the threat, (2) definition of the system boundaries and identification of critical components, and (3) identification of component vulnerabilities. Figure 8 illustrates a typical network diagram with firewalls and an intrusion detection system. These are typical system components which must be described. Any such network may also include wifi and smart phones. Other example networks include Supervisory Control And Data Acquisition (SCADA) systems for remote monitoring and control and dedicated military systems with stand-alone dedicated processors.

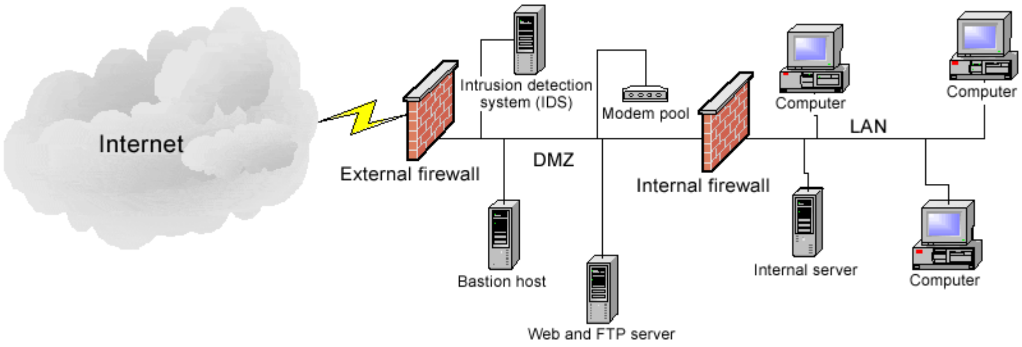

Figure 8 Typical Network Diagram

In Phase 1, the analyst will identify the threat and begin to gather baseline information. This will include a brief description of the threat, relevant photos or schematic drawings, top level FALTs, and a list of assumptions pertinent to the analysis. It is important to recognize that the complexity of the threat will affect the type and amount of information available. Is it a multi-faceted system with numerous nodes or is it a distinct element like a cell phone or a website? Is it is a commercially available product like a communications center or is it a limited-access product like a military radar system? If it is a limited-access product, does it include commercial components? Are specifications widely available? Can failures in the threat system be easily determined?

In Phase 2, the analyst will begin to develop a threat model to include a detailed description of the threat, a network model (if appropriate), a detailed FALT, and a FMEA. For a cyber evaluation, the physical components of the threat are less significant. Instead, the software code and its functional elements are the items to be evaluated. The system boundaries are important when developing the network model. Too broad of a system boundary leads to an overly complex system definition; too narrow of a boundary may exclude key elements that are affected by the weapon. The key aspect of Phase 2 is the FMEA. It identifies the critical functional elements and the conditions that need to be altered in order to change the state of the threat system and achieve the desired effect. For example, the FMEA can identify a servo controller as a single point failure node. A well-designed cyber weapon can then alter the state of the servo causing loss of system control.

When determining the boundaries of the threat, the question may be raised: should the network path be considered part of the cyber threat characterization or is it part of the cyber weapon characterization since the weapon cannot exist without the network? Or is it part of the environment, merely the medium through which the weapon travels to its targeted threat? This author holds the position that the network path is independent of both the threat and the weapon but it is important because it enables the access points associated with the threat.

In Phase 3, the analyst will identify the vulnerability of the identified critical cyber components. The vulnerability can be considered a flaw in the software or environment that can be exploited. Identified flaws without an exploitation path are not vulnerabilities; they are merely design weaknesses. Vulnerabilities can exist in the threat system design, within installed software, within its network configuration, or be associated with its business operations. Some known vulnerabilities include (Sood & Enbody, 2014):

- Backdoors and Hardcoded Passwords – hardcoded passwords embedded in the firmware that allow attackers who discover them to gain complete access to these systems;
- Remote Code Execution (RCE) – security issues such as buffer overflows (stack, heap, and integer), use-after free errors, race conditions, memory corruption, privilege escalations, dangling pointers in operating system components, browsers, critical

systems such as ICS/SCADA, routers, other software such as Microsoft Office, Adobe Reader, Java, etc.;

- Insecure Protocols, Spoofing and Hijacking – undocumented and insecure protocols allow hijacking and spoofing of communication channels
- SQL Injections – weaknesses in web applications that allow attackers' queries to be executed directly in the backend database; and
- Insecure Authentication and File Uploading Flaws – security issues arising from inability of the systems to implement granular control through proper authentication and authorization checks.

Sood and Enbody list real-world cases associated with these vulnerabilities. These are summarized in Table 2.

Table 2 Significant Cyber Vulnerabilities and Real-World Cases

Vulnerability Types	Real World Cases – Vulnerable Systems
Backdoors and Hardcoded Passwords	• Global Positioning System (GPS) Satellite Communication (SATCOM) systems provided by Harris, Cobham, JRC, Iridium and Hughes were vulnerable • Supervisory Control and Data Acquisition Systems (SCADA) provided by Siemens, TURCK, etc. were vulnerable
Insecure Authentication and File Uploading	• Global Positioning System (GPS) Satellite Communication (SATCOM) systems provided by Harris, Cobham, JRC, Iridium and Hughes were vulnerable
Remote Code Execution	• SCADA systems provided by ICONICS GENESIS32, BizViz, IntegraXor, Sielco Sistemi, etc. were vulnerable to Buffer Overflows • XMLDOM Zero-day vulnerability was exploited to attack U.S. Veterans of Foreign Wars' website • Operation Pawn Storm uses vulnerabilities in MS office files to target U.S. military officials
SQL Injections	• Royal Navy website hacked using SQL Injection • U.S. Army website hacked using SQL Injection
Insecure Protocols, Spoofing and Hijacking	• Global Positioning System (GPS) Satellite Communication (SATCOM) systems provided by Harris, Cobham, JRC, Iridium and Hughes were vulnerable • Possible attacks to spoof GPS communication to control U.S. drones

All of the various cyber components must be listed with their associated vulnerabilities. This will provide the cyber weapon designer with a complete description – equivalent to the kinetic weapon Threat Geometry Model – against which to choose the most appropriate available cyber capability to cause damage.

Cyber Weapon Characterization

As described in Chapter 2, a cyber weapon is a software capability by which an attacker exploits vulnerabilities within a targeted system to cause damage. None of the kinetic weapon characteristics apply: items such as warhead fragmentation and blast overpressure data, guidance methods, fuze functions, and reliability. Instead, new characteristics will have to be developed. These should be categorized according to cyber weapon's functional responsibilities: Reconnaissance, Lateral Movement, and Payload.

In order to penetrate and exploit an adversarial network, like the one illustrated in Figure 8, some aspect of the cyber weapon will require networking reconnaissance tools to map out the threat network, to probe potential avenues, and to monitor activity. The weapon will be required to locate the desired target components and identify ways to get to them. By utilizing host and port scan applications to map out the network resources, the weapon will develop an inventory of relevant target components. The reconnaissance characterization should include descriptions of its function and the operational environment in which it operates. Based upon a 2016 analysis of attack behaviors, the ten most popular networking and hacking reconnaissance tools are provided by Table 3. This report also notes that 99% of reconnaissance and lateral movement threats originated from legitimate applications or from riskware (software whose installation and execution poses a potential yet not definite risk to a host computer); only 1% originated from malware (Lightcyber, 2016).

Once the target system has been successfully penetrated, the cyber weapon will have to extend across the network to the vulnerable component. It will do so by using lateral movement applications. Lateral movement allows the attacker to maintain persistence in the network, gain control of the administrative privileges, and move to the key vulnerable components. The lateral movement characterization should include descriptions of its function and the operational environment in which it operates. The ten most popular administrative tools for lateral movement are provided by Table 4 (Lightcyber, 2016).

Table 3 Reconnaissance – Top Ten Networking and Hacking Tools

Tool Name	Function	Percentage of Top 10
Angry IP Scanner	IP address and port scanner	27.08%
PingInfoView	Program that pings multiple hosts at once	25.00%
Nmap	Network discovery and security auditing tool	14.58%
Ping	Ping command program	12.50%
Mimikatz	A tool that extracts plain text passwords stored in Windows	6.25%
NCrack	High-speed network authentication cracker	4.17%
Perl	Scripting tool that can be used to script hacking and reconnaissance tasks	4.17%
Windows Credential Editor	A tool that manages Windows logon sessions and credentials; can be used to perform "Pass-the-Hash" attacks	2.08%
SmartSniff	Network packet sniffer	2.08%
PDF Exploit Generator	An app that generates malicious PDF files that can infect vulnerable PDF applications	2.08%

In addition, remote desktop tools are used to move laterally within a network and to remotely control elements. Legitimate Information Technology administrators use them and cyber weapons can utilize them to control elements that have been compromised. The ten most popular remote desktop tools for lateral movement are provided by Table 5 (Lightcyber, 2016).

Table 4 Lateral Movement – Top Ten Administrative Tools

Tool Name	Function	Percentage of Top 10
SecureCRT	SecureShell (SSH) and Telnet client	28.48%
Putty	SSH and Telnet client	25.95%
BeyondExec Remote Service	Utility to spawn processes and shutdown remote workstations	10.13%
VMWare vSphere Client	Management utility for VMware vSphere Server Virtualization	8.86%
MobaXterm	Xserver and tabbed SSH client for Windows	8.23%
PsExec	Light-weight telnet replacement for executing processes on remote systems	8.23%
PowerShell	Task automation and configuration management framework	5.70%
Private Shell SSH	SSH client	1.90%
Telnet	Telnet client	1.90%
Xshell	Terminal emulator that supports SSH, SFTP, telnet, rlogin and serial access	0.63%

Table 5 Lateral Movement -- Top Ten Remote Desktop Tools

Tool Name	Function	Percentage of Top 10
TeamViewer	Cloud-based or locally hosted remote desktop and web conferencing software; can be used for command and control and lateral movement	37.22%
WinVNC	Remote desktop software using Virtual Network Computing (VNC) for remote access	27.44%
Radmin	Remote desktop and technical support software	9.09%
AnyDesk	Remote desktop software	6.86%
LogMeIn	Cloud-based remote access and remote desktop service	4.12%
NetOp Remote Control	Cloud-based or locally hosted secure remote access	2.92%
Ammyy Adminn	Free remote desktop and remote control software	1.72%
Citrix Client	Application used to access Citrix XenDesktop and XenApp programs	0.86%
Remote Desktop Connection	Microsoft’s native remote desktop solution	0.69%
UltraVNC	Remote desktop software that also includes file transfer and chat messaging	0.34%

In addition to the reconnaissance and lateral movement functions, a cyber weapon must deploy a payload. Payload refers to the component of a computer code that executes an activity that is unwanted by the targeted system. This does not include the reconnaissance and lateral movement code required to get the payload packet to its destination. Some example effects of payloads are data manipulation or destruction, interrupted or inconsistent messages, and the delivery of spam emails through an infected user's account. Payloads can be developed by black hat hackers and by government operatives.

The payload characterization should include descriptions of its function and the operational environment in which it operates. For example, the characterization should indicate that it exfiltrates data from computers that utilize the Windows 10 operating system.

Cyber Lethality/Effectiveness Estimate Generation

The lethality/effectiveness estimate is the point in the process where the analyst predicts component response to the weapon. Determining Probability of Kill (P_K) or another lethality metric is the final piece of the system effectiveness process. For a kinetic weapon system, P_K is often part of the system requirements. It is also used by logisticians to determine weapon load-out and by mission planners to develop tactics. Even though there are not production line or storage magazine concerns relating to cyber weapons, mission planners and combatant commanders will be critically concerned about the effectiveness of the weapon when it is deployed. Commanders must have confidence in weapons before using them. This is especially true when physical damage may not be evident as confirmation.

An effectiveness equation for a typical missile intercept event was illustrated in Figure 6. In that model it is clear that the majority of the uncertainty, and the associated probabilities, occur after the engagement begins. Similar kill chain models for cyber engagements have been developed by Lockheed Martin and Mandiant (now FireEye) for an advanced persistent threat (APT) attack. Figure 9 shows the similarities between these models (Holmes, 2015). In both of them there are distinct stages of the engagement. The duration of these stages are much longer than the stages of a kinetic engagement. In addition, the pre-compromise stage where reconnaissance occurs is actually prior to the engagement start; that is, prior to when the commander wants to engage the cyber weapon.

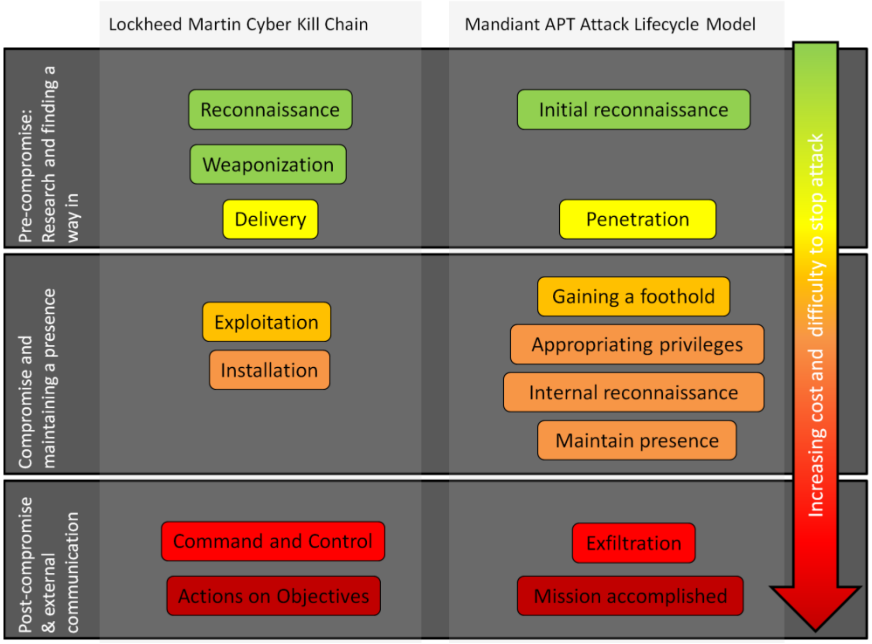

Figure 9 Cyber Kill Chain Models

Since these APT attack phases are well defined and understood by the cyber community, these have been selected to form the basis for an initial cyber effectiveness relationship. As in the case of the kinetic effectiveness equation, cyber effectiveness is calculated by multiplying the probability of various contributors. The most significant difference between the kinetic and the cyber effectiveness models is the cyber weapon payload probability of success can likely be considered equal to one. It has been tested and proven in a lab setting to perform the action necessary to achieve the desired kill effect. However, the other events leading up to the payload activation have differing uncertainties.

In order to add meaning to the kill chain, it is necessary to associate probabilities with each of these steps: Intelligence (Reconnaissance), Delivery, and Exploitation.

Thus, the cyber equivalent to the kinetic equation in Figure 6 can be shown as the following relationship:

$$P_k = f(P_{Intel} * P_{Deliv} * P_{Exploit}) \text{ where}$$

- P_{Intel} is dependent upon the probabilities of the knowledge of access points, hardware and software configurations, completeness of network map, understanding of operations tempo, and the latency (or timeliness) of information ($P_{Intel} = f(P_{Access} * P_{Config} * P_{Map} * P_{Tempo} * P_{Latent})$),
- P_{Deliv} is dependent upon the likelihood of a patch to address software vulnerabilities being implemented and IT's ability to detect and respond to the delivery ($P_{Deliv} = f(P_{Patch} * P_{IT})$), and
- $P_{Exploit}$ = is the likelihood that the payload will achieve the desired mission effects.

Note that P_{Deliv} is actually a product of the survival rule for P_{Patch} and P_{IT} because a poor response by the defending asset gives a greater likelihood of success by the attacker. Also, other factors may also be included in the P_{Intel} and P_{Deliv} terms. Some of these uncertainty factors include the likelihood of knowing the password or having the proper credentials, the chance that a hardware upgrade has occurred, the impact of network congestion on the timing of the attack, and even if the proper node has been targeted. A cyber reconnaissance tool may be required to ascertain all the appropriate factors and to quantify their impacts on the likelihood of success.

The reconnaissance tool may also be necessary to confirm that the correct element has been targeted. Figure 10 shows the resulting cyber effectiveness relationship for a path through an example network.

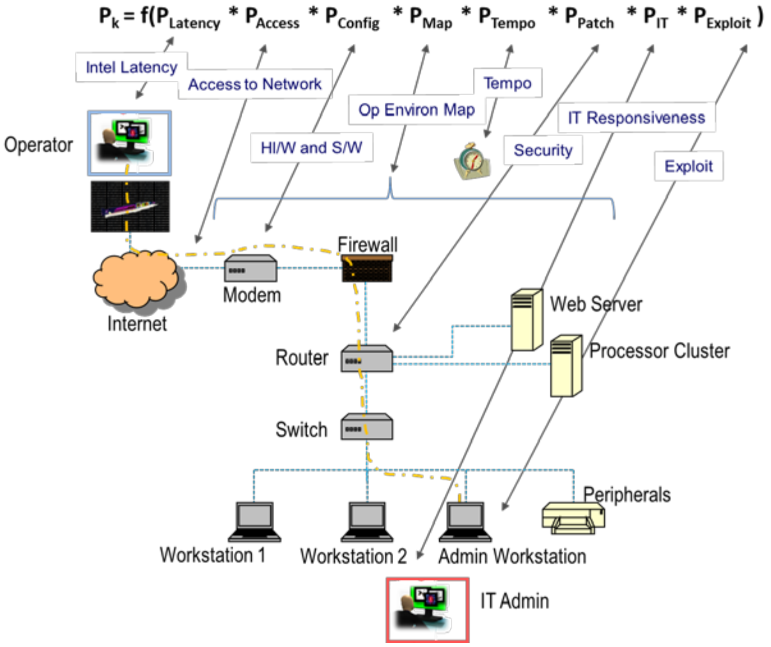

Figure 10 Cyber System Effectiveness Kill Chain

Upon completion of the cyber lethality/effectiveness evaluation, the information must be documented for the user. This is done by creating a Cyber JMEM for the product. Remember that the JMEM information includes damage/kill probabilities for specific weapons and threats, physical and functional characteristics of munitions and weapon systems, threat vulnerability, obscuration on weapon effectiveness, and analytical techniques and procedures for assessing munitions effectiveness. In the case of a Cyber JMEM, the weapon must be described in terms of an exploit – a means by which the attacker uses a vulnerability to cause damage to the target system. The Cyber JMEM will provide the commander with the necessary information to choose the most appropriate attack means to achieve his or her operational mission.

The commander makes this decision through the process outlined in Joint Publication 3-60, *Joint Targeting*. Targeting is a systematic process which enables the commander to analyze and prioritize targets and then match appropriate lethal and non-lethal actions to those targets to achieve specific desired effects. Targeting links the desired effects to actions and tasks (U.S. Department of Defense, 2013). The Joint Targeting process is illustrated in Figure 11.

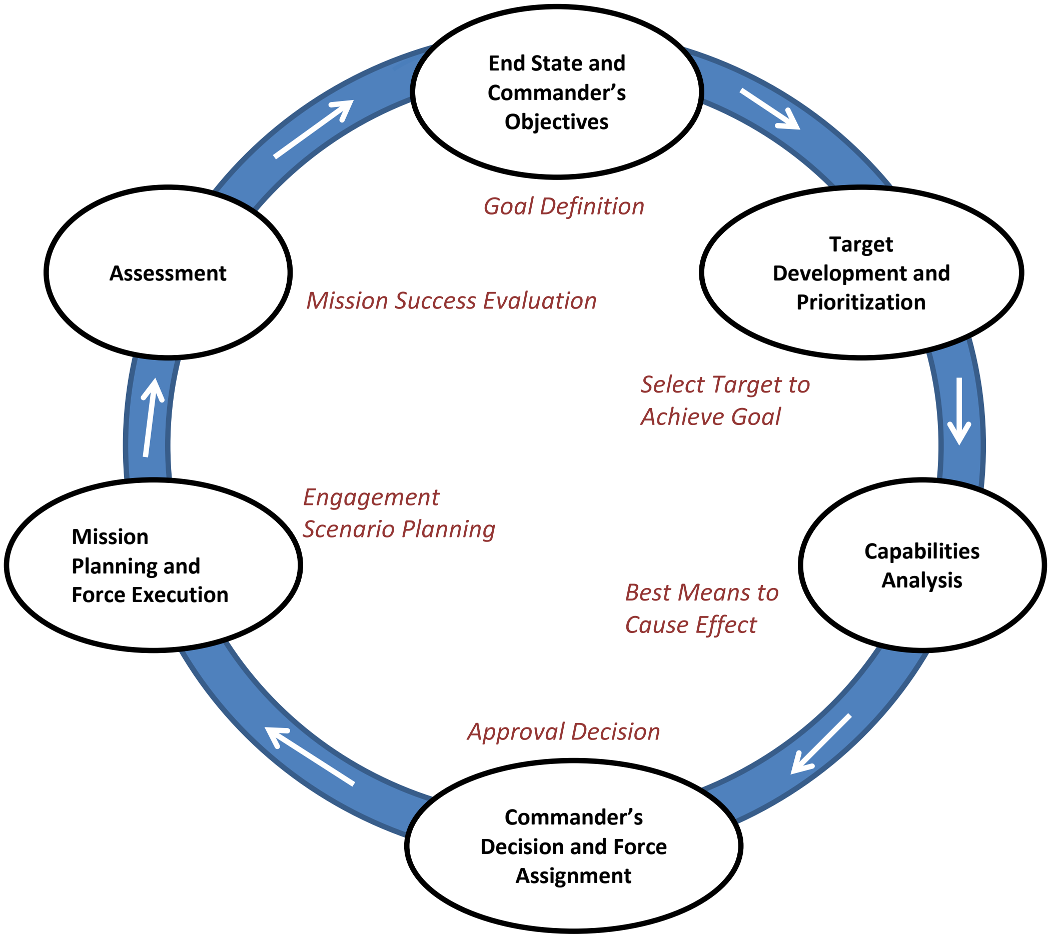
End State and Commander's Objectives
Goal Definition
Target Development and Prioritization
Select Target to Achieve Goal
Capabilities Analysis
Best Means to Cause Effect
Approval Decision
Commander's Decision and Force Assignment
Engagement Scenario Planning
Mission Planning and Force Execution
Assessment
Mission Success Evaluation

Figure 11 Joint Targeting Cycle

For engagements implemented with kinetic weapons, there is significant data and accredited models available to estimate system performance. Threat models, or approved surrogates, exist to allow for the selection and prioritization of targets. Performance models can readily predict performance of specific weapons against those targets. The results of these are summarized in JMEM documents. In order for cyber weapons to be considered as a viable capability, an equivalent level of maturity must be obtained. That is, target models must be created and verified, weapon characteristics must be standardized and thorough, and performance models must be developed and accredited so that the operational forces will trust the findings. The Cyber JMEM will encapsulate this information for the commander.

3.5 Follow-on Tasks and Research

The methodology proposed here is intended to support the tri-service cyber teams and mission planners. An operationally relevant cyberspace lethality and effectiveness tool is an unmet need of the cyber community. Ultimately, a fielded cyber JMEM tool that incorporates accredited cyberspace quantitative and qualitative models, effectiveness data on cyberspace delivered effects/associated risks, and potential collateral consequences of employing cyberspace effects mechanisms is desired. The proposed methodology is a first-cut attempt to conduct a cyberspace vulnerability characterization and a cyber weapon lethality assessment. But it cannot be implemented without additional work and without the cooperation of the other JTCG/ME and U.S. Cyber Command activities.

Aspects of this proposal were presented to the JTCG/ME through existing contacts via the NSWCDD Lethality and Effectiveness Branch. A JTCG/ME Joint Non-Kinetic Effects Configuration Control Board (CCB) exists to consider these types of issues. The methodology was discussed by the CCB and has formed the basis for future efforts.

The first task – create data standards for the target, weapon, and network models – has been initiated. With these, the practitioners at U.S. Cyber Command can be engaged to help finalize the standard formats and content for the cyber target vulnerability model and the cyber weapon characterization. The formats must be acceptable so that they become adopted across the community. The cyber target vulnerability model can, based upon experience, be modified to reflect changes to the cyber domain and the types and characteristics of potential targets. The cyber weapon characterization is critical information for the cyber JMEM product. Ongoing dialogue is necessary and expected to develop these formats. Cyber target and weapon data requirements will be gathered through discussions with various types of government and academic personnel including: basic research individuals, weapon system developers, analysts, system modelers, intelligence analysts, vulnerability experts, and weapon system program managers. The analysis must consider the scope, level, and duration necessary to construct target models and cyber payloads that encompass the physical, functional, or behavioral state changes typically associated with mission and damage criterion of the target. Standard business tools such as surveys and working groups will be used to develop a consensus. The products will be qualitative in nature since there is no numeric value that can be associated with a template.

Clearly, the effectiveness relationship for cyber operations also needs to be reviewed, critiqued, investigated, and improved. The initial proposal needs to be examined by the cyber professionals and they must be presented with the opportunity to refine the variables. Therefore, the second research task will determine the factors and numeric contributions of the cyber effectiveness kill chain factors. This will require the creation of test standards and the collection of appropriate data to build quantitative assessment values. Test and evaluation requirements will be gathered through discussions with government and academic personnel. The proposed cyber relationship will be presented to the cyber teams for their critique. Feedback will be used to modify the relationship with the intent to eventually formulate a cyber effectiveness equation. Most importantly, the terms and values associated with the relationship contributors will be adopted. Test data will then be gathered and analyzed to determine confidence values or bins. The goal is to create a standard by which required organizations can adequately and succinctly capture the performance of a cyberspace capability and its unique configuration against a target and its unique attributes.

It is the author's belief that value of the weaponization element of the effectiveness relationship ($P_{Exploit}$) should be one since testing can be concentrated and extensive. It is up to the test community to prove this to be true by demonstrating that tests and test reports cover all criteria. This will give the combatant commanders confidence that the cyber payload will achieve the desired mission effects. This will have the subsequent effect of increasing the commander's confidence that cyber is a viable option so that more than just kinetic weapons will be considered part of the available arsenal.

These research tasks have either begun or should be initiated this fall with the anticipated completion by the end of September, 2018. This will allow the DoD cyber community ample time to implement the standards in Fiscal Year 2019 and beyond.

A larger research area that is beyond the scope of this paper pertains to the effectiveness model for cyber operations in support of information operations information-related influence efforts. These are efforts that attempt to inform, influence, and persuade others to change their behavior or attitudes. They are often directed at the strategic level, but there are situations where they are necessary at the operational area. The effectiveness of cyber operations to influence the attitudes and behavior at hard-to-reach or challenging audiences needs to be researched. This type of assessment goes beyond altering computer commands and, thus, the value for $P_{Exploit}$ is likely to be less than one. A thoughtful evaluation of identifying objectives and measuring progress toward those objectives must be completed and the results folded back into the cyber effectiveness relationship.

While it is being completed and implemented, it will be important that NSWCDD and the other organizations that support the JTCG/ME develop a workforce that is suited to evaluating cyber weapons. It is recommended that knowledge, skills, and abilities criteria be established and the workforce be trained to achieve them. Existing commercially available training should be evaluated to determine its applicability. If it is found to be lacking, specialized training should be procured. It may be possible to coordinate with the other Services to create a schoolhouse for analysts and operators. Defining the necessary knowledge, skills, and abilities may be the subject of follow-on research.

CHAPTER 4

4. RESULTS

Progress has begun on the tasks outlined in this proposal but there is much more to accomplish. This will require continued collaboration between various activities.

4.1 Proposal Acceptance

As indicated, the proposal has been adopted by the JTCG/ME. The Joint Non-Kinetic Effects CCB has adopted the structure of this proposal as the basis for the cyber JMEM development effort. Tasks have been initiated to define data standards to define the weapon characterization, the target vulnerability characterization, and the operational environment characterization. These tasks are being led by different groups within the JTCG/ME. The products will be reviewed and, if satisfactory, adopted by the CCB.

The author, on behalf of the CCB, also presented the concept to the JTCG/ME Steering Committee in late spring, 2017. The Steering Committee reviews and approves task proposals on a fiscal year basis. The Steering Committee noted that there is much work to be done but agreed to the overall process. Some members of the Steering Committee, in particular, noted that this work must be done in a close relationship with the U.S. Cyber Command and its cyber mission teams.

The Steering Committee met again in early November to approve tasks for Fiscal Year 2018. Approval of the cyber tasks outlined by the Joint Non-Kinetic Effects CCB is considered to be confirmation of the soundness of the proposal by an independent body. On 26 October, the chair of the Steering Committee was briefed in advance of the meeting. She indicated that she understands the basis for the proposal and would like to be kept well-informed of the progress. The full Steering Committee subsequently approved the cyber tasks as proposed.

4.2 Engaging U.S. Cyber Command

In accordance with the consensus of the JTCG/ME Steering Committee, the first task of this proposal requires engagement and collaboration with U.S. Cyber Command. Initial efforts have begun to standardize the cyber lethality data standards. With funding in FY18, operational user group meetings will be conducted with participants from the cyber combat mission teams. These teams are being established to provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations (U.S. Department of Defense, 2017). Their purpose is to achieve military and security objectives with precision such that there is minimal loss of life and property.

Since not all commands will be able to attend simultaneously, multiple operational user group meetings will be held. They will be conducted at various commands to reduce the travel and time demands on the operators. The developers and operators will be surveyed to determine how they currently document weapon characteristics, targets, and the operational environment. The initial draft standards will be discussed and recommendations taken to improve them. Minutes will be taken and the results will be incorporated into later versions of the data standards.

Operational user groups will also be utilized to help determine cyber kill definitions. The cyber mission teams will each likely have a particular area of focus and expertise. So, in addition to achieving a consensus on the data standards, it will be important to understand the different kinds of effects they intend to implement. This will drive the cyber-specific kill effects and definitions.

Test results from the mission cyber teams and other activities will be evaluated to confirm the hypothesis that the probability that a particular cyber weapon works against a target is either one or zero. Other uncertainty metrics, however, will remain to be evaluated. The operational user groups will be used to determine the criteria that make up the P_{Intel}, P_{Deliv}, and $P_{Exploit}$ terms. The probabilities associated with each of these will likely be determined by the Intelligence Community.

This task will be considered successfully achieved if upgraded data standards are finalized by the end of September 2018, initial uncertainty metrics are compiled, and the test data confirms or refutes the hypothesis that a well-defined cyber weapon can be considered to have a probability of one against particular targets.

CHAPTER 5

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Summary

This dissertation describes the lethality prediction processes for kinetic and directed energy weapons and outlines the research necessary to develop a methodology to implement a cyber weapon lethality process. It is noted that cyber mechanisms can induce different kinds of effects and can be reversible. Cyber targets and environments are also likely to be more dynamic than traditional military targets. Therefore the existing kinetic processes must be tailored to account for the different timelines necessary to design and engage cyber targets. Since the armed forces understand and utilize the JTCG/ME process for kinetic weapons, the cyber methodology will mirror that process as applicable.

The current cyber JMEM development effort being undertaken by the JTCG/ME is utilizing this methodology. The concept was presented to the JTCG/ME Steering Committee in the late spring and the proposed tasks for Fiscal Year 2018 are meant to implement it. The Steering Committee met in early November and approved the cyber tasks for Fiscal Year 2018.

5.2 Recommendation

The cyber lethality methodology will be developed over the next several years. During that time, additional studies and efforts are recommended.

In order to ensure that all parties describe the weapons, targets, and networks consistently, the JTCG/ME must collaborate with U.S. Cyber Command, the cyber mission teams, and the cyber test community to confirm that the data standards are accurate and implementable. Likewise, to most efficiently develop the cyber effectiveness equation, the same collaborative effort must be utilized to review, critique, and refine the variables that will comprise it. User groups will allow all parties to provide their recommendations and explanations.

Kinetic weapons operate solely in the physical domain. As shown in Figure 1, cyberspace encompasses three layers: the physical network layer, the logical network layer, and the cyber-persona layer. An additional academic study may investigate the cyber lethality nuances associated with the various cyber layers. There may be different factors associated with each cyberspace layer. This study may provide insights into the fault trees associated with the layers and potential collateral effects. The temporal relationships of cyber-personas may also result in corrections or corollaries to the cyber lethality relationship equation.

Physics-based models exist that allow analysts to predict the performance of kinetic and directed energy weapons. The same spectrum of tools does not exist for cyber evaluations. An academic study of the available cyber ranges and tools would be beneficial to the community by recognizing the state-of-the-art methodologies and identifying gaps in the community’s simulation capabilities.

REFERENCES

Ambrose, S. (1999). *Duty, Honor, Country. A History of West Point.* Baltimore: Johns Hopkins University Press .

Beck, D., Kirillov, I., & Chase, P. (2014). *The MAEC Language Overview*. Mitre Corporation.

Clarke, R. A. (2010). *Cyber War.* New York: Harper Collins.

Collins, A. (n.d.). *MISCELLANY: Miscellaneous Technical Articles by Dr. A.R. Collins*. Retrieved December 22, 2016, from http://www.arc.id.au/RobinsOnBallistics.html

Connolly, J., Davidson, M., & Schmidt, C. (2014). *The Trusted Automated eXchange of Indicator Information.* Mitre Corporation.

Dahlgren, J. A. (1852). *A System of Boat Armament in the United States Navy* . Philadelphia: Hart.

Daniel, L. (2011, February 11). *Department of Defense News.* Retrieved February 20, 2017, from U.S. Department of Defense News: archive.defense.gov/news/newsarticle.aspx?id+62790

Driels, M. (n.d.). *History of the Joint Technical Coordinating Group for Munitions Effectiveness*. Retrieved December 19, 2016, from Weaponeering : Conventional Weapon Systems Effects: http://www.weaponeering.com/jtcg_me_history.htm

Driels, M. R. (2013). *Weaponeering.* Monterey, CA: American Institute of Aeronautics and Astronautics, Inc.

Frieden, D. R. (Ed.). (1985). *Principles of Naval Weapons Systems.* Annapolis: Naval Institute Press.

Hogan, M. (2000). *A Cross of Iron: Harry S. Truman and the Origins of the National Security State, 1945-1954.* Cambridge, United Kingdom: Cambridge University Press.

Holmes, S. (2015, January 29). *Kill Chain Models*. Retrieved February 20, 2017, from Kill Chain Models: https://www.lowmanio.co.uk/blog/entries/kill-chain-models/

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2014). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Lockheed Martin.

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press.

Lightcyber. (2016). *Cyber Weapons: 2016 Report.* Los Altos: Lightcyber.

Marks, J. (2017, February 09). *There's Cyberwar and Then There's the Big Legal Gray Area.* Retrieved February 10, 2017, from Nextgov: http://www.nextgov.com/cybersecurity/2017/02/theres-cyberwar-and-then-theres-big-legal-gray-area/135298/

Naef, W. E. (2011, February 13). *The Information Warfare Site*. Retrieved February 05, 2017, from The Information Warfare Site: http://www.iwar.org.uk/psyops/

Naval Surface Warfare Center Dahlgren Division. (2014, January 8). System Analysis Overview.

Paul, C., Yeats, J., Clarke, C. P., Matthews, M., & Skrabala, L. (2015). *Assessing and Evaluating DoD Inform, Influence, and Persuade Efforts: Handbook Practitioners.* Santa Monica, CA: RAND Corporation.

RAND Corporation. (2017). *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below.*

Rid, T. (2012, February). Cyber War Will Not Take Place. *The Journal of Strategic Studies, 35*(1), 5-32.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *RUSI Journal, 157*(February/March), 6-13.

Schmitt, M. N. (2013). *Tallin Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Shamah, D. (2012, June 06). Latest viruses could mean 'end of world as we know it,' says man who discovered Flame. *The Times of Israel*.

Sood, A. K., & Enbody, R. (2014, December 19). U.S. Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers. *Gerogetown Journal of Internationa Affairs*.

The American Heritage Dictionary, Second College Edition. (1982). Boston: Houghton Mifflin Company.

Tucker, P. (2017, March 03). *Pentagon Advisers Want Cyber 'Tiger Teams,' More Authorities for Cyber Command.* Retrieved March 03 2017, from Defense One: http://www.defenseone.com/technology/2017/03/pentagon-advisers-want-cyber-tiger-teams-more-authorities-cyber-command/135861/

U.S. Army Material Systems Analysis Activity. (2016, September 13). *Joint Technical Coordinating Group for Munitions Effectiveness Program Office*. Retrieved December 23, 2016, from https://web.amsaa.army.mil/JTCGMEOPO.html

U.S. Department of Defense. (2012). *Sustaining Global Leadership: Priorities for 21st Century Defense.*

U.S. Department of Defense. (2013). *Joint Publication (JP) 3-12 (R). Cyberspace Operations.*

U.S. Department of Defense. (2013, January 31). Joint Publication (JP) 3-60. *Joint Targeting*.

U.S. Department of Defense. (2015, February 15). Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*.

U.S. Department of Defense. (2017). *The Department of Defense Cyber Strategy*. Retrieved July 21, 2017, from https://www.defense.gov/news/special-reports/0415_cyber-strategy/

U.S. Navy. (2013). *U.S. Navy Information Dominance Roadmap 2013-2028.*

U.S. Navy. (n.d.). *NSWC Dahlgren Division*. Retrieved December 22, 2016, from http://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Dahlgren/

U.S. Navy. (n.d.). *United States Naval Academy*. Retrieved January 03, 2017, from A Brief History of USNA: https://www.usna.edu/USNAHistory/

U.S. Strategic Command. (2016, SeptembeR 30). *U.S. Cyber Command (USCYBERCOM).* Retrieved February 15, 2017, from U.S. Strategic Command: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/

United Press International. (2014, January 31). *Israel combats cyberattacks, 'biggest revolution in warfare'*. Retrieved January 5, 2017, from Home / Business News / Security Industry: http://www.upi.com/Business_News/Security-Industry/2014/01/31/Israel-combats-cyberattacks-biggest-revolution-in-warfare/UPI-24501391198261/?st_rec=35101391453421

War in the fifth domain. (2010, July 01). *The Economist*.

Wilson, C. (2015, June 04). *Cyber Weapons: 4 Defining Characteristics.* Retrieved February 09, 2017, from GCN: https://gcn.com/Articles/2015/06/04/Cyber-weapon.aspx?p=1

Zetter, K. (2014). *Countdown to Zero Day.* New York: Broadway Books.

Zook, J. (1977). *An Analytical Model of Kinetic Energy Projectile / Fragment Penetration.* Aberdeen: US Army Ballistic Research Laboratory.

Zurasky, M. W. (2015, August 10). Lethality and Effectiveness Branch Overview.

VITA

Mr. Matthew W. Zurasky is fulfilling the requirements for a Doctorate of Engineering from Old Dominion University in 2017. Mr. Zurasky currently serves on the staff of the Missile Systems Integration & Weapons Effectiveness Division at Naval Surface Warfare Center, Dahlgren Division (NSWCDD). In this position he leads a strategic initiative developing methodologies to perform cyber weapon target characterizations. Mr. Zurasky has over thirty-four years of systems engineering experience supporting Navy Research, Development, Test, and Evaluation (RDT&E) programs from exploratory development efforts to Production, Fielding/Deployment & Operational Support (PFDOS). He has successfully served as a branch head and project manager for a number of years with wide ranging technical expertise in electro-optics, Ballistic Missile Defense, systems safety, and, more recently, weapons effectiveness and target vulnerability. He also recently served as the acting head of the Combat Systems Cyber Engineering Branch. Mr. Zurasky graduated from Duke University School of Engineering in 1983 with a Bachelor of Science in Engineering (BSE) and earned a Master of Business Administration (MBA) from Averett University in 2002.