THE COLLEGE OF INTERNATIONAL SECURITY AFFAIRS

NATIONAL DEFENSE UNIVERSITY

Student Name: Major Matthew Nordmoe, Special Forces
Joint Special Operations Master of Arts Class of 2015

Thesis Title: The Ghost in the Machine: Defining Special Operations Forces in Cyberspace

Thesis Submitted in Partial Fulfillment of the
Master of Arts in Strategic Security Studies

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF THE NATIONAL DEFENSE UNIVERSITY, THE DEPARTMENT OF DEFENSE OR ANY OTHER GOVERNMENTAL ENTITY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

ABSTRACT

Today, our entire modern way of life, from communication to commerce to conflict, fundamentally depends on the Internet. Technological advances have profoundly impacted everyday life by introducing creative inventions that were once confined to the realm of science fiction and are now common use. The exponential growth of cyberspace has also changed the dynamics of the joint operating environment. The modern threat environment is a world that is less contained by boundaries and one that allows a shadow war, known as cyber warfare, to occur. Adversaries of the United States and allies are using the cyberspace domain as a platform for warfare where rule of law is abstract and limitations are mostly self-imposed. While there are technically no "rules of engagement" for cyberspace, the United States has self-imposed restrictions that make it more difficult to conduct discrete levels of cyber operations. This form of warfare is currently working for our adversaries because they don't limit themselves, much less allow someone else to limit them.

The *ARSOF Operating Concept* calls for the use of the cyber domain to facilitate surgical strikes and intelligence operations (Cleveland 2014, 27). Rapidly defining capabilities, methodologies, and authorities (without containing out-of-the-box thinking is a way to show what cyber warfare is. Another way to define cyber operations is by showing a reflection of current cyber operations, that is, by giving some empirical examples. These can be seen in the recent events in Crimea and the operationalization of the Stuxnet virus in Iran. Hybrid warfare is the use of political, economic, technological, and informational tools that together make up the phenomenon of social infrastructure. One particular element of this type of event – human political protest - is now known to be a very important component in what we are learning about hybrid warfare. This is supplemented by military means of a concealed character, including carrying out actions of informational conflict, combined arms tactics, cyber operations and the actions of Special Operations Forces. I intend to explain how SOF can employ technological advances in cyber tools and networked social media to coerce, disrupt, or deter adversaries. This information will be of particular use to the SOF community. In an increasingly globalized and interconnected world, Special Operations must recognize, learn, adapt, understand and examine new and innovative ways to modernize irregular warfare fighting capabilities.

LIST OF ACRONYMS AND ABBREVIATIONS

4GW	Fourth Generation Warfare
APT	Advanced Persistent Threats
ARSOF	Army Special Operations Forces
ASO	Advanced Special Operations
CC	Counter Cyber
CIPoE	Cyber Intelligence Preparation of the Environment
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CO	Cyberspace Operations
CW	Cyber Warfare
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DOD	Department of Defense
EW	Electronic Warfare
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IO	Information Operations
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
ISR	Intelligence Surveillance Reconnaissance
IW	Irregular Warfare
MDMP	Military Decision Making Process
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OCO	Offensive Cyberspace Operations
OPE	Operational Preparation of the Environment
SCADA	Supervisory Control and Data Acquisition
SE	Social Engineering
SECDEF	Secretary of Defense
SMT	Social Movement Theory
SR	Special Reconnaissance
TCP	Transport Control Protocols
UW	Unconventional Warfare

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

Almost everything that happens in the physical domain is paralleled in cyberspace. The introduction of the Advanced Research Projects Agency Network (ARPANET) in 1969 created the fifth domain, cyberspace (Kent, Froehlich, and Fritz E. Froehlich 1990). Cyberspace is an operational space defined by the use of electronics to communicate through interconnected communication systems. These systems reside simultaneously in both the physical and cyberspace domain. However, in order to enter cyberspace, we require the use of man-made technology to transmit digital information. Every day, corporations use cyberspace to facilitate global trade, exchange funds, and manage critical infrastructure. It is also the domain in which shadow wars are currently being waged. In an increasingly globalized and interconnected world, Special Operations must recognize, learn, adapt, understand and examine new and innovative ways to operationalize that which is available in cyberspace. The *ARSOF Operating Concept* calls for the use of the cyber domain to facilitate surgical strikes and intelligence operations (Cleveland 2014, 27). As this paper will highlight, cyberspace itself cannot be ignored, because if not used effectively it may be the difference between success and defeat.

A great deal of information on the employment of cyber operations and cyber warfare is not open source information. To promote discussion about the topic, this body of work will only deal with the unclassified and open source information.

Statement of Purpose and Scope

The purpose of this research is to define Special Operations Forces role in cyberspace. Cyberspace is a borderless domain used by our adversaries. We must dramatically improve our understanding of the technology, law and capabilities, so that SOF can factor cyberspace into full spectrum operations. Specifically, this thesis will demonstrate how discrete cyber warfare capabilities are a viable option for use during a Title 10 U.S.C. unconventional warfare (UW) campaign. Initial research indicates that there is a clear misunderstanding of how to leverage cyberspace in support of unconventional warfare. This misunderstanding has resulted in restrictive guidelines, and misapplication of cyber capabilities. There is an echoing demand to establish and promulgate cyber rules of the road for SOF, backed by a foundational knowledge instilled within senior leaders and Judge Advocate Generals (JAG). United States Special Operations Forces (SOF) can accomplish UW tasks in the cyberspace domain from thousand of miles away, yet there is a debate—should SOF be operationalizing cyberspace? This thesis will dissect the Title 10 and Title 50 authorities for UW in Cyberspace; define SOF in cyberspace by providing a theoretical picture of SOF using cyberspace capabilities.

Research Question

This thesis intends to answer the following research question: *How can Special Operations Forces (SOF) employ technological advances in cyber tools and networked social media to coerce, disrupt, or deter adversaries, thereby defining their role in cyberspace?* To answer this question, this thesis will first demonstrate how SOF can justify their role in cyberspace by differentiating between Title 10 and Title 50 operations in support of Unconventional Warfare (UW). Secondly, this work will examine the current use of cyberspace by our adversaries through two case studies. Lastly, further to refine the mosaic of SOF's role in cyberspace, this thesis will create a step-by-step tutorial in the framework of the applying cyberspace towards an UW campaign. This thesis focuses specifically on cyber attacks as an element of warfare.

Background

Terrorist organizations, state actors, and international extremist use the Internet as a tool for radicalization and recruitment, a means of communication, and as a weapon to disrupt critical infrastructure. While there are no known report incidents of cyber attacks against U.S. critical infrastructure, there are cases of strategic and tactical cyber attacks abroad in pursuit of a political agenda. Terrorist organizations such as Al-Qaeda and regional insurgencies such as Islamic State in Iraq and Syria (ISIS) make use of the Internet in a variety of ways. Terrorist ideological material is often circulated through jihadist websites, forums, chat rooms, and blogs to inspire individuals to fight jihad against non-Muslims who oppose Islamic religious law.[1] Radical Islamist use dedicated servers and websites, and social networking tools as propaganda machines, and as a means for significant fund-raising (Theohary and others 2011, 5). YouTube channels and

[1] The Arabic word jihad is derived from a verb that means, "to struggle, strive, or exert oneself." Historically, key Sunni and Shia religious texts most often referred to jihad in terms of religiously approved fighting on behalf of Islam and Muslims. Some Muslims have emphasized nonviolent social and personal means of jihad or have sought to shape the modern meaning of the term to refer to fighting only under defensive circumstances. This report uses the term "jihad" to denote violent Sunni Islamists' understanding of the concept as a religious call to arms and uses the terms "jihadi" and "jihadist" to refer to groups and individuals whose statements indicate that they share such an understanding of jihad and who advocate or use violence against the United States or in support of transnational Islamist agendas. Alternative terms include "violent Islamist" or "militant Islamist."

social media are used to radicalize Western-based sympathizers, and also act as a means for communication between members of a decentralized terrorist network. There is particular evidence in the Ukraine that state actors have used the Internet as a weapon against critical infrastructure by taking down the communication networks prior to physical attacks. Recent developments have demonstrated the rise in our technical acumen of our adversaries' use of cyberspace in support of warfare in cyberspace. The emergence of virtual currencies such as Bitcoin, further promote a novel way discretely to procure and transfer funds for terrorists. As ingenuity and resources become even more readily available, Bitcoin mining will create an untraceable method for obtaining funds. Cyberspace, whether used by Al-Qaeda or ISIS is being operationalized in new ways against the United States.

In 2005 the Emir of Al-Qaeda, Ayman al-Zawahiri wrote, "We are in a battle, and more than half of this battle is taking place in the battlefield of the media" (Theohary and others 2011, 6), indicates how early in the Global War On Terror (GWOT) that terrorists desired to exploit the Internet. Highlighting this fact is a common quote found on ISIS affiliate's Twitter page stating, "50% of Jihad is 'media.' To support this statement, an international architecture of dedicated servers was developed to support terrorist websites, such as *Inspire,* that produces strategic narratives for the global jihad. Further codifying this narrative is the recent torture and burning of the Jordanian Pilot Moath al-Kasasbeh is an example of how the Internet is exploited to spread propaganda for jihadist. Jihadist websites are also used to convey step-by-step instructions about how to "build and detonate weapons, including cyber weapons" (Theohary and others 2011, 7). As mentioned in the 2011 Congressional Report, jihadist websites are now being used to recruit cyber talent and coordinate cyber attacks (Theohary and others 2011, 2). With the rapid emergence of mobile handheld devices and tablets, desktop computers are no longer the medium of choice against which cyber threats are exercised.

As Admiral Michael Rogers, director of the NSA explained to an audience at the University of North Carolina, "US Central Command was not hacked" (Rogers 2015). The social media accounts that reside on civilian networks were hacked not the ". mil" domain, but it was the perception. Nonetheless, terrorists do have an unsophisticated capability to conduct low-level attacks. The recent emergence of "The ISIS Cyber Caliphate" introduced the hacker-for-hire concept to the repertoire of terrorist organizations. In lieu of creating the capability, terrorist organizations recruited a network of hackers to conduct large-scale DDOS attacks. Recent intelligence reports identified a computer worm in government networks that was linked to a Libyan Hacker known as the "Iraq Resistance" and belonged to the hacker group "Brigades of Tariq ibn Ziyad" (Theohary and others 2011, 9).[2] Primarily terrorists use Twitter and Facebook to expand their global outreach and exchange real-time information, and recruit. Their ability to imbed malicious codes into devices and hack government systems is limited. One must differentiate between the terrorist *modus operandi* and large nation states that boast a sizeable offensive cyber capability.

Cyber power is especially attractive to large nation state actors, primarily because of its low relative cost, high potential impact and the general lack of transparency that surrounds it (Feakin 2013, 73). State actors like Iran, China and Russia are known to have a formidable cyber capability. Their units avowal the capability to infiltrate U.S.

[2] The worm's code had a digital fingerprint that identified the owner. This trademark is discussed as part of the motivations and characteristics of cyber personas.

computer systems that control the electrical grid, nuclear power plants, air traffic control, and subway systems (“The Future Economic War” 2015). Russia routinely employs its cyber prowess by disrupting Internet connectivity in Estonia and Georgia. Recently, Russia has flexed its cyber muscle by using cyber attacks as part of a hybrid warfare strategy in the Ukraine. Estimating the size of the cyber units of these countries isn’t the key to success. Numbers of personnel measure strength in the physical realm; however in the logic of cyberspace, capabilities define the threat.

The leaders of Tunisia and Egypt resigned after mass anti-government uprisings in 2011 known as the Arab Spring. The demonstrations that occurred were employed in some part by the emergence of online social media campaigns through Twitter and Facebook. As discussed below, the protests that occurred in Tahrir Square were synchronized through elaborate social networks, made accessible by the wide use of mobile phones and the Internet. For the purpose of this section I will establish how cyberspace is used for conducting Information Warfare (IW) and Unconventional Warfare (UW), which will be explored in greater depth in the case studies. When addressing the application of IW in cyberspace, the case studies of the Arab Spring highlight three “functional areas” for social media. These areas are psychological operations, network-centric warfare, and command and control warfare (Niekerk, Pillay, and Maharaj 2011, 2). On February 5, 2015 The Global Cities Conference hosted a lecture by Nezar AlSayyad from University of California at Berkeley to discuss the phenomena of virtual uprisings in Tahrir Square during the Arab Spring. Tahrir Square, in downtown Cairo, was the epicenter of antigovernment protests that led to the removal of President Hosni Mubarak. Both political and social activists used the Internet to further their objectives of political change.

Nezar explained how social media through websites such as Facebook and Twitter mobilized the masses in cyberspace, creating a new way for media to interact with individuals. Nezar highlights that “Tahrir square started in cyberspace and finished with blood on the streets—this is the future of conflict” (AlSayyad 2015). *#January 25* mobilized millions of Egyptians and propelled the decision to oust President Hosni Mubarak, who ran the regime for over thirty years. Over a span of eighteen days, from the 25th of January to the 11th of February 2011, Tahrir square became residence to upwards of two million Egyptians focused on the removal of Hosni Mubarak. Protestors used January 25, the national holiday Police Day, as the calling for an end to corruption, injustice, and poor economic conditions. This day was used to symbolize the beating of a 27-year old man, Khaled Mohamed Saeed who was viciously attacked by Egyptian police outside of a Cyber Café in Cairo. Once his post-mortem photos were leaked, Google marketing executive Wael Ghonim created a Facebook page, *We are all Khaled Said,* in his remembrance, sparking outrage and mobilization. This page became the hub for reporting humanitarian crimes and turned everyday Egyptians into citizen journalists.

This quick synopsis of Tahrir square indicates how the Internet affected the will and perception of the Egyptian and international community—it transformed Mubarak’s removal into a moral necessity, effectively removing any possible objections. This was an elaborate psychological operation, planned and executed by a social movement. By creating a virtual uprising behind the façade of humanitarian rights, a cohesive fighting force was developed to maximize effective power against the Mubarak regime. Social media, in particular, facilitated communications and provided a degree of command and control for the protestors, therefore forming a pillar of network-centric warfare (the ability to communicate in sync) (Niekerk, Pillay, and Maharaj 2011, 8). The efficacy of command and control during the uprisings in Tunisia and Egypt is a result of mobile phones and online social networks used to orchestrate anti-government protests. Social media was not only able to communicate to millions of people, but it was also used as a tool for broadcasting the authoritarian police response. This is the first occurrence of a crowd sourced command and control system, commonly referred to in the Army as the FBCB2[3].

Key Concepts

This section will define the key concepts and terminology that are built upon for the remainder of this thesis. It is imperative that we define each domain, look at key factors of the domain, and the influence on defining SOF in cyberspace. It is important to differentiate between academic and the military terminology when discussing these concepts. For the purpose of this research, the DoD definitions will be applied versus other widely used definitions from industry. The areas discussed consist of cyber warfare, unconventional warfare (UW), and Information Operations (IO) along with any key concepts that apply to cyberspace.

Cyber Warfare

[3] Force XXI Battle Command Brigade and Below is an applique that provide situational awareness and command and control to the lowest tactical echelons.

As cyberspace emerged as an operational domain, it is important that a common framework of terminology be established prior to any further analysis. As mentioned by Major Robert Trent, "cyberspace has gained traction as the catchphrase for anything having to do with the internet, especially as it has fostered the growth of technology for the military" (Trent 2014, 2). Cyberspace is defined by the Department of Defense as: “A global domain consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Department of Defense 2013). Conversely, the DoD has yet to define the most essential term, *cyber warfare*. In the absence of DoD terminology we are going to use Adam Liff’s version:

> A state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of CNA against an adversary’s critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military of civilian networks in order to reduce the adversary’s ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes .

The difficulty in defining *cyber warfare* is that experts like Thomas Rid believe that in order to be considered warfare it must include violence and the destruction of physical objects according to Carl von Clausewitz’s definition of warfare. To date there has been only one documented cases of this occurring—Stuxnet. There is an emerging definition that is being discussed by policy makers that would broaden the term cyber warfare beyond cyber attacks with physical damage. As tentatively defined by the CRS Report R43848, cyber warfare is “the exfiltration or corruption of data, the disruption of services, and/or manipulation of victims through distraction” (Theohary and Harrington

2015, 5). The following is a summary of concepts and terms that will be further discussed.

Computer Network Attacks (CNA) are a category of fires employed for offensive purposes in which actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate or destroy information resident in these networks (Cartwright 2011, 3). This definition differs from Computer Network Exploitation (CNE), which is an enabling operation and intelligence collection capability conducted through the use of computer networks to gather data about a target or adversary *automated information systems* (Cartwright 2011, 5). The distinction between these two is the desired effects. A cyber attack is considered any hostile act using computers with the intention to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions (Cartwright 2011, 5). Cyber Operational Preparation of the Environment (C-OPE) are non intelligence enabling functions within cyberspace conducted to plan and prepare for follow-on military operations (Cartwright 2011, 6). Offensive Cyberspace Operations (OCO) are undertakings through the use of cyberspace, actively to gather information from computers, information systems, or networks, or manipulate, disrupt, deny, degrade, or destroy targeted systems (Cartwright 2011, 13). These terms will be used throughout, and it is important to understand the difference between them.

Unconventional Warfare

FM 3-05 Army Special Operations Forces Unconventional Warfare (U) provides the current definition of UW as follows:

> Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla

> force in a denied area (JP 1-02 Department of Defense Dictionary of Military and Associated Terms 2014, 252).

As further highlighted in FM 3-05, there are two essential criterion for UW. It must be conducted by, with, or through surrogates and such surrogates must be irregular forces. UW is a subset of Irregular Warfare (IW) which is defined as violent struggle among state and non-state actors for legitimacy and influence over the relevant populations (JP 1-02 Department of Defense Dictionary of Military and Associated Terms 2014, 126). Irregular warfare favors indirect and asymmetric approaches, though it can employ capabilities to erode an adversary's power, influence, and will. It is also important to distinguish the difference between clandestine and covert operations. Clandestine Operations are: "Operations sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment" (JP 1-02 Department of Defense Dictionary of Military and Associated Terms 2014, 33). Covert operations are defined as: "An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor" (JP 1-02 Department of Defense Dictionary of Military and Associated Terms 2014, 56). Covert actions are activities conducted within the authorities of Title 50 to pursue objectives by conducting secret activities for a desired outcome. Typically, covert actions reside within the intelligence community, specifically the CIA, since the United States House Permanent Select Committee on Intelligence has jurisdiction over Title 50 organizations. For the purpose of this research, we are concerned with Title 10, clandestine operations only.

Army FM 3-05 describes a U.S. sponsored UW operation in seven phases: preparation, initial contact, infiltration, organization, buildup, employment, and transition. These phases may occur in sequence, in parallel, or not at all. However, each phase has unique characteristics and tasks to be addressed. During Phase I, Special Operations Forces conduct assessments of the target populations and regions to determine resistance potential, and irregular forces capabilities (United States Army John F. Kennedy Special Warfare Center and School 2008, 4–5). This phase consists of intelligence preparation of the operational environment (IPOE), planning and shaping activities. Phase II is arguably the most dangerous and difficult phase of UW. Special Operations Forces Pilot Teams infiltrate the Joint Special Operations Area to make initial contact with an indigenous element. Phase III Infiltration involves the link up with the follow-on personnel from the SFODA with the pilot team and irregular forces. Phase IV Organization SFODAs organize and develop irregular forces, as well as establish rapport with the local leadership by demonstrating an understanding of their capabilities and limitations. During this phase insurgent groups are divided into three components: Auxiliary, Guerilla, and Underground elements. Phase V Buildup involves the expanding of the irregular elements and their capabilities to meet mission objectives. Phase VI Employment, insurgent combat operations increase against occupying forces. The use of conventional forces may be introduced and subsequently transitioned to conventional warfare. During Phase VII Transition, hostilities cease and the new government is re-established, the insurgents are disbanded and transitioned into a legitimate security force or civilian status. (United States Army John F. Kennedy Special Warfare Center and School 2008, 4–6 – 4–10).

Thesis Structure

The remainder of this thesis is organized into five chapters, besides the Introduction and Conclusion. Chapter 2 of the thesis provides insight to help explain the relevance of cyberspace to the physical, virtual and human domains. Chapter 3 provides a dissection of Title 10 and Title 50, followed by a discussion about how SOF can differentiate between the two lexicons as justification for UW operations in cyber space. A Title 10 authority refers to the operations conducted by the Department of Defense (DoD). Title 50 authorities refer to operations conducted solely by the intelligence community and covert actions. Chapter 4 demonstrates how adversaries and allies have used cyberspace to achieve desired effects. This is accomplished through a case study of the Stuxnet Virus and Russian use of hybrid warfare in Ukraine—two distinctively different operations. Chapter 5 of this thesis pulls all this information together and creates a theoretical framework for how cyberspace can by employed by SOF, thereby defining *The Ghost In the Machine* based on the legal limitations and technological constraints.

CHAPTER TWO

CYBER SIGNIFICANE TO UNCONVENTONAL WARFARE (UW)

Cyber's Effect on the Physical Environment

How *virtual* cyberspace exists within the *physical* environment is a question that creates confusion. Military planners in the COCOMs and USSOCOM have a seminal opportunity to draw a corollary between how terrain analysis relates to cyberspace. The Department of Defense (DoD) has defined cyberspace but failed to define the terrain, within which it operates. Terrain is often thought of as a terrain feature or location that is on a map. In cyberspace terrain manifests itself over multiple layers and is more logical than physical. The 2014 NATO Cyber Conference on Cyber Conflict defines cyber terrain as "the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace" (Conti et al. 2014, 287–289) This definition codifies Cyber terrain analysis seamlessly. Military strategists analyze terrain for advantages in both offensive and defensive operations. This is done by analyzing the following: Observation and Fields of Fire, Avenues of Approach, Key Terrain, Obstacles, Cover and Concealment (OAKOC). This same method can be used in the cyberspace domain; however, the terrain is not tied to specific geographic location.

The virtual composition of cyberspace makes it impossible to correlate cyber terrain with a physical location. Physical location is still relevant when discussing attacking physical hardware devices that reside in the physical domain (i.e. an internet café in Raqqah, Syria frequented by enemies is key due to its location in a hotspot). An example of a cyber terrain feature discussed during the 2014 CYCON was a physical router that connected a network to an Internet service provider (ISP). The router resided at a specific physical location; it was not the physical location that made it key terrain, but the logical location of the device in the network (Conti et al. 2014, 288). Within the cyber domain, terrain can be altered, dynamically created, or destroyed with a keystroke. However, it is difficult to detect who has leverage since networks can be compromised from thousands of miles away.

Understanding Cyber Terrain

Observations and fields of fire refer to the ability to see and engage enemy forces from a particular vantage point. Reconnaissance techniques that use commercial services such as *whois* and *whatsmyIP* can locate contact information for domain administrators, DNS Server addresses and IP addresses. Scanning a target network identifies what hosts, ports and network services are accessible from your vantage point. Other tools like *nmap* can be used to determine the operating system that is running on a particular device along with different types of software running on the system. Tools like these assist in determining which cyber weapons (fields of fire) might be successful.

Key Terrain is anything that gives an advantage to an attacker or defender. The U.S. Army defines key terrain as “any locality or area, the seizure or retention of which affords a marked advantage to either combatant.” Key terrain is represented on maps with a purple star and its very occupation lends an advantage. However, in cyberspace, adversaries may compromise and control networks without anyone knowing. Key terrain is equally as important in the cyber domain as the physical domain; it is temporal and in some instances, hardware may be considered key terrain. Key terrain is either logical or physical. If a person's adversary has a single router connecting him to a specific network and the person's end state is to deny his adversary access to the network, the router would be considered key terrain (Conti et al. 2014, 288).

Obstacles in cyberspace are those technologies that limit freedom of movement within a network. Obstacles can be either natural ridgelines or manmade minefields; in the cyberspace bandwidth constraints are natural obstacles and firewalls are man made (Conti et al. 2014, 293). Obstacles sometimes put target systems out of range of an attacker. Examples of these include router-based access control lists, air gaps and devices that monitor and control the flow of network traffic.

Cover and Concealment protect from observation and enemy fire. Cover in cyberspace is provided by firewalls, which prevents malicious traffic from reaching systems and protects from observation. An intrusion prevention and detection system (IPDS) can be used to place hosts out of range of an attack by monitoring network activities for malicious activity and actively blocking intrusions that are detected.

Avenues of approach in cyberspace are the pathways to reach a network. This is comprised of physical hardware such as switches, routers, and Ethernet cables. Additionally, there are Internet connections to these devices, which is the logical pathway for the virtual Internet.

Human Hacking

The cyber persona layer of cyber space discussed in Joint Publication 2013 is the layer at which social engineering is exercised to gain access to otherwise impenetrable electronic systems. Our personal hygiene in cyberspace is our weakest link, according to

Admiral Rogers, Director of the National Security Agency (NSA) and Cyber Command (Rogers 2015). At a recent speech at the University of North Carolina, the Admiral asserts that the greatest challenge to cyberspace is the choices we make everyday: the emails we open, the attachments we click and the data we download (Rogers 2015). Cyber defense is strong, but the exploitation of the human interaction that targets your pattern of behavior is even more formidable (Hadnagy 2015). Chris Hadnagy, as one of the industry's most prestigious and recognized developers, defines social engineering as any act that influences a person to take an action that may or may not be in his best interest (Hadnagy 2015). Social engineering is a blend of science, psychology, and art used to gain access to systems by manipulating the weakest security link-- the human mind. There is little difference between the security professionals who believe their system is impenetrable and the everyday person with a security system; they have a false sense of *safety*. Both of these systems, regardless of virtual intrusion detection systems (IDS)--physical steel doors-- can be penetrated through human interaction. Hackers are akin to psychiatrists in that they manipulate their patients or targets to take actions through a series of questions, neurolinguistic programming or pretexting. Social engineering takes this one step further when applied to Special Operations by targeting the personality, physical, and technical characteristics of the cyber persona layer.

The most effective cyber attack has not been against the computer networks, but has been against the minds of the humans that use the computer systems. This method is focused on influencing a person's thoughts and actions after receiving information, instead of physically attacking the communications infrastructure or launching malicious code (Parker 2004, 222). The cyber persona layer cannot be ignored when creating a framework for Special Operations Forces in cyberspace in support of hybrid warfare. By understanding the SE framework, it will become apparent how important SE is in developing the capability of the ghost in the machine (SOF in Cyberspace). The *virtual* environment connects with the *physical* environment by human interaction. The social engineering framework allows SOF to gain access into systems, and further improve information awareness (IA). The human mind is similar to software and should be treated similarly. SE can be used to overflow the human mind and inject any command, a process exactly like overflowing software to run unauthorized code.

Social engineering can be as simple as *guessing* someone's password from his biographical data. Often people (including some of the leading security experts), use the same password for their personal e-mail, social media, and access into confidential databases. Another trend that is exploitable is users often like to use the same username across multiple platforms. A person is likely to use that username for Twitter, Facebook, Gmail, etc. A website called *namechk* can research a username across several applications for that same username. Password profilers such as Common User Passwords Profiler (CUPP) and Who's Your Daddy (WYD) can assist a SE of the potential passwords that may be in use. Something as ordinary as a child's birthdate, spouses name or anniversary can be used to get access to the desired information. Gaining access to this information takes only a few key logs and Google searches until you have enough information to begin. For SOF's use of social engineering, our targets will not be as recognizable or accessible; therefore a more aggressive approach is mandatory. This is where the beauty lies within social engineering—it incorporates technology into the process to manipulate the target. The equation for social engineering is "pretexting + manipulation + attachment [to something] = target being socially engineered" (Hadnagy and Wilson 2010, 19).

Just like any military operation, social engineering begins with *information gathering*. Gaining access into state and non-state systems, such as the Iranian Nuclear program or ISIS IRC will likely not offer direct avenues of approach. Gaining access into these systems will rely upon a tiered effort with multiple efforts. All you need is a morsel of information to begin; for instance an e-mail address or cell phone number. This information can be obtained from personal websites, social media, blogs, and *Google Dorking*. *Google Dorking* is a technique that acts like a sniper rifle for information. This allows SE to the Internet for servers, routers, specific software, and malicious traces of information. As mentioned by Hadnagy, "Google forgives but never forgets [information]" (Hadnagy and Wilson 2010, 34).

From there, you begin to peel back the layers of information set 'A' to determine what is connected to information set 'B'. There are multiple tools available to harvest information; two of which I have used are *Maltego* and *Kali-Linux*. These systems connect all known relationships between social media, e-mail addresses, and phone numbers. Furthermore, the programs correlate and prioritize the relationships. For instance, an e-mail address is used to communicate with or logon a computer that shares the personal e-mail address of an individual. Once you have the linking adjacent piece of information you can begin to exploit information about "*Mr. Y*." As an example, social engineering would determine that one of those e-mail addresses is used to access a jihadist forum used to communicate with terrorists. Once the forum is identified, a SE with a .PDF document with malicious code can submit a forum post in order to gain unrestricted access for anyone who clicks on the link. Information is vital and the building block for SE.

Not all-SE information is attainable on-line. Social engineering also harvests information through direct communication. Direct communication is both verbal and non-verbal, comprised of the sender, receiver and message. For the purpose of this analysis, we care only about addressing the message for social engineering. The message in essence is comprised of the words contained within an e-mail or social media post. When they receive the message, they decode the message. Decoding the message is dependent upon their mode and environmental conditions. SE attempts to alter how the target perceives the message in order to behave in a manner the SE desires. The goal is to alter the target's perception through the use of nonverbal and verbal cues—altering the target's behavior (Hadnagy and Wilson 2010, 56). This is done in cyberspace by developing phishing attacks against individuals using e-mail as a channel of communication. An example of SE using phishing as a way to gain access to system is by embedding executable code into message forum or executable document. Alternatively e-mail could be generated that requests a user to 'login,' redirecting him to non-existent webpage while loading malicious code. Information about the target in this scenario is the lynchpin for success. Understanding your target's vulnerabilities increases the probability of his being socially engineered.

The next step in social engineering is *elicitation*. This is the ability to draw someone out of his or her normal comfort area and coerce him into behaving differently. Elicitation is defined as "stimulation that calls up (or draws forth) a particular class of [unwanted] behaviors. Eliciting information means you can fashion questions that draw people out and stimulate them to take to take the paths of behavior you want them to take. Elicitation is the subtle extraction of information that is low risk and difficult to detect. Furthermore, humans are wired to behave within social norms. When asked a question they want to respond in a way that shows that they are knowing and intelligent. We are also inherently social and want to divulge information when praised and challenged. By gaining rapport with targets, you lower the barrier; you overcome their hesitation to answer your questions, while simultaneously extracting valuable information. Becoming a master of successful elicitation requires human capital investment. Social engineering emphasizes the importance of planting ideas or thoughts in a way that is not obvious or overbearing in order to sensitize the targets to elicitation. Preloading involves understanding your elicitation goal before you even start elicitation. It encompasses personal emotions and gives a person no reason to doubt you when asked for something you preloaded into their behavior.

In order to socially engineer a target requires pretexting. Pretexting is your fictitious persona; it is defined as the act of creating an invented scenario to persuade a targeted victim to release information or perform some action. In essence it is the background story. Pretexting for SOF can be pictured as your online identity. Pretexting creates the conditions that allow their targets to divulge information they normally wouldn’t. Social media is the perfect medium in which this can be accomplished. Pretexting requires a vast amount of information about the target and the image you are conveying to the target. A pretext feeds on the emotions of an individual target. Successful pretexting further relies upon understanding the sub-modalities of your target. In other words, what senses generate the most significant response from a target?

Pavlov's research with dogs highlights the importance of programming your target. Understanding your target will further allow you to use Neuro Linguistic Programming (NLP) to push him over the edge. NLP is how we embed commands to influence a target to think a certain way or take a certain action. People are often more responsive to how things are said versus what is said. The same goes for on-line dialogue. By placing emphasis on certain words and word structure, your message appeals to a specific mindset that decodes the message in a scientific way. Within the framework of Unconventional Warfare, this technique can be used to target adversaries, manipulate existent forces, or coerce resistance forces.

Science is characterized by the scientific method. Social engineering uses elements of science and art to produce a desired outcome. This outcome is the ability to persuade and influence human actions or beliefs. Persuasion is coercing someone to *want* to perform an action we *want* him or her to perform. In the context of Unconventional Warfare, SOF can incorporate the science of social engineering by dismantling the resistance of adversary sympathizers, creating discontent amongst a group, or targeting adversary cyber personalities. Influencing and persuading someone should be imperceptible—it is the Mad Men approach to marketing. Something as simple as a billboard or the annoying banner advertisements in a webpage are examples of this in everyday life.

Persuading someone is *not* just building rapport. It is influencing a person to take an action that is out of his best interest. The power of persuasion can be exercised by employing five steps over a period of time. The first of these steps is setting a goal for each message or engagement (Hadnagy and Wilson 2010, 182). By setting a goal, you are creating a roadmap to get to your final destination of *persuasion.* Each engagement is a micro increment closer to persuasion and relies on NLP. The next step is building rapport with someone. This is not the TRADOC version. This requires getting into the mental frame of your target. This requires understanding a person's environment, emotional baggage, and thought process. We must align our influence with the target's logic and frame of mind. In the AMC hit show Breaking Bad, Walter White convinces his partner, Jesse, to kill a rival drug manufacturer by influencing Jesse's environment. Walter White convinced Jesse, that the rival had almost killed the 12-year-old son of Jesse's girlfriend. Without understanding Jesse's mindset, Walter would not have been able to persuade Jesse.

Having a firm understanding of yourself and your surroundings is the next step, and is self-evident. The final step of persuasion is being flexible. An effort to persuade may not go as planned, and may require a shift in strategy. Because a goal for the engagement was developed, it does not mean it will be obtained by a pre-planned strategy. All of these steps require an understanding of Neuro Linguistic Programming (NLP). NLP as discussed by Hadnagy "studies the structure of how humans think and experience the world" (Hadnagy and Wilson 2010, 135). NLP is in essence the psychological coding of a person's frame of mind. It suggests that a change in a person's behavior can be influenced by injected language patterns. For instance, the text a person reads on Twitter or Facebook, the YouTube videos they watch, and the Television shows they follow. All of these influence a person's behavior. The coding of NLP is focused on the mental state of your target's mind-- both the conscious/unconscious relationships, and perceptual filters (Hadnagy and Wilson 2010, 138). NLP is the process of embedding commands to take a person down the road you want him to take.

Social Engineering is an important role in defining SOF's interaction with the cyber persona layer of cyberspace. The synthesis of information within social engineering concludes with a viable recommendation for SOF to counter cyber personas by exercising this skill. Furthermore, the prospect of social engineering to influence mass movements within social media is limitless. For the purpose of this research, a seminal moment will occur when information operations are married with social media to influence mass movements. Social engineering permits SOF to maintain the advantage by operationalizing marketing toolsets that offer trend and metric analysis for determining relational tendencies between multiple actors.

Hacking the Cyber Persona Layer

Performing Social Engineering (SE) is only part of the equation for SOF in hybrid warfare. Admiral Michael Rogers mentioned that hybrid warfare is underway in Ukraine, being exercised by Russia. We are still trying to understand it (Rogers 2015). The most difficult step in operating within the cyber persona layer is peering into the window of your adversary's mind. A cyber adversary is "someone who sees doors where others see walls or built bridges that looked to the uninitiated like planks on which one walked into shark-filled seas" (Parker 2004, 25). Cyber adversaries are those hackers who exist within terrorist organizations, and those involved in state sponsored hybrid warfare. For the purpose of this research we are not concerned about those who are referred to as hacktivists[4].

To understand further the cyber persona layer, it is important to profile the mental characteristics of the terrorist and state cyber actors. Without analyzing the adversarial mindset, you will never understand what it is that motivates an adversary. Cyber adversaries differ in the way they value their targets. In SE terms, this is what is important to understand: the values are placed on certain pieces of information or end-state. Does someone value schematics about military bases or is he more concerned with defacement? By understanding your adversary's methodology and mindset, it will provide an opaque picture of how a person would likely compromise a system. State actors are distinctively different from terrorists; therefore they behave differently in cyberspace. Ultimately, their digital thumbprint resembles others within their state sponsored organization. Because of this hive approach to cyber warfare, it is difficult to characterize each person. The approach for social engineering is to understand the mindset of the person; this must be based on the forensic tools used during compromise that illustrates a skill level. A complimentary approach would be a theoretical characterization that creates a profile of real hackers. The profile of a cyber hacker would show the techniques, tactics, methodologies, and style used to compromise a system (Parker 2004, 49). As mentioned in the abstract—the best way to understand a threat is to study its reflection.

[4] Hacktivists are individuals or online coalitions that promote or resist political or societal change through non-violent means. The on-line protests and other activities were originally legally questionable, but a recent evolution in tactics that includes data breaches, hacking for profit, and CIP intrusion crossed the legal threshold (Friedman 2013, 77).

Nation states and terrorists pose the largest threat of causing widespread damage. Both groups differ in their methodology and intentions. Terrorist organizations typically want attribution for actions within cyberspace, unlike state actors. State actors such as Russia, employ large-scale cyber operations, and strive for anonymity. State actors are primarily focused on information warfare versus attacks against critical infrastructure since this would accentuate the conditions for Clausewitz warfare. They are also more likely to use cyberspace to inflict further damage during a physical attack, as witnessed in Crimea. Terrorists differ from state sponsored adversaries, in that they rely on the Internet for communications, and recruitment. Terrorists further distinguish themselves from state actors in the tools they use. They download scripts written by others and execute them, versus developing their own capability, something synonymous with state sponsored activities. All cyber adversaries leave clues behind in the form of digital fingerprints. Their digital signatures include a repertoire of technical, security and behavioral science clues that are visible in the files they destroy or the networks they compromise. For example, whereas many cyber adversaries confine their attacks to malicious code, others accompany their attacks with digital messaging (Parker 2004, 146). As we will discuss, Stuxnet had multiples clues written into the code, indicating the origins of the program.

An area that needs further research is developing a psychological profiling algorithm; this would be useful when evaluating the psychological state of behaviors on social media, to decide who might be susceptible to influencing efforts in support of U.S. objectives. This approach would target at-risk people by using their electronic communication to detect changes in their behavior. The metrics produced from this algorithm would showcase the effects of a large-scale social engineering operation gaining a foothold within a population.

CHAPTER THREE

AUTHORITIES: THE DIFFERENCE BETWEEN TITLE 10 AND TITLE 50

Cyber Space Limitations

State actors, and non-state actors, such as extremists and terrorist organizations, use the Internet. Terrorists, non-state actors and extremists have compensated for their inadequacies in the physical domain by harnessing cyberspace. By penetrating and networking the diaspora communities through the Internet, non-state actors have created a network of continuity. The Internet is a tool for radicalization and recruitment, a method of propaganda distribution, a means of communication, and a weapon to deal with tactically superior opponents. Terrorist groups such as Al-Qaeda and ISIS are on the Web proselytizing, fundraising, and inspiring imitators (Alexander 2013, 4).

Domestically, the use of cyber attacks against critical infrastructure has yet to occur against the United States; unfortunately it is just a matter of time before this takes place. The most recent defacement of the Central Command's (CENTCOM) Facebook profile and Cyber vandalism against Sony Pictures did not cause physical damage, but had significant psychological and financial impact. The US government has limited methods for countering terrorist and insurgent information operations through counter propaganda techniques. Special Operation Forces (SOF) is limited in their ability to sway public opinion through counter-propaganda efforts. The challenge is whether the US should remove these sites or allow them to exist as a "honeypot" and monitor for intelligence. These decisions to counter cyber threats are made at the national level. Each national level agency has a different approach and oversight to combating adversarial use of the Internet. What Special Operations Forces (SOF) needs to define further is what statutory law and authority, commonly referred to as “rice bowl,” supports SOF cyber operations in support of full spectrum warfare.

The Department of Defense (DoD) owns seven million networked devices and has thousands of enclaves dedicated to enhance intelligence and situational awareness in the cyberspace domain (Alexander 2013, 6). A networked SOF requires integration between the military and intelligence community. Concerns about SOF’s role in cyberspace, commonly referred to as “rice bowls,” are raised when the discussion of unconventional warfare and cyber warfare are mentioned in the same context. This section will distinguish Title 10 from Title 50 and will articulate the legal basis for SOF cyber warfare. A Title 10 authority refers to the operations conducted by the Department of Defense (DoD). Title 50 authorities refer to operations conducted solely by the intelligence community and covert actions. Unfortunately the line between covert title 50 actions and clandestine military Title 10 operations has blurred, particularly because Title 10 operations do not have oversight from the Intelligence committees (United States Senate Select Committee on Intelligence 2009, 6). Of particular importance is the difference between legal authorities codified at 10 U.S.C., which authorizes U.S. Cyber Command to initiate computer network attacks, and those stated at 50 U.S.C., which enables the National Security Agency to collect intelligence data. Recently the classified Presidential Policy Directive 20 (PPD-20) on U.S. Cyber Operations attempted to create rules of engagement for cyberspace. Moreover, the conference report on H.R. 1540, National Defense Authorization Act For FY 2012 Section 954 *Military Activities in Cyberspace* authorizes the DoD to conduct offensive cyberspace operations upon presidential approval. Section 962 of this same NDA authorizes the Secretary of Defense to conduct *clandestine cyberspace* activities in support of military operations pursuant to the use of military force.

The Difference Between Covert and Clandestine

Before going on, it is important to make the distinction between *covert* and *clandestine* operations. Leon Panetta quoted this statute and defined covert action as "an action by the U.S. government to influence conditions abroad where the role of the U.S. will not be acknowledged" (United States Senate Select Committee on Intelligence 2009, 6). Furthermore he states that traditional military activities are *exempt* from covert actions.   A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of identity of the sponsor (*Joint Publication 3-05.1* 2007). JP 3-05.1 defines clandestine as "operations sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment." U.S.C Title 50 governs how the United States conducts wars and ensures national security by outlining intelligence operations. Specifically, 50 U.S.C. § 413b(e)(1) defines covert intelligence activities of the U.S.G. to "influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government *will not* be apparent or acknowledged publicly." 50 U.S.C.§ 413b(e)(2) distinguishes that traditional military activities such as UW are excluded from covert actions.

10 U.S.C. § 113(b) Title 10 created the Office of the Secretary of Defense and assigned the Secretary of Defense all "authority, direction and control" over DoD, including all subordinate agencies and commands. It also created U.S. Special Operations

Command (USSOCOM) and provided the definitions and authorities for special operations missions that include strategic reconnaissance and unconventional warfare (UW). Executive Order 12,333, directs the Secretary of Defense to "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and counterintelligence" (Wall 2011, 99). Title 50 establishes and defines authorities within the intelligence community, but it also clarifies that the Secretary of Defense controls those members of the U.S. intelligence community who are part of DoD.47 (*§ 403–5* 2006). It does not include intelligence activities solely focused on the planning and execution of tactical military operations.

To put this discussion into a broader context, it is important to address the legal authorities for UW activities, which have corollaries to activities in support of cyber warfare. Unconventional warfare tactics and techniques typically include intelligence collection, subversion, and sabotage through the use of small SOF teams working by, with, or through indigenous forces. UW is a form of limited war where conventional military forces are not able to achieve the desired outcomes. Unconventional warfare's end state is accomplished by exploiting an adversary's political, military, economic, and psychological vulnerabilities through the development of indigenous forces in order to meet US objectives. UW operations are conducted in secret, on foreign soil where public acknowledgement of SOF involvement may raise diplomatic and national security concerns (Wall 2011, 92). By replacing the context of the physical domain with cyberspace, SOF can actually accomplish the strategic objectives of UW through tactics in cyberspace as long as the operations are under military command. This is where the rice bowls become disproportionally filled and policy makers mistake these activities as belonging to Title 50.

Military operations can resemble intelligence activities due to mutually supporting initiatives and synergy. The SECDEF can direct intelligence activities by the military in response to national intelligence requirements or to the tactical needs of DoD. Lieutenant General Keith B. Alexander was the Director of the National Security Agency, and also serves as the Commander of U.S. Cyber Command; this is an example of Title 10 and Title 50's duality. During his confirmation hearing, he explained the synergy between NSA and Cyber Command, and how each has its own mission and authorities along with oversight (Wall 2011, 115). Title 10 and Title 50 are mutually supporting authorities that can be employed by the same person; to arrive at the true distinguishing feature, one must ask the question: who is sponsoring the activity? Title 10 provides less oversight than Title 50; however this is taking rice out of the intelligence communities rice bowl. Cyber warfare resembles UW in that they both could be considered a military operation, an intelligence activity or a covert action. As mentioned earlier by Leon Panetta, traditional military activities are not intelligence activities or covert actions, which is why we need to identify the differences, and how they relate to cyber warfare and UW. Arthur Wall, in his research for Harvard's Security journal, states that "military operations preparatory to anticipated conflict are traditional military activities" and unacknowledged military operations are not necessarily *covert action (Wall 2011, 123)*. During Leon Panetta's confirmation he hinted at this when he defined military operations as operational "preparation of the environment" (United States Senate Select Committee on Intelligence 2009, 6).

A military operation that is conducted by SOF in support of unconventional warfare that is conducted in pursuance of a tasking from the SECDEF is still a military operation—no difficulty in understanding this. Therefore if military personnel, through the same tasking by the SECDEF, conduct cyber operations, then this should be considered a military operation. As long as this operation is authorized and funded by T-10, and is supported by USSOCOM, which is not part of the intelligence community (IC), this should be considered Title-10. Arthur Wall explains that the difficulty that exists is that Title 50 includes a provision that the Title 50 retains control over all covert actions. NSC Directive 1012 lists those actions, for which the U.S. Government can plausibly deny responsibility as: "propaganda, economic warfare; preventive direct action, including sabotage, anti-sabotage, demolition and evacuation measures; subversion against hostile states, including assistance to underground resistance movements, guerrillas and refugee liberation groups, and support of indigenous anticommunist elements" (Wall 2011, 128).

The point that is most important for distinguishing why cyber warfare, like UW, is a military operation differs from covert actions which are not intended to be acknowledged. That is, if the activity is eventually going to be acknowledged at some point in time, then the military operation is not covert action. Additionally, the statute does not provide a time window for when the operation must be acknowledged by the U.S. Government and excludes the following activities from being covert: traditional military activities or routine support to such activities; activities to provide routine support to the overt activities; and activities where the primary purpose is to acquire intelligence (*§ 413b* 2006, 1–4). Hence Arthur Wall concludes that even unacknowledged unconventional or cyber warfare activities are not covert action if they are a ‘traditional military activity’ or considered ‘routine support’ to a traditional military activity (Wall 2011, 132). Traditional military activity is exempted from the Title 50 U.S.C. covert action definition since the identity of the sponsor of a traditional military activity may be known.

Unconventional Warfare and Cyber Warfare as Traditional Military Activity

10 U.S.C. § 167 (e) (j) authorizes Special Operations Forces to conduct activities to include Unconventional Warfare, thereby creating a *possible* niche for UW activities in cyberspace. Furthermore, 10 U.S.C. § 167 (g) establishes limitations for conducting intelligence activities by the DoD by requiring notification from the Select Committee on Intelligence to conduct these activities. SOF’s presence and niche in the cyber domain is categorized as a traditional military activity or routine support. According to the Conference Report from H.R. REP. NO. 102–166, traditional military activities have four components. These are: activities by military personnel; activities under the command and control of a United States military commander; activities either preceding or related to hostilities which involve US military forces; and activities that are either apparent or acknowledged (Wall 2011, 134). It is rather straightforward that, with an authorization order, and within the limitations of that authorization order and Title 10 code, SOF can conduct those cyber operations in support of traditional military activities. Furthermore, SOF can conduct operational preparation of the environment (OPE) through cyberspace since this is constituted as a traditional military activity despite some arguments against this designation. OPE fails the third requirement for a Title 50 covert action since OPE is a clandestine activity that is conducted secretly; however the United States intends to

disclose the activity and will acknowledge it if discovered. By expanding Title 10 to include “military source operations” authority, commands are able to conduct clandestine HUMINT operations by using cyberspace.

Unconventional or cyber warfare is considered a traditional military activity that may legally be conducted when directed by the SECDEF in preparation for an anticipated conflict even if unacknowledged (Wall 2011, 140). Fortunately, social engineering of the human domain is a skill that lies within the scope of Advanced Special Operations (ASO) and can be practiced in cyberspace. Examples of these activities are identifying individuals on social forums, blogs and networking sites and building lines of trust within social media to establish reputable cyber personae. The possibility exists for cyber warfare operations to exist within both Title-10 and Title 50 authorities, but for the purpose of this research we are limiting these activities to non-covert “clandestine” Title-10 operations.   This extricates the approval and reporting requirements for military cyberspace operations.

CHAPTER FOUR

LITERATURE REVIEW ON CYBER OPERATIONS

Understanding the Internet

Terrain matters because it is the predominant component of any military strategy in the physical and cyberspace domain. In terms of military strategy, specific terrain offers a tactical advantage over adversaries by offering the high ground or a defensive position. This concept is generally understood by military theoreticians, thanks in part to the sixth century writings of Sun Tzu. By analyzing his writings on terrain, one can surmise that knowing your enemy and yourself is not enough when in battle. A tactician must understand how the "conformation of the ground [cyberspace] is of the greatest assistance in battle." By understanding the enemy's connection in the physical domain, a superior adversary can control victory. Sun Tzu wrote "with knowledge of these factors he [the cyberspace adversary] is certain to win; he who does not will surely be defeated" (McNeilly 2014, 77). According to Joint Publication 2013 (R), cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona—this is the terrain for conducting operations in support of warfare. There is a correlation between how military doctrine applies in the physical domain and how it *should* apply in the cyberspace. Sun Tzu identified six types of terrain and their importance to military generals in warfare. The correlation between the six types of physical terrain and cyberspace is generalized into three separate layers identified by JP 3-12 (R). Terrain that is easily passable can be thought of as the physical network;

terrain that is steep is embodied in the logical layer; terrain that is narrow can be illustrated in the cyber-persona layer. Another way to understand a virtual network is by comparing it to a tree's root system. The roots of a tree traverse in all directions underground. An observer can be touching the root of a tree either at the end-point of the root rather than at the trunk, commonly referred to as the networked center location. In both circumstances an observer is touching the root, but the physical network location varies drastically. Therefore, an adversary that is using a web client service is not necessarily broadcasting a more accurate location than someone using an Android or IPhone. The physical location of mobile devices on the virtual root system is actually more accurate than trying to determine the location of an IP address on a network. An injustice is occurring by visualizing a devices location within an ellipse or radius: in actuality, it should be viewed on a virtual root.

A body of literature has grown calling attention to a strong possibility that many future conflicts will occur in the Cyberspace domain. This domain is an essential part of every day life, but arguably the most difficult to understand. Presidential directives, Joint Publications, and policy memoranda are being churned out to provide guidance and direction for operating in Cyberspace; however some recipients are unable to understand the Cyber domain. A startling trend amongst policymakers is that *only* the Infrastructure Technology (IT) technicians need to understand the interworking of the Internet—this is a fallacy. The world of cyberspace is an unbelievably intimidating place, resulting in confusion. This has led to a growing concern of how offensive cyber operations are to be conducted and how Special Operations Forces (SOF) use their niche of Unconventional Warfare (UW) in the cyber domain. In fact, this thesis proposes that Special Operations

Forces need to have a defined role within cyberspace, and argues in support of using the cyberspace for operations in support of Hybrid Warfare. It also raises the more problematic debate between offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO), which is based on their intended use of cyberspace. Prior to defining the role of the ghost in the machine (SOF Cyber Operator), policymakers and military leaders must understand how this *cyber stuff works* (Friedman 2013, 1–7). Evidence supporting this approach comes from extensive review of military doctrine and understanding the Internet. Cyberspace operations take place in environments that are not under any nation's control. There are innumerable adversaries; and technology proliferates rapidly and often makes attribution impossible (Department of Defense 2013, 14).

My three-year-old son was introduced to his iPad Air twelve months ago and this changed his life. With a swipe of his tiny finger, he is able to navigate YouTube, iTunes, and ask Siri for directions home. He is connected to the Internet at all times and understands how to communicate with two swipes and a tap on the screen. This skill is remarkable considering his age; however what is most impressive is when he knows that his Internet connection is not working. He understands that in order for him to get this magnificent machine to work, he needs the Internet. When the Ipad ceases to function as prescribed, he goes into his abbreviated iPad battle-drill, checking the Wi-Fi connection and resetting the router and modem.[5] At the age of three, he essentially understands how the world has become interconnected through the use of the cyber domain. So why is it so challenging for the general public and policy makers to understand Cyberspace--

[5] Battle drills provide standardization for immediate action when faced with an incident. U.S. Army FM 7-8 refers to these as a quick practiced response that minimizes the decisions to be made.

specifically the physical interaction with the physics of cyberspace? The reality is that defining and understanding the Internet is extremely difficult because it deals with physics. It took until 2008 for The Department of Defense to define Cyberspace as: "The global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Department of Defense 2013).

Peter Singer defines cyberspace as the realm of "computer networks (and the users behind them) in which information is stored, shared, and communicated online" (Friedman 2013, 13). Cyberspace is both a physical and virtual information environment that graphically depicts data between computers (and users). Information is stored and transmitted between computers through the use of networked computers, closed intranets, cellular technologies, fiber-optic cables, and satellites. It is expanding at a rate of 2,500 terabytes daily partly due to the expansion of the smartphone market (Friedman 2013, 15). Cyberspace is the central nervous system of the world that is comprised of a thirty-year-old man-made infrastructure with human beings sitting behind terminals controlling key features. Hence, in order to affect Cyberspace, adversaries must consider the human domain and the physical domain of where those humans and infrastructure amalgamate—this is SOF's niche in Unconventional Warfare (UW).

The Virtual Internet

Packets are small digital envelopes of data that are transmitted between users; this is the Internet. The envelope is addressed with information similar to what is written on physical envelopes: network source, destination, and content information. The envelopes are divided into smaller decentralized components and reassembled at the receiver. Computers are essentially doing a virtual handshake and accept information based on packet protocols known as Internet Protocol (IP) or Transport Control Protocols (TCP). TCP are responsible for routing application protocols to the correct application on the destination computer. TCP's are reliable connections unlike IP's that are connectionless and send information to other computers regardless of the routing of information (Shuler 2002).

The protocol stack provides instruction on how information is constructed and is a network of networks. The protocol stack is also comprised of a hardware and application layer for translating packets into visual information. Information is displayed on a networking interface known as the Hyper Text Transfer Protocol (HTTP) and an accompanying system of URL's that link documents. Essentially this is what allows systems to communicate and has opened the new door of warfare. With the click of a mouse a half a world away, adversaries can disrupt or destroy critical infrastructure like utilities, transportation, communications, and energy (Friedman 2013, 4).

To further unpack how the Internet works, it is important to walk through how information is passed transferred in cyberspace. Understanding the architecture is vital due to the military definition of the cyberspace domain. JP 3-12(R) articulates that cyberspace consists of the often overlapping networks, as well as the AS nodes on those networks, and the system data that support them.[6] A device creates a connection with the server that contains the information you are researching. This is done by requesting

[6] JP 3-1 2 (R) classifies that any device or logical location with an Internet protocol address or other analogous identifier is considered part of the cyberspace domain along with the routing tables

information through HTTP, which defines how to ask and deliver information. An Internet Service Provider (ISP) assigns your device an IP address and you establish a connection with the end point. The Internet is a series of connected devices, each one having a unique IP address. Most ISP's assign a dynamic IP address for your connection in the form of a twelve digit numerical address (255.xxx.xxx.xxx). ISP's form nodes known as Autonomous Systems (AS) in the global Internet. Autonomous Systems define the architecture of Internet connections where traffic is routed. Each AS has a set of contiguous blocks of IP addresses. To find the information you requested all you need to do is find the AS that houses your IP.

ISP's act as the backbone of the Internet and bridge the networks of information. To track the information, your device looks for the endpoint of this information (IP address) by routing to the Internet through a router, which has a separate IP address. This information is transferred to the Domain Name System (DNS), which is the protocol infrastructure that connects computers to websites or IP addresses. The DNS acts as an upside down funnel that points information into a more specific location. Once the information reaches the neck of the funnel, your computer will learn the specific IP address from the name server for the information you originally requested. Once the request for information reaches the IP address, this information is transmitted back in a series of packets.

Information is passed through the nodes, which read the packets and divert the information through routing tables that get the information to its destination. Routers are responsible for sharing of information with other routers in order to complete the process by taking a snapshot of the current image of the Internet. Most people don't recognize that the Internet is a cache of information that morphs every second. To see this process in action type: *tracert www.foxnews.com* into your search engine and pay attention to the physical infrastructure that is queued. By understanding the transfer of information now we are able to understand the physical component of the Internet. The blurring of cyber and physical has come to fruition; digital systems are embedded in the physical domain.

The Internet backbone is a transcendent idea comprised of a hierarchy of systems and controls. At the highest level of the hierarchy are Internet Exchange Points (IX). These are commonly referred to as privately owned Metropolitan Area Exchanges (MAE) or government Network Access Points (NAP). The next layer down in the hierarchy is the Network Service Provider (NSP) that is connected to both the MAE and NAP in order to transfer information packets. The NSP's sell bandwidth to regional ISPs that in turn sell connectivity to the consumer. Unlike the virtual Internet mentioned above, the physical architecture of the Internet is something that can be viewed and touched.

The Physical Internet

A common misconception is that the cyberspace world inside of a screen is not considered a reality; however this is untrue. A person *is* able to tug on the physical connection of cables and trace it to a physical place. Large datacenters comprised of petaflop supercomputers, processors, and server racks exist and manage information. There are dozens of physical locations around the world where the virtual networked world meets the physical world turning mother earth into a motherboard. One of these locations is at 60 Hudson Street in New York City which houses a network of networks that connect the submarine cables, which travel underneath the ocean (Blum 2012). In essence, the physical network layer of cyberspace is comprised of both the geographic component and the physical network. These components include the following: physical hardware; wired, wireless, optical, satellite, and cabled networks; software and infrastructure (physical connectors, routers, switches, and servers) (Department of Defense 2013, 16).

A 3000-mile cable that is slightly larger than a garden hose connects the world. At this point is where the computational process meets the physical process. Light is sent from one side and every fifty miles the signal is amplified to boost the rate of transmission to upwards of 10 gigabyte per second. Once the cable reaches a junction point on the other continent it branches out and contours the coast, increasing connectivity and effectively wiring all physical locations together. Networks of physical cables connect locations around the world and change the perception of Cyberspace from a cloud to a physical *thing*. According to Neal Stephenson of Wired Magazine, "it behooves wired people to know a few things about wires-how they work, where they lie"(Stephenson 1996, 2). The unfortunate truth is that in order for SOF to affect cyberspace, we must understand the physical network and stay abreast with technology. Technical ignorance must be eradicated to define SOF roles in cyberspace. This includes educating the Director of the Department of Homeland Security on how to use e-mail since she was not able to in 2012 (Blum 2012, 5).[7]

The Military Cyberspace Domain

[7] The DHS is responsible for the cyber security of the United States.

To bring back this concept full-circle, recent doctrine and command guidance has been published defining operations in cyberspace, but the SOF role has only been minimally defined. In order further to understand the use of offensive cyber weapons and their role within the US military, *Offensive Cyber Operations* in US Doctrine provides the dialogue for US military offensive cyber operations (OCO). This new offensive capability was originally classified SECRET. However, it was recently disclosed in Joint Publication 3-12(R). This was previously echoed by Admiral William McCraven during the *Department of Defense Authorization of Appropriations for Fiscal Year 2015 and The Future Years Defense Program.* In March 2014, Admiral McCraven explained to Senator Reed that SOF currently provides operational demands to the National Security Agency (NSA) when individuals are being sought. When asked about USSOCOM developing internal SOF cyber capabilities, McCraven requested to discuss this topic in a closed-door meeting, which foreshadowed the upcoming guidance from USASOC in ARSOF 2022.

The *ARSOF Operating Concept 2022* calls for the use of the cyber domain to facilitate surgical strikes and intelligence operations (Cleveland 2014, 27). Lieutenant General Cleveland calls on ARSOF operators to embrace the cyberspace domain and the way in which core activities are enabled in the cyber domain. ARSOF Cyberspace operations will be conducted by: cyberspace domain-enabled intelligence capabilities through the leveraging of social media exploitation capabilities; offensive cyber operations; and Cyber Intelligence Preparation of the Environment (CIPOE) according to ARSOF 2022. Furthermore, SOF must adapt to rapidly emerging technological advancements to keep pace with commercial cyber domain advancements and adequately manage attribution (Cleveland 2014, 64). The command strategic guidance provides a reference point for the vision of a Globalized Special Operations Network, though it is characterized by uncertainty. But what does this command guidance look like in the fifth domain? JP 3-12 (R) provides a joint doctrine for the planning and execution of cyber operations across the range of military operations and is the most transparent guidance to date. The military cyberspace domain is defined thoroughly in the Joint Publication; however it does not capture the most important factor of cyberspace: The military cyberspace domain is supported by the civilian cyberspace domain and infrastructure. The civilian networks that are used daily allow the military to be everywhere and anywhere. The civilian networks give the military the residency in civilian cyberspace, considering that regardless of the sophistication of *intranets*, they are always connected to the Internet.

Joint Publication 3-12 describes the operational environment of cyberspace in three layers: A physical network, a logical network, and a cyber-persona layer (Department of Defense 2013, V). The physical network is composed of the geographic and physical network components; the logical network consists of the virtual elements; the cyber-persona layer uses the logical network layer to develop to create a digital identity in the logical network. There is a growing demand to identify and explore new uses for cyber weapons in support of Special Operations. The U.S. will need to examine new and innovative ways to modernize its irregular warfare fighting capabilities. Within its Unconventional Warfare (UW) capabilities, the U.S. will need to know how to leverage cyber weapons for tactical advantages. Movement and maneuver in cyberspace can occur in all three layers: the physical network, logical network, and the cyber-persona layer. Cyberspace operations require the integration of offensive, defensive, and timely operational preparation of the environment (OPE) (Department of Defense 2013, 23). The contrast between the application and effect of cyberspace operations will determine the potential role for cyber capabilities in UW. Cyber weapons can be categorized by their ability to affect the physical domain.

The Department of Defense categorizes missions in cyberspace as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense Information Network (DODIN) based on their intent. The intent of cyberspace operations is to meet the objectives utilizing cyberspace weapons. There is a trend amongst some academics discussed in this paper to advocate the use of cyber weapons, such as malware in support of national policy. Some authors pinpoint the benefit of using cyber weapons through social media; others believe that cyber weapons should be offensive in nature. The uses of each of these operations can be viewed in the case studies of the Stuxnet Virus in Iran, the Arab Spring Revolutions, and Russian cyber attacks. US doctrine agrees that there is a role for cyber operations. The question is, what part will SOF play in this role?

Cyber Warfare Through Social Media

The Arab Spring of 2011 in Egypt, Tunisia, and Libya painted an important picture for the utility of social media as a cyber weapon in support of Unconventional Warfare. As referenced earlier by JP 3-12 (R), social media is considered the cyber-persona layer (on-line identity) where people are actually on the network. The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the logical network layer to develop a digital representation of an individual or entity identity in cyberspace (2013, 46). The Arab Spring Revolution demonstrates that uprisings greatly benefit from the use of social media. The rapid flow of information from social networks, blogs and SMS text messaging has changed the social fabric of how we communicate and methodologies were developed as a result. LTC Brian Petit stated the future success of UW operations by U.S. Special Operations Forces depends upon incorporating social media (Petit 2012). His analysis of social media in the 2011 Arab Spring Revolutions is focused on the nexus between Twitter and Facebook and UW. Upon further dissection of the Arab Spring, research demonstrated that key benchmarks of a UW campaign can be accomplished in the cyber domain through the following: "Social mobilization, the digital underground and the weapon of the narrative"(Petit 2012).

Social networks in the cyberspace were used to incite popular support and to spread ideology beyond geographical borders. All of which has profound implications for adversarial use. The fusion of civil unrest in the physical and cyberspace domain observed during the Arab Spring, and more recently in the Crimea, proves the salience of social media in bringing about political change. SOF should pay attention to the characteristics of social media exhibited during the Arab Spring; these can be leveraged during UW campaigns. The Arab Spring demonstrated the power and potential of social mobilization and collective action as a form of cyberspace operations in support of hybrid warfare by operationalizing social movements[8]. The Arab Spring revolutionaries were able to achieve significant effects using mobilization through social media. The goal of

[8] Hybrid warfare is being used to describe the form of warfare that incorporates UW and cyber warfare. This term was incorporated into the recent published doctrine for Russia and was exhibited during the Crimean war.

UW is to coerce, disrupt, or overthrow an occupying power or government; this draws a corollary to that of the Arab Spring accomplishments using social media. The Arab Spring revolutions won control of the political state by winning control of the population through social media.

The contemporary operating environment is cyberspace and there is an increasing trend for social movements to rely on information technology to achieve their objectives (Lee and Johnson 2014, 1). During the Arab Spring, social media took a loosely organized group of cyber-personas and transformed them into a powerful, politically charged revolutionary movement. The revolution of cyber-personas related to an actual person, incorporating some biographical data, e-mail and IP addresses, web pages, and phone numbers. Individuals could have multiple cyber-personas that vary depending on what message is being propagated. Through the use of Twitter and Facebook, a common grievance could be shared through pictures and stories—creating a digital alliance. Through social media, online communities shared a similar collective action and were able to spark an unstoppable revolution. Brian Petit discovered that "digital networks that [propagate] social-media content present both an environment and a communication-based weapon system" (Petit 2012).

Social media has the ability to influence the goals of Unconventional Warfare by aiding in the disruption (or overthrowing) of an occupying power or government, which is precisely the aim of a revolution. The evolution of warfare and conflict is occurring, depicted by four emerging patterns—all of which can be leveraged by social media. War is becoming increasingly characterized by irregular conflicts fought by transnational actors where states work through non-state actors against adversaries taking advantage of internal grievances (Lee and Johnson 2014, 1). Wars, specifically internal conflicts, are also becoming increasingly protracted without a well-defined truce. The rise of worldwide politics, on-line propaganda, and public opinion during conflict is resulting in an increasing success rate for insurgencies. This is by far the most significant pattern to recognize since war has become more about controlling perceived legitimacy, politics and public support, than just inflicting damage on the opponent (Lee and Johnson 2014, 1). Inferior insurgencies are outgunned, outnumbered, and unable to win using typical military tactics and weapons; therefore they leverage popular perceptions through propaganda to increase their odds of a favorable outcome. The fourth pattern that Doowan Lee and Glen Johnson point out is that non-military tactics are becoming more effective. The use of civil unrest and social movements are more effective at achieving objectives than violent armed conflict.

The likelihood of a successful UW campaign relies on being able to take advantage of the aforementioned patterns. Lee and Johnson cited that sponsor should "look for existing, organic opposition movements [online] capable of using both nonviolent and violent tactics to maximize popular support" (Lee and Johnson 2014, 2). They further explain that a UW campaign should seek to co-opt and develop existing opposition groups and networks, if available, and organize them into a larger opposition movement (Lee and Johnson 2014, 2). Social media allows the users to project influence across time zones and international boundaries, coining the term "borderless social mobilization" (Petit 2012). Mass digital movements that span international borders become the new resistance movements in a multi-front UW campaign. The movements draw a corollary with the integrated employment of information operations (IO) during operations. IO (social media) is used to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while projecting one's own narrative (Department of Defense 2013, 18). Traditional methods of building resistance movements involve high-risk operations that endanger U.S. military and civilian lives. By using the digital-centric mobilization (social media), revolutions can take place in the cyber domain versus the physical domain. Social media has the ability to create a digital underground, auxiliary, and guerilla force—in essence a digital mass movement. It behaves like an accelerant and affects a movement's perceptions and behavior in support of US objectives (Petit 2012). Furthermore, social movements that use limited violence surgically and strategically are twice as likely to achieve their objectives as violent campaigns (Lee and Johnson 2014, 3).

Petit notes the challenges of the digital underground, which are comprised of a chaotic leaderless force. (Petit 2012) Therefore, a UW campaign strategy needs to be applied against the cyber domain, which will focus the direction of mass social movements. By adopting and integrating social movement theory (SMT) tools, we can view and conduct UW in the cyber domain differently. The social movement approach to UW influences the environment and co-opts existing organic movements in order to influence strategic outcome (coercion, disruption, or regime change) (Lee and Johnson 2014, 1). By leveraging already existing social movements, the potential blow back against the sponsor or negative propaganda is minimal, therefore increasing the overall legitimacy of the movement. This SMT approach to unconventional warfare depends on long-term activities that have an enduring impact on the strategic consequences (as opposed to a synthetic insurgency). Historically UW campaigns are focused on coercing or disrupting a government. Between 1950 and 2005, the United States sponsored twenty-four UW campaigns, of which only 30% were designed to overthrow the government. By leveraging the SMT approach through social movements in cyberspace, SOF would focus on disrupting or coercing adversarial governments versus paying the political price of a regime change. This capability is something that SOF is better suited to manage versus Cyber Command.

Social media operations centers can be used to trigger reactions in the physical domain through manipulation of flash mobs, denying Internet service, or bypassing state sponsored Internet censors. (Petit 2012) The author finds that tactical actions could be executed based on anticipating, shaping and exploiting social and psychological conditions. This is done through the following: "monitoring (understanding), posting (shaping), denying (blocking), spreading (pushing coverage), swarming (mass) and messaging (tactical or digital actions designed for psychological effect)." (Petit 2012) Thus a common use for cyber weapons could be accomplished through the use of social media tools.

Doowan Lee and Glenn W. Johnson codify the social movement approach into four lines of effort. Their research does not specifically state in which environment, physical or cyber, this is to be propagated. However, based on recent historical case studies in the Ukraine and in the Arab Spring the contemporary operating environment was cyberspace. The following lines of effort are in essence interchangeable between the physical and cyberspace domain. Their recommended approach focuses upon deepening already existent socioeconomic grievances. Secondly, they will create a political cleavage by exploiting elite fractures or supporting indigenous dissidents. Concurrently the organization effectiveness of the sponsored group will be enhanced. Throughout the duration of the campaign, there will be an effort to expand the indigenous narrative to support strategic objectives (Lee and Johnson 2014, 3). In order for this to happen, UW campaigns need to begin mapping the human domain in geopolitical hotspots and countries. The most effective method in the persistent mapping of the human domain is through social media, which is referred to as the cyber-persona layer. Detail orientated analysis will provide SOF with the ability to align our objectives with already existent indigenous narratives. Focusing efforts to identify and co-opt a self-sustaining movement can be accomplished by mapping the following: Identifying elite fractures; Understanding strategic network dynamics; and exploiting fractures (Lee and Johnson 2014, 3). Analysis of social media will further enrich the understanding of how movements are structured and can identify what methods (if any) are needed to influence UW campaigns, thereby creating a measure of effectiveness.

Petit's research indicates that though the use of cyber weapons is strictly limited to non-offensive techniques, these techniques have the ability to shape and influence the human domain. The connection between networks, individuals, groups, and interaction with cyber personas is necessary for a UW campaign. As stated by Lee and Johnson, "human domain maps [in cyberspace] will aid in identifying the strategic networks" within the insurgent movements and assist in aligning objectives (Lee and Johnson 2014, 3). The relational data points in turn will create the framework for developing a Global SOF Network. Moreover, SOF Cyber operations should develop cyber-persona terrain maps that resemble topographic maps to monitor anomalies and flashpoints. This would allow military planners to take advantage of the increasing usage of social media social movements. Not all research concludes that cyber operations should be limited to non-offensive operations. Technology and adversarial ingenuity are outpacing U.S. policy in determining the extent to which cyber attacks can be used.

Cyber Intelligence Preparation of the Environment (CIPOE)

Understanding the cyberspace domain and its relationship to the physical domain is the first step in planning military operations. All military operations require a thorough analysis of the situation, referred to in the U.S. military as Intelligence Preparation of the Operational Environment, or IPoE. Cyber Intelligence Preparation of the Environment or CIPoE consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations (Department of Defense 2013, 23). CIPOE is conducted under military authority, coordinated with the intelligence community in order to prevent compromise. This activity is passive in nature and researches the composite of metadata conditions, circumstances, and influences that affect the cyberspace domain. As previously noted, the cyber terrain is an aggregate of cyber-personas, networked systems that collect, process, disseminate, information. The information (operational) environment is broken down into the physical, informational, and cognitive dimensions (Department of Defense 2013, 18). CIPOE includes activities in cyberspace conducted to gather intelligence that may be required to support future tactical operations, and other cyber (offensive and defensive) operations.

Intelligence gathering in cyberspace focuses on intelligence requirements, in addition to the mapping of adversary cyberspace activities. This is referred to as situational awareness and is the essential current and analytical knowledge of cyberspace.

This includes all factors that affect adversarial forces in cyberspace. These intelligence requirements (IR) of cyberspace integrate into the planning and operation of cyberspace operations. The intelligence requirements of the adversarial cyberspace may include: network infrastructures, unique cyberspace signature identifiers such as unique hardware, server locations, software versions, and configuration files. CIPOE is referred to as cyber intelligence and blends signals intelligence and open-source intelligence. CIPOE gathers intelligence requirements from collecting and analyzing intelligence from an array of sources such as social media sites, Skype and Voice Over Internet IP (VOIP). Additionally, cyber reconnaissance entails collecting open source information from foreign news media, chat rooms frequented by threat actors, and YouTube videos from crisis areas, or commercial imagery, to cite just a few applications (Hurley 2012, 13). Cyberspace operations that resemble these activities against the physical networks can be referred to as computer network exploitation (CNE).

CNE's are defined as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data about a target or adversary network (Cartwright 2011). The physical network is the primary target for open source intelligence, CNE, and human intelligence, further obscuring the lines between the intelligence collecting capabilities and authorities. CNE's are usually performed behind proxy sites that are dedicated to anonymization activities, onion routers, and other techniques used to obscure identity and positive attribution. CNE is deliberately performed through a toolbox that penetrates adversarial systems for intelligence collection, and is not necessarily surfing the Internet for ISIS Twitter handles or hash tags. This is a deliberate intrusion into target hardware, software, or related networks and does not incorporate passive collection of intelligence that has value (Hurley 2012, 14). It is important to understand that this is a deliberate function that leaves no evidence on a network regardless of whether it is a chat room or YouTube.

In the black hat communities, CIPOE is often referred to as advanced persistent threats (APT).[9] An APT is a deliberate function by a team of professionals who are trying to learn everything they can about a target they are going after along with key vulnerabilities. APT is a form of target development that practices an array of online search tools and social networking to develop a target. In essence, APT is not just trying to understand the organization but also its key concerns and even tendencies (Friedman 2013, 57). Advanced persistent threats are *persistent* phased operations consisting of specialized teams that case targets (surveillance), intrusion teams that target specific information, and exfiltration teams that use all sorts of tricks to sneak out the information and disguise their tracks (Friedman 2013, 59). APT's often include phishing attacks that are considered a CNA and are categorized as offensive cyber operations.

Offensive Cyber Operations

Offensive cyber operations (OCO) are intended to project power by the application of force in and through cyberspace (Department of Defense 2013, 8). Cyber operations are concerned with using cyberspace capabilities to create effects which support operations across the physical domains and cyberspace. Offensive cyber operations do not have the Hollywood appeal of special operations teams slipping through Pakistani air defense networks to kill Osama Bin Laden, but they have strategic

[9] Black Hats are hackers with extensive computer knowledge whose purpose is to breach or bypass Internet security.

implications if understood and applied effectively. Cyber operations are skill oriented and require tremendous resources and patience. As cited by joint military doctrine and the recently leaked Presidential Policy Directive 20 (PPD-20), these highly classified and controlled capabilities are approved at the highest level against military targets.

The effects of cyber attacks are generally unknown since their attribution is rarely discovered. The appeal of OCO is that they do not require physical proximity; many CO's can be executed remotely from the comfort of an office. There is an overarching trend to use cyber weapons to affect adversaries, whether through complex niche weapons or rudimentary malware. Operations in the physical domains can create effects in and through cyberspace by affecting the transfer of data, or the physical infrastructure.

Cyberspace actions create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation leads to denial that is hidden or that manifests in the physical domains. These specifications are: Deny, Degrade, Disrupt, or manipulate. In order further to understand the use of offensive cyber weapons and their role within the US military, Steve Aftergood, in Offensive Cyber Operations in US Doctrine, provides the dialogue for US military OCO. He determines that these operations are a new territory for use by the US military and still evolving. He identifies that this new offensive capability was originally classified SECRET. However it was recently disclosed in Joint Publication 3-12(R). He warns that caution needs to be exercised when using OCO. According to the author, OCO actions are used to degrade, disrupt, or destroy access to a target's capability to support a commander's objective (Aftergood 2014). OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD). OCO requires de-confliction in accordance with (IAW) current policies. The author concentrates on the discriminating use of OCO and highlights that they are only used against military targets, the only lawful targets. He ascertains that the definition of military targets. He ascertains that the definition of military targets is broad, leaving commanders the ability to meet their objectives through unconventional targets.

According to Aftergood, what defines a military target? The ability to eliminate a terrorist leader through a drone strike is acceptable to the American populace, but is killing him by turning off his pacemaker acceptable? Emerging technology brings to light ethical questions on the application and use of OCO. Medical devices and hospital medical equipment have recently been identified as targets being exploited by hackers. (Finkle 2014) There have been twelve reported instances of cyber attacks against medical devices, which allow cyber attacks to injure or kill the person attached to the device. Devices such as pacemakers, defibrillators, and IV pumps rely on wireless technology and Internet connections (Finkle 2014). The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is responsible for ensuring the safety of patients and critical infrastructure from unintentional threats and now is focusing on deliberate cyber threats. The ability to attack a target through his or her medical device poses another possibly of OCO if the target is military. Dina Maron discovers that multiple medical device manufacturers are scrambling to protect patients and users of medical equipment (Maron 2013). Cyber Security Specialist Thomas Ridd believes that a cyber defense is never 100% effective; therefore through diligence and ingenuity, any medical device can be hacked. The example of cyber attacks against medical devices is specific with grave consequences. Vulnerabilities will be defeated by the ingenuity of adversaries, alike to the Stuxnet Operation in Iran.

Another example of a sophisticated cyber attack is the Stuxnet virus. The Stuxnet Virus has changed the opinions of offensive cyber operations by demonstrating that cyber weapons can affect and control the physical environment. This resulted in policy makers seeking cyber weapons that have this capability (Peterson 2013). Cyber weapons can be designed to target Industrial Control Systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS that manage critical infrastructure. These systems are vulnerable with less security than ATM cards; they offer a large payoff for cyber attacks. (Peterson 2013) Since the use and strategy of using cyber weapons is still evolving, there are limitless opportunities for attacking these systems. Peterson provides a detailed explanation of such opportunities that can be used to create maximum damage. The use of cyber weapons in this article not only highlights vulnerability, but also a capability that should be explored for implementation. (Peterson 2013)

Thomas Ridd and Peter McBurney focus on high-end offensive cyber weapons by distinguishing the five objectives of these weapons. The first goal is to get inside systems and to conduct a deep penetration. (Rid and McBurney 2012) The second objective is to target a specific component of a hacked system, not just get access to a vulnerable component. The third and fourth characteristics are directly related. These weapons are meant to break through security barriers and cause physical harm to the infrastructure these barriers protect (i.e. SCADA). The last characteristic is that the weapon should influence an active process in a malicious way by making it impossible to turn it off. The authors discuss how specialized weapons have been used to destroy dams, flood areas with sewage, and control nuclear reactors. These findings are important to understand since they are ways in which cyber weapons can be employed in support of a commander's objective. The author's most significant contribution is identifying that highly destructive cyber weapons will require significant intelligence and resources. (Rid and McBurney 2012) Developing a highly sophisticated cyber weapon and not employing the weapon is like parking a Ferrari in a garage and never driving it. Once it is developed, the next step is how to employ it.

CHAPTER FIVE

CASE EXAMINATION

This section will examine two cases relevant to defining SOF's role in cyberspace. The first case study, the Stuxnet virus, will be conducted in three parts: the technical dissection of the malware, the employment of the malware, and the effects of the malware. The approach for the second case study will examine the on-going physical and cyberspace events in Ukraine. This case study will address the use of hybrid warfare by the Russians, primarily focusing on the use of cyber operations (CO), information operations (IO) and special operations (SO). You want to explain why and how you chose these two examples: what is important about them in terms of them informing your thesis objectives?

Despite being relatively common, cyber attacks were not known for impacting every day life. This all changed on November 24, 2014 when Sony Picture Entertainment was hacked, releasing 100 terabytes of confidential data and costing the company over $15 million as well as, tarnishing the company's image (Frizell 2015). The cyber attack corresponded with the up-coming release of the film *The Interview,* and blackmailed the company into capitulation. This event is important to recognize, because it increased the importance of cyberspace for influencing and yielding a target. The Sony attack is considered *cyber vandalism* and is not relevant to the rest of this discussion, but like both of the following case studies, it highlights cyberspace's impact on strategic objectives. Differentiating between cyber vandalism, cyber terrorism, and cyber warfare is difficult. For research purposes, this thesis focuses primarily on *cyber warfare*.

It is important to have a broad appreciation of how the cyberspace layers are affected by cyber attacks. Each of the case studies illustrates a different tactical and/or strategic use of cyberspace. Like the Sony attack, cyberspace operations such as Stuxnet and Russian Hybrid warfare are employed with cyber weapons, commonly referred to as toolkits. The common tools have the ability to disrupt or deny Internet service, destroying networked architecture and even affecting the physical environment. The following are the most common cyber weapons: Phishing, Malware, Botnets, and Distributed Denial of Service (DDoS) attacks.

Phishing is the practice of sending out emails with lucrative messages, links or files to be opened to receive malicious information or payloads. Phishing is a term coined to describe how a wide net is casted against a group through e-mails in order to disclose information that can be used for later attacks. Once opened the malicious payload will open a virtual doorway inside of your machine to exploit or supplement information. Malicious software known as malware is a prepackaged exploitation of a vulnerability. It is comprised of a “payload of instructions detailing what the system should do after it has been compromised” (Friedman 2013, 43). A malware’s behavior determines its effects, instructions for reproduction to spread an attack are known as “worms”. Malware is also used to take control of individual computers and possibly entire computer systems. This is done to create a powerful resource of the multiple computation speeds of thousands of computers. Once under the control of an adversary, the computer system is controlled, becoming a member of a larger symphony of remotely controlled computers. This technique is commonly referred to as “botnets,” and users rarely know when they are compromised. Botnets, through a malicious script, establish a communication link between thousands of computers that binds the systems together (Theohary and Harrington 2015, 7). Once under the control of a Botnet, a computer is used to transfer information to a host or to launch a Distributed Denial of Service (DDoS) attack (Friedman 2013, 44). During the DDoS, the host orders the botnet to overload a target system with massive amounts of information. This attack targets the subsystems’ vulnerabilities that handle connections to the Internet. By overloading the system with incoming queries, the system “consumes computation and bandwidth resources” by overloading the DNS that eventually results in an outage (Friedman 2013, 44). DDoS use botnets from thousands of computers that makeup a hive of computers to distribute an attack of overwhelming traffic through a vector on an entire adversarial network. DDoS are unique because they exploit vulnerabilities in an adversary’s operating systems; they are attacks that ride on the infrastructure of legitimacy, efficacy measured in duration of outage (Theohary and Harrington 2015, 8). This overview provides the foundational knowledge of how the following adversaries are using cyberspace.

Case Study of Russian Hybrid Warfare

What happens when a complex distributed denial of service (DDoS) offensive cyber attack occurs in combination with Information Operation (IO), and Special Forces (SOF) against a state? In early 2014, this is exactly what happened when Russia launched an integrated cyber and unconventional warfare attack in Crimea—catching the international community off guard. As this section outlines Russian hybrid warfare characteristics, it also explores the contemporary use of these tactics by paramilitary separatists in the Ukraine. This case study attempts to answer the question of how regional adversaries are blurring the lines between cyber and special operations; physical and cyber domain; information operations and disinformation. The following case study will assess the Stuxnet virus, theoretically an intelligence operation that blended covert and clandestine tradecraft. This case study further seeks to clarify how U.S. Special Operations can formulate a definition of SOF in cyberspace by looking at the reflection of Russian hybrid warfare.

In 2012, the Department of Defense defined a hybrid *threat* as, "the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects (Department of the Army 2011, 1–5).[10]" However, the Department of Defense (DoD) has not defined hybrid *warfare* nor

[10] FM 3-0 Unified Land Operations updated the definition in 2012. The Joint Publication 1-02 has not defined hybrid warfare due to DoD reluctance. According to the DoD, hybrid warfare is considered Unconventional Warfare or Irregular Warfare.

do they have any intention of defining it since current definitions encompass all elements of warfare across the spectrum (D'Agostino 2011, 1–2). For the purpose of this research, though, hybrid warfare is defined as "violent conflict utilizing a complex and adaptive organization of regular and irregular forces, means, and behavior across multiple domains to achieve a synergistic effect which seeks to exhaust a superior military force indirectly" (McCulloh, Johnson, and Joint Special Operations University (U.S.) 2013, 56). This definition is analogous to the one given by the Chief of the General Staff, General Valery Gerasimov. He defines hybrid *warfare* as "The broad use of political, economic, informational, humanitarian and other non-military measures, supplemented by firing up the local populace as a fifth column and by [the use of] concealed armed forces" (Nielsen 2014). While I do not agree with his classification of political, economic, informational and humanitarian measures as being "non military" in the previous definition, his point about the use of the populace as a fifth column is well taken. As the United States continues to struggle with defining hybrid warfare, the emergence of techniques that encompass both the physical and cyber domain have created a formidable asymmetrical capability.

When Russia annexed Georgia's regions of South-Ossetia and Abkhazia in 2008, this was likely the first test case of the application of hybrid warfare. Since 2008, Russia has learned some valuable lessons in applying hybrid warfare. These lessons result in the adaptation of techniques of warfare that bears resemblance to traditional KGB and GRU tactics. The conflict in the Ukraine played out against a backdrop of political, economic, and ethnic tensions between the strong state actor, Russia, and the weak state actor of Ukraine within Crimea. The Ukrainian crisis positioned the Ukrainian government against Russian GRU, separatists, proxy fighters, and Russian ultranationalists (Hoffman 2014). This crisis illustrates the methods of hybrid warfare that Russia practices to create instability in the Ukraine. The Russian paramilitary separatists (through advisement from Spetznaz) gained asymmetrical superiority over the conventional Ukrainian military by asserting themselves against all elements of national power.

The current Ukrainian crisis traces back to events in 2004 when Viktor Yushchenko (leader of the Orange Revolution) won the presidential election over pro-Russian candidate Viktor Yanukovych. In 2010, Yanukovych would win re-election and sentence Prime Minister Yulia Tymoshenko to jail. Coincidently, Yulia was a leader of the Orange Revolution with Yushchenko in 2004. The situation in Ukraine spiraled out of control starting on November 21, 2013 when Yanukovych abandoned agreements for closer trading ties with the European Union in favor of closer ties with Russia.

After the Russian parliament decision to use force in the Crimea on March 1 2014, state-sponsored cyber units and groups of hacktivists initiated attacks on Internet infrastructure, conducted information warfare, and executed a DDoS attack (Paganini 2014). Russian state-sponsored cyber units conducted an infrastructure-IP telephonic attack on Ukrainian mobile phone infrastructure and disrupted the Ukraine's telecommunications system. This act effectively severed communications within the Ukraine and was considered an intolerable act of war by the Ukrainian government. This set the conditions for Russian paramilitary separatists to seize telecommunication offices from Ukrtelecom, severing all communications. As the Ukrainian military became disconnected, Russian Spetznaz would secure key infrastructure and relinquish control to the paramilitary separatists (Duggan 2015). The goal was to segregate the Crimea from the Ukraine—the separatists succeeded through the use of DDoS attacks on networks, the seizure of telecommunication facilities, and the physical damage of fiber optic cables or jamming of signals – the entire communications network was shut off. Crimea had only one Internet Exchange Point (IXP), which made this a vulnerable and easy target for Russian cyber units (David Talbot 2014).

The Ukraine is layered in tens of thousands of miles in fiber optic cable, connecting the country to all of its adjacent neighbors. The country has eight Internet Exchange Points (IXP); however, the sliver of the Crimea was left vulnerable with only one IXP, leaving the region susceptible to cyber attacks. A Russian cyber weapon known as Uroburos is believed to contribute to the preliminary cyber attack. Uroburos is an "advanced rootkit…[that] is used to infect networks belonging to high-level targets, stealing data after setting up rogue P2P networks" (Paganini 2014). The characteristics and references left behind in the rootkit source code indicate a sophisticated state-sponsored Russian malware. Capable of spying on every machine infected and jumping air-gapped computer networks, Uroburos was able to transmit data continuously (Paganini 2014). This capability allowed Russia to gain invaluable insight into Ukrainian military operations in the Crimea and ultimately severed communication with the rest of the Ukraine.

As the events were transpiring in cyberspace, they were also playing out in the physical domain. The disruption of the physical and virtual layer of cyberspace acted as a prologue to kinetic military action. Russian Special Forces previously referred to as *Spetznaz* were on the ground, operating independently of conventional Russian forces, advising and coordinating kinetic attacks through the Russian separatists. It is highly likely that the clandestine Spetznaz teams entered the country years in advance, assimilated with the populace, and began to foment provocateurs shortly after the events in Georgia in 2008. Operating under the guise of mercenaries or paramilitary separatists, their goal was to induce anxiety and outrage among local populations in order to generate a genuine indigenous protest movement.

The clandestine physical attacks were being coordinated in conjunction with cyber attacks—demonstrating "masterful Unconventional Warfare tactics" (Duggan 2015). Russia's ability to merge Spetznaz operations with cyber operations illustrates the hybrid warfare model. The *2014 Quadrennial Defense Report* stated that Russia is exploiting "rapidly mobile and well-equipped special operations forces with coordinated political warfare and cyberspace capabilities" which is a rendering of hybrid warfare (United States Institute for Peace 2014, 19–20). Hybrid warfare's evolution has transformed the fabric of the battlefield from vast plains of land to the cyber domain: a land without borders or boundaries. Russia's ingenuity in cyberspace resulted in a novel approach to a cyber-enabled UW operation to destabilize Crimea. Like most masterpieces, hybrid warfare is something that cannot be drawn or painted overnight--it takes an extensive amount of time to appreciate it fully.

Demonstrating hybrid warfare's effectiveness to an even greater extent, Russia employed all means of cyber capabilities during the most recent disinformation campaign to lend credibility to Moscow's intentions, including ideological, political and socio-cultural sabotage; provocation and diplomatic activity. Information warfare was waged against the population in order to destabilize a region over a period time. The goal of information warfare is to utilize methods in order to subordinate societies in other countries through both secret and overt channels, psychological operations, and political sabotage. Russian Information Operations (IO) was designed to create anxiety and outrage populations, uniting ethnic Russians in Ukraine. Vladimir Putin was willing to create a genuine indigenous uprising regardless of the timeframe, which is why the events in the Crimea were effective (Ambinder 2014). The list of those who developed the disinformation mechanisms reads like a Russian Who's Who. General Aleksandr Mikhailov, former head of the FSB's Directorate, stated, "information warfare is comprised of virtual and physical elements responsible for blocking the opposition influence" (Darczewska 2014, 24). This led to success in Crimea by convincing the population that the 'black' propaganda was legitimate regardless of whether it came in the form of a poster or tweet. Russia's utilization of online propaganda efforts was the key instrument in their online campaign, targeting geopolitical rivals such as the US and NATO. The Russians understood the importance of using cyberspace and developed a strategy that targeted elements within the Ukraine and the international community. The conflict in the Crimea demonstrates how hybrid warfare combines a robust information warfare strategy in conjunction with cyber and special operations.

The information warfare strategy of the Russian propaganda campaign against the Ukrainian government demonstrates the importance of cyberspace. The Ukrainian diaspora and members of the international community were inundated with misinformation and psychological messaging that left them defenseless. As reported in *Analysis of Russia's Information Campaign against Ukraine,* Russia's control over the mass media was effective in controlling the narrative against the Ukraine (NATO StratCom Centre of Excellence (COE) 2014, 3). Television was used to alter perceptions by framing the Ukrainian problem in line with Russian strategic objectives. Furthermore, the use of social media and fabricated news reports firmly changed opinions to favor Russia. The overarching Russian narrative focused on the following: the Russian Slavic Orthodox opposition to the Euromaidan (fascist, Nazi, nationalistic) Europe; promoted Ukraine as integral to the Eurasian Economic Union; unification of all Slavs under a Russian Federation; sparked hate against the European Union objectives, and promoted legitimacy and justification (NATO StratCom Centre of Excellence (COE) 2014, 4). Russia understands their target audience; more importantly Russia understands how to leverage deception, information and psychological operations through social media propaganda to achieve effects.

The exploitation of social media has primarily been focused on deception and disinformation. Russia restricts access to media sites that are considered pro-Ukrainian sources and uses the popular social networking website *VKontakte* to target Russian Opposition movements. Another novel use that fits into the disinformation ampoule is referred to as "internet trolling." This is a practice entailing GRU use of social media and well-known bloggers to spread a favorable Russian narrative and drown out the opposition voice[11]. Russia has been known to create troll farms that are responsible for posting comments and blogs that marginalize the opposition message. The trolls are primarily focused on spreading disinformation through social media campaigns and hash-tag (#) Twitter movements. Social media has also become a proving ground for deception and fabrication capable of being tweeted or shared with millions of people.

[11] "An internet troll is a person who foments discord online by starting arguments or upsetting people, by posting inflammatory, extraneous, or off topic messages in an online community with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion" (NATO StratCom Centre of Excellence (COE) 2014, 29).

This was witnessed by the story produced by the Russian *TV Channel One*, spreading through *Youtube*: an eyewitness account of a 3-year old boy being tortured and crucified by Ukrainian military in Slovyansk. Local residents denied that this atrocity ever occurred, especially since the town in which it was supposed to have happened does not have a public square (NATO StratCom Centre of Excellence (COE) 2014, 31).

The initial IO technique applied during the Ukrainian crisis can be labeled influence blocking, which is a form of special propaganda that targets social groups. The Russians were able to capitalize on enduring propaganda, which started years ago (learning from mistakes in Georgia). Secondly, they conveyed information that people desired to hear, versus what was accurate. Russia was able to convince the Russian speaking population of the Crimea that Russia was in the Crimea to protect people's rights. They were able further to incite emotional agitation and the mob mentality when they conducted misinformation about the Ukrainian ban on the Russian language. The next noteworthy technique was the application of direct and obvious messaging. Polarizing messaging conveyed the Russian Spring as patriotic, portraying the world in black and white terms. This propaganda intimidated and provoked people against each other by declaring that they were either for or against the Russian government "WE know if you are against US." This messaging was reminiscent of cold war tactics and used hateful language, obscenities, and painted a picture of a malignant world. The most savvy and ingenious use of disinformation was simply to call the Russian paramilitary forces (most likely Spetznaz) "nice men." Who could resist if they encouraged peace (Paganini 2014)? Hybrid warfare seduced Ukraine into a prolonged battle at a distance (cyberspace and technology) in order to draw them into a close-range battle when they are defenseless.

The crisis in the Ukraine is the first contemporary example of a holistic asymmetrical strategy being applied in both cyberspace and in the physical domain. The Ukraine was the largest cyberwar battlefield since the 2007 cyber attacks in Estonia (NATO StratCom Centre of Excellence (COE) 2014, 38). Secured communications were hacked to show the weakness in western technology and divide international support for the Ukraine. Telecommunications were severed; DDoS attacks took down government websites; cyber attacks penetrated the financial and military institutions causing civil unrest. This hybrid warfare is waged by focusing on the following key characteristics: "escalation, dominance, speed, momentum and deception" (NATO StratCom Centre of Excellence (COE) 2014, 34). Secondly, Russia demonstrated a mastery of Unconventional Warfare by preparing and setting the conditions for kinetic activities by controlling the dissemination of the strategic narrative. The heavy reliance on IW is attributed to the following characteristics mentioned in the *Analysis of Russia's Information Campaign Against Ukraine:* Target Audience Analysis, controlling the narrative in social media, manipulating the social, political, economic conditions and mental changes being achieved through manipulation, and the use of SOF on the ground physically to spread this IO narrative (NATO StratCom Centre of Excellence (COE) 2014, 34). Russian Spetznaz further complimented this hybrid strategy by conducting subversive clandestine actions that supported the propaganda narrative and disrupted the government legitimacy of the Ukraine. The Spetznaz also carried out traditional UW activities such as developing auxiliary support with local pro-Russian sympathizers, creating auxiliary supply chains for smuggling weapons, organized paramilitary separatist operations, and disseminated tailor-made IO narratives (NATO StratCom Centre of Excellence (COE) 2014, 38). Despite the elaborate efforts by the Spetznaz, the Russian takeover of the Crimea could not have occurred without information superiority in cyberspace.

This strategy quickly became tethered to the phrase 'hybrid warfare,' although General Valeriy Gerasimov refers to this as "non-linear" warfare. This strategy includes the use of technologic advances or "weapons of new physical principles" in order to gain a battlefield superiority over another through a non-contact or network-centric methods (Roger McDermitt 2014). The Russian term "*Maskirovka"* exemplifies the application (how) of hybrid strategy through the following: surprise, camouflage, maneuvers intended to deceive, concealment, the use of decoys and military dummies, disinformation to deceive" through any means necessary (Ash 2015). The question we should address is how we can learn from the Ukrainian conflict by integrating technological advances into SOF doctrine.

Case Study of Stuxnet Operation in Iran

Cyberspace is now a common domain for international conflict. The idea of cyber warfare taking place in the distant future is a fallacy-- cyber warfare is happening now. When examining Stuxnet, there are thousands of pages that detail the complexity of the Stuxnet virus and countless hours of discourse pertaining to its development and attribution. For the purpose of this case study, the intent is to focus on the capabilities and tradecraft of the virus and methodology for employing Stuxnet. Stuxnet is referred to as a "Frankenstein patchwork" of the best cyber attack weapons that resulted in the first recorded instance of a cyber weapon causing physical damage (Farwell and Rohozinski 2011, 4). Stuxnet was designed to penetrate and establish control of Industrial Control Systems (ICS) representing a new generation of 'fire and forget malware' that targeted impenetrable air-gapped systems[12]. The ICS were not connected to the Internet; therefore penetration required the use of intermediary personnel, equipment, software, companies, four zero-day vulnerabilities and malware updates for the payload to work as planned.[13]

Stuxnet's brilliance is that it leveraged vulnerabilities of all three layers of cyberspace, manipulating each layer for increased efficacy—this is the future of cyber warfare. Don't let this overshadow the fact that the worm borrowed through cyberspace, only targeting selected ICS based on their geographical locations and manufacturer. A recent report by the German Federal Office for Information Security (BSI) indicate that a cyber attack occurred in a German steel mill that disrupted an ICS to such a level that a blast furnace could not be properly shut down, resulting in damage (Zetter 2015). The attack occurred when cyber weapons infiltrated corporate networks through a spear-phishing attack, opening a malicious website loaded with malware that would subsequently be downloaded onto a computer. Once the malware gained access into a system, the cyber attackers were able to gain access into the industrial components of the production network—and effectively stopped production (Zetter 2015). As previously mentioned, there is no such thing as an impenetrable wall, only a difficult window. Nearly every cyber attack involves some form of tradecraft, techniques, and code; therefore it is important to understand how to mimic this pattern. For the purpose of this

[12] Air Gapped systems are not connected to the public Internet and penetration required the use of intermediary devices such as USB sticks to gain access and establish control (Farwell and Rohozinski 2011, 3)

[13] Zero Day Exploits are vulnerabilities previously unknown, so that there has been no time to develop and distribute patches (Farwell and Rohozinski 2011, 3)

case study, Kim Zetter's seminal research on Stuxnet was used as the backbone due to the conflicting and often misleading research by parochial research institutes.

On June 23, 2009, a destructive cyber attack was unleashed against the Iranian uranium enrichment program located at Natanz in order to sabotage Iranian control systems and preventing the construction of a Nuclear weapon. In June 2010, a Belarusian named Sergey Ulasen, working for a company called Virus-BlokAda discovered what would be known as Stuxnet. Upon initial discovery, Stuxnet was using a rootkit to hide itself from antivirus software, alongside a Zero-day exploit, so it could reproduce with any system with which it came in contact.[14] Zero day exploits are the WMD of cyber weapons. They attack undiscovered vulnerabilities within software and operating systems—meaning there are no known patches available to fix the attack vector or antivirus detection (Zetter 2014, 116). The kernel of an operating system that makes everything work—it is the center mass of a target. The use of a kernel rootkit added further complexity to the cyber weapon since this was hidden out of the purview of anti virus software. Since most virus scanners only scan the outer layers of operating systems where users operate software, the kernel rootkit undermines detection. The purpose of the rootkit was to hide four additional files within the operating systems—known as .LNK. LNK files instruct the PC to automatically to scan and show the contents of a USB drive when inserted into an electronic device. When a USB drive is inserted into the computer, a list of files is generated by the .LNK to show the user visually what contents are on the USB. Once the USB was inserted into a computer, the exploit housed inside of the .LNK surreptitiously deposited the virus onto the Windows operating system

[14] Rootkits come in several varieties, but the most difficult to detect are kernel-level rootkits, which burrow deep into the core of a machine to set up shop at the same privileged level where antivirus scanners work (Zetter 2014, 137)

(Zetter 2014, 157). This was the first of five Zero day exploits, and showcased the importance of understanding your target's networked infrastructure. The cyber weapon exploited every version of Windows operating systems since 2000 and contained four different versions of .LNK to ensure it properly infected everything (Zetter 2014, 166).

The efficacy of Stuxnet relied upon vulnerabilities in the virtual domain, specifically the legitimacy of the networked security architecture. Software security is based on private cryptographic keys and digital certificates to ensure legitimacy of the software. The digital certificates are trusted security documents that are used to authenticate programs and show their trustworthiness—in essence it is a seal of authenticity. However, Stuxnet used a legitimate digital certificate to authenticate malicious files undermining the trustworthiness of any files signed with digital certificates thereafter—fooling computers into thinking malicious code is legitimate code. It was discovered that the digital certificates from Relatek and JMicron, two semiconductor companies located in Taiwan, were the two certificates used to deliver the attack codes—it also shows the importance of the physical domain in cyberspace (Zetter 2014, 232). Once the superficial surface of Stuxnet was removed, the true deviance of the virus became known: this was a malware focused on espionage. Stuxnet was crafted to search for two Siemens proprietary software programs installed on machines--SIMATIC Step 7 or SIMATIC WinCC. These programs are part of an industrial control system (ICS) designed to work with Siemens programmable logic controllers (PLCs) (Zetter 2014, 246). These software programs are used as interfaces between a manufacturing device and a computer to make the device work with the machine.

Stuxnet was fifty times larger than the typical virus of 10-15 Kilobytes, highlighting the complexity of the code and payload. Within Stuxnet a large dynamic link library (.DLL) file was discovered that contained another layer of .DLL wrapped up in encryption like “Russian nesting dolls.” This was in addition to a configuration file that allowed attackers to change the external communication pathways of computers infected with Stuxnet. The genius of Stuxnet was that if a computer system did not contain the targeted Siemens software, it would remove itself from the computer—minimizing signature and bandwidth. Stuxnet would further store its malicious code inside the flash memory of a system, out of view from antivirus software. Furthermore, Stuxnet reprogrammed part of the Windows operating system to include Stuxnet on all processes being executed on a machine. When antivirus software became suspicious of the Stuxnet code, it would convince the Antivirus software the file locations in question were empty and contained no threat.

The genius of Stuxnet was that data was deposited into a sinkhole that allowed attackers to collect real-time data on Stuxnet’s discoveries_(Zetter 2014, 512). Stuxnet did not behave like a typical outbreak—it became apparent that this virus was specifically designed to focus on Iran. Of the first 38,000 infected computers, 22,000 were located in Iran and 217 of these computers contained the Siemens software (Zetter 2014, 517). Stuxnet was able to do this because it contains two parts—the delivery system responsible for spreading the virus and the payload, which performs the attack. Stuxnet’s payload was the malicious code that hunted the Siemens software and PLCs (Zetter 2014, 947). Once infected, Stuxnet would determine if the computer was 32-bit or 64-bit Windows. If a computer were 64-bit, Stuxnet would remove itself. Stuxnet was clever; it only wanted select computers with Siemens software in Iran. Secondly, it contained Zero Day exploits that took advantage of vulnerabilities in keyboard files to allow attackers to gain administrator rights and the printer spooler function that allowed it to spread between machines (Zetter 2014, 1647). Stuxnet contained four zero day exploits, characterizing it as a multi-tool of features. Stuxnet was a precision weapon that conducted reconnaissance for Siemens software attributed to the Iranian Nuclear program, sabotaged the S7-315 and S7-417 PLC of Siemens Step 7 machines configured in a manner known only to the Iranian Nuclear program (Zetter 2014, 3182). Stuxnet was sabotaging the PLC of the IR-1 centrifuges used at Natanz. The program increased the frequency of the converters to 1,410 Hz from 1,064 Hz, the breaking point of an IR-1 rotor. Any irregularities in a centrifuge's processes will result in an unexpected imbalance, causing it to spin out of control (Harrington and Englert 2014). Ultimately, Stuxnet would destroy over 1,000 Iranian centrifuges—casting doubt on their scientific ability for creating nuclear technology (Zetter 2014, 4485).

Stuxnet was designed to target specifically the illegal Iranian enrichment program located at Natanz, a small town 200 miles south of Tehran. Due to the geopolitical climate between Iran and the International Atomic Energy Association (IAEA), Iran established front companies to procure materials and technology for Natanz. The most notable front company was Kalaye Electric Company; it became the initial target of the Stuxnet virus that would eventually infect the Iranian Nuclear program. The Stuxnet employment scheme *theoretically* blended covert and clandestine services. Employment required detailed foreknowledge of the exact centrifuges, PLC's, SCADA, and computer software that was to be installed at Natanz as well as the configuration. This operation likely started as early as 2000, when the CIA recruited key suppliers of A.Q. Khan's nuclear supply channels (Zetter 2014, 5722). As previously mentioned, the cyber persona layer is the weakest link. Furthermore, it was discovered that in addition to Kalaye Electric, a company called Neda Industrial Group was responsible for procuring additional equipment. Discovering Neda's involvement was the Achilles' heel of the supply chain, since they were the *only* option to install Siemens software in Iran. To get Stuxnet onto the PLC at Natanz, it was now necessary to jump the air-gapped network; piggy backing onto the Siemens/Neda employee's computer that would eventually be connected to the PLC did this.

Since the PLC was the vector of attack for Stuxnet, four down stream companies with connections to Neda were targeted as a doorway through which to transport surreptitiously Stuxnet to Natanz. These four contractor companies were involved in industrial control manufacturing, assembly, and installation of industrial control systems. As in the U.S., government contracts are won by prime contractors, and then subsequently issued to sub prime contractors with less stringent standards and security. The three additional companies targeted were: Foolad Technique, Behpajooh, and Control Gostar Jahed. On July 22, 2009 confirmation of the infection occurred when a Neda control engineer posted on a Siemens user forum that computers were having problems with "Siemens Step 7 .DLL" (Zetter 2014, 6276) The icing on the cake was that he used an alias username, but signed his real name-- Mohammad Reza Tajalli, a control engineer specializing in control systems for the oil industry, according to his LinkedIn profile (Zetter 2014, 6546). At the end of the day Stuxnet infected ten patient zeroes at the aforementioned companies. Stuxnet replicated and spread to 12,000 other machines, of which 69% were linked to Behpajooh, likely due to an unwitting victim (Zetter 2014, 6546).

Stuxnet was a sophisticated virus that hunted down frequency converter drives that responded to a PLC computer command, regulating the speed of a centrifuge motor. The virus in itself is a work of brilliance, and took over two years to dissect fully. The purpose of including this case study is to realize where SOF's are able to integrate capabilities like Stuxnet on the battlefield. As detailed above, Stuxnet represents a perfect storm of all three layers of cyberspace being manipulated and exploited for a desired effect—slowing the Iranian nuclear program.

CHAPTER SIX

ANALYZING UNCONVENTIONAL WARFARE CAPABILITIES IN CYBERSPACE

This section will discuss how to employ cyberspace capabilities in support of an unconventional warfare campaign. By utilizing cyberspace, SOF lessens the risk to mission, risk to U.S. personnel, risk to collateral damage, risk to discovery and political fallout. This section advocates for the heavy reliance of cyberspace for unconventional warfare, but does not discount the importance of physical interaction. UW operations conducted under a veil of anonymity are essential in cyberspace, but certain elements of UW require hard power.

Acquisition of Advanced Capabilities

Before forming a mosaic of unconventional warfare cyberspace capabilities, there needs to be a brief discourse pertaining to the current acquisition process. This thesis is not advocating for the purchase of specific software, nevertheless it does advocate for a rapid fielding of technological capabilities that may be proprietary to industry. Technology is clearly outpacing policy and the acquisition process. Therefore, in order to sustain SOF's agility in all domains, USSOCOM must acknowledge our current acquisition dilemma, particularly considering that computational power is doubling at a rate of 18 months according to Moore's Law.

Following the failure of Operation Eagle Claw, which attempted to rescue fifty-two U.S. Diplomats hostages from Iranian control on April 24, 1980. Congress determined that there needed to be a single coordinating command; this would bring the Special Operations community under one hat and coordinate these types of missions. USSOCOM was created to ensure an expeditionary focus. Over time, the acquisition process has lost an expeditionary focus and gradually devolved into the traditional JCIDS (Joint Capabilities Integration and Development System) process. This stove piped process is a risk averse and milestone driven process that discourages rapid fielding.

Ostensibly, this process is designed by to prevent corruption and preclude undue command influence for a specific vendor; the result is in a multi-layered legal process—neither rapid nor creative—that benefits only the military industrial complex. By its very nature, the current acquisition process for emerging technology in cyberspace within SOCOM is now largely identical to the process used by the conventional forces—the introduction of groundbreaking capabilities to a PM represents risk rather than innovation. It should be noted that there have been recent attempts to expedite processes by pioneering the Joint Capability Technology Demonstrations (JCTD) and an internal Rapid Equipment Fielding (REF) element; however all of these initiatives fall victim to the lengthy acquisition process versus being cutting edge.

USSOCOM has a robust Research, Development, Test and Evaluation (RDT&E) budget of $427 million (USSOCOM Public Affairs Office 2013, 21). Of this budget, only fifteen percent ($28.7 million) is used for technology development (USSOCOM Public Affairs Office 2013, 21). The remainder of the budget is reinvested into established programs. From this author's perspective, a larger percentage should be allocated towards RDT&E that can be leveraged against industry initiatives in cyberspace. As such, USSOCOM could serve as a crowd funding initiative for specific emerging technology in collaboration with industry.

Methodology: Unconventional Warfare in Cyberspace

Phase I-Preparation

Wouldn't it be innovative to conduct this preliminary phase of UW from the security of a remotely located CONUS location when confronted with an operational that is denied or limited in accessibility? This section will demonstrate how SOF can accomplish the three key tasks of preparation without entering the UWOA. The initial phase of unconventional warfare begins with operational preparation of the environment that studies the physical and cyberspace domain of the UWOA. During this phase SOF conducts intensive analysis of populations to determine the potential success for resistance forces and to determine enemy capabilities. The second key task conducted during this phase is focused on resistance sponsors conducting psychological preparation to unify a population and the preparation of the environment to accept U.S. support (USAJFKSWCS (A) 2011, 1–8). Lastly, the preparation phase contains the intelligence preparation of the environment (IPOE) that analyzes a resistance movement's capabilities, weaknesses and predispositions for violation of Leahy Vetting requirements. By leveraging cyberspace to create a rich understanding of the environment, SOF is able to begin shaping that environment in parallel with activities in Phase I.

Similar to the techniques orchestrated by Russian hybrid warfare and ISIS utilization of social media, SOF can leverage cyberspace to accomplish these tasks. It must do so by conducting a thorough CIPOE of the UWOA (obtaining real time accurate assessments of resistance movements personnel strengths, logistical capabilities, tactics and operational tempo). The key to conducting *effective* Phase I tasks in cyberspace is to do so without attribution. It should be noted that the following capabilities and software are available commercially. However to use these without the security of air-gapped systems, Tor networks, VPNs and non-attributable hardware would violate OPSEC[15]. An example of violating this paradigm would be to use the same MAC Address, IP Address or social media profile to crowd source data from a target area *and* also use this same device to strategic messaging against an adversarial government. To most this seems like a benign error; however to foreign intelligence services, this highlights potential U.S. involvement due to the digital fingerprint left behind.

[15] Joint Publication 3-13.3, Operations Security outlines OPSEC as a systematic method used to identify, control and protect critical information and subsequently analyze friendly actions (Raymond, Cross, and Conti, n.d., 4).

Cyber operations are designed to prevent discovery; therefore it is necessary to prevent attribution that an activity is occurring, and even more important is the identity of sponsor (Raymond, Cross, and Conti, n.d., 4). A novice operator in cyberspace would advocate that encryption tools and firewalls preinstalled on government computers are enough for conducting CIPOE. Unfortunately, encryption only works to prevent disclosure of what was being said. Encryption does not mask the fact that the communication between two electronic devices occurred—in essence, a whisper was seen but not heard. In the context of Phase I activities, it is important to hide with whom we are communicating with and what we are doing. Tools that SOF cyber operators should use to protect OPSEC must prevent their IP addresses from displaying in the server log files inside authoritarian states and link resistance movements with whom they're working with. The solution to ensure anonymity is by utilizing a combination of Tor Networks and virtual privacy networks (VPNs). Tor is an "overlay network" that provides online protection against surveillance and traffic analysis (Friedman 2013, 109) and is commonly known as an "onion router" since it uses multilayer encryption. The overlay network is an additional virtual layer that rests on top of the Internet and functions as an encryption routing system (Friedman 2013, 109). The nodes of this virtual layer are user machines that are part of the network—the more machines connected, the more nodes available. Just like the already existent Internet packets that are used to transmit information, Tor consolidates that packets and encrypts each piece for greater security. The information is further encrypted, and then transferred from its point of origin to numerous other nodes prior to reaching its end-point. Tor uses an algorithm that bounces a message hundreds of time prior to reaching its end point, making it virtually impossible to determine the source of communication. Tor further adds anonymity by masking your IP address when surfing the Internet and piggybacks Tor message traffic on other message protocols such as Skype when end points are under surveillance. However, Tor is detectable due to characteristic network traffic and the ports used; therefore it is important to also to use a Virtual Private Network (VPN) to remain anonymous.

A VPN enables an electronic device to communicate on a public network as if it were connected to a private network, while benefiting from the increased security of the private network. A VPN provides a secure method for encrypting and encapsulating private network traffic and moving it across a public network. This methodology increases anonymity and masks users true identity. The most robust VPN is from a commercial company called “hide my ass” (HMA) which is based out of London. HMA can be used to access region restricted websites and material, bypassing network filters to social media in autocratic countries, and prevent unauthorized access into your computer by criminal ISPs. HMA boasts a global network of 831 servers located in 172 countries, with 111,612 IP addresses (Privax Ltd. 2014). The VPN works by disclosing to a website an IP address for the VPN provider instead of the machine being used. This prevents information from being traced back to your machine. An additional layer of anonymity offered by a VPN is that since there are hundreds of servers; you can cycle through VPN server location to further obscure your location. With your anonymity secured through a VPN and Tor network, CIPOE will be achieved with greater efficacy.

Cyber Intelligence Preparation of the Environment (CIPOE) offers SOF the unique capability of identifying resistance leaders, movements, operations and capabilities by analyzing social media along with their electronic communications. As stated by the United States Special Operations Commanding General, General Joseph Votel, "Social media is another component of unconventional strategies, and the security environment in general...we must therefore develop our ability to interact with key influencers through this medium, or else risk blinding ourselves" (Gertz 2015). By using Facebook, Twitter, YouTube, VK, and other regional social media platforms, SOF can have access to the cyber persona layer of cyberspace in an otherwise denied physical environment. The initial step in creating this capability is by conducting digital operational preparation of the environment (DOPE)—a technique that resembles crowd mapping but requires additional software to generate greater detail. Scrolling through each individual kilobyte of information across numerous social media platforms is time consuming; therefore SOF operators need to be skilled, trained, and equipped in the field of advanced social media analytics.

The first layer of tools should be considered a set of triage instruments for an emergency room. DOPE should be conducted on an unclassified commercial network versus piped into an air-gapped system by hand carrying DVDs since information changes with a moments notice. A SOF cyber operator needs to determine the fidelity of the information versus automatically deep-diving into a data set of social media information. This triage can be conducted with tools such as *Hootsuite*, *Social Harvest*, and *Trackur* to crowd map the topography of social media, since sifting through billions of accounts is like searching for a needle in a haystack. These tools are able to aggregate massive amounts of publically available data for any trends and links. The marketing tools mentioned above are designed with the analyst in mind. Hootsuite offers analysts the ability to monitor conversations across the globe or within a neighborhood and broadcast exactly where your audience is located. It also has the capability of listening in multiple languages, monitor emerging trends based on conversations, and identify on-line social media influencers (Hootsuite Media Inc. 2015). *Trackur* behaves similarly, but provides additional insight into sentiment analysis and influencer scoring.

The second layer of DOPE involves a further refinement of the information harvested from the first layer. This layer uses an additional toolkit and methodology for greater analysis. Before operators 'click' on the additional tools additional option, a SOF digital operator must exploit the data by 'Google dorking' the mined information. Google Dorking was previously mentioned; nevertheless to add further clarification of how Google can be used, here is an example. If an operator is interested in a particular website and needs to identify all members associated with that website, they need to modify the Google Dork "*intitle:"index of" members OR accounts"* for that website and hit "search" on the Google search engine. Once Google Dorking is exhausted an operator can switch over the tools associated with the second layer, which are *OpenIO*, *Maltego*, and Endgame's *Crunchy Panda* and *Light Storm* software. The mastery of these tools allows SOF operators to scan and data mine social media for individual faces, sifting through millions of online postings for an image of a single person. Social media's prevalence worldwide operates as an interconnected sensor, allowing anyone anywhere to post a picture, therefore geo-locating an event or person without their knowledge. *OpenIO* culls information and geo-locates the social media post onto a map. Moreover, *OpenIO* traces a relationship between users and illustrates how that relationship evolved over time. The most noteworthy feature for use in DOPE is the program's ability to track a person's location based on their location-based services for their smartphones.

Maltego is a cutting-edge platform that provides a threat picture of an environment by highlighting the complexity of electronic relationships that exist within a problem set by aggregating data from all over the Internet. The difficulty in information gathering is ensuring that you collect the right information. Maltego removes the guesswork in DOPE by conducting a digital reconnaissance of a target—thereby identifying a digital fingerprint. *Maltego* is open source intelligence and forensics application that mines and analyzes information as well as graphically illustrating its findings. (Paterva 2011). Maltego takes various bits of information and converts these to other entities such as a web address to an IP address. The program is able to accentuate otherwise unrecognized relationships into a comprehensible graphic that illustrates how everything is connected (network analysis). *Maltego* determines the real and virtual world links between people, social media accounts, documents, electronic devices and Internet infrastructures. This is a complete network analysis tool that is essential in targeting online activity.

The last tool and most robust capability for DOPE is Endgame's suite of OPE tools known as *Light Storm* and *Crunchy Panda.* These tools provide SOF operators the edge over adversaries by supporting the entire cycle of information gathering and operational planning—thereby creating an adversarial digital thumbprint in cyberspace. The Endgame suite of tools enables SOF operators to have an unrestricted view of a target device. These tools are used to dissect a target device for any security exploits along with mapping out an adversary's network worldwide. For example, you can discover the country, industry, or adversary specific software or operating system that is running on a target machine by peeling back the layers of their network. Furthermore, you can discover that a cellphone or other electronic device purchased in an autocratic state is operating in a different region—indicating that this person is susceptible to social engineering. Regardless of the manufacture or software developer, these capabilities were leveraged in the case studies; therefore are necessary for SOF in cyberspace.

Phase II-Initial Contact

The Initial Contact Phase of unconventional warfare is the most dangerous phase of the operation due to the quantity of uncertainties. During this phase, Special Forces and Other Governmental Organizations (OGA) establish contact with resistance organizations to assess the compatibility of U.S. and resistance interests and objectives (USAJFKSWCS (A) 2011, 3–3). Additionally, teams conduct a detailed area assessment and human terrain analysis to expand their understanding of the operational environment. Concurrently, during this phase Military Information Support Operations (MISO) are conducted to gain popular support for the resistance, recruit additional support, and undermine the legitimacy of the oppressive government. No longer is physical ‘link-up’ necessary, these tasks can be achieved in cyberspace, thereby reducing risk to U.S., OGA and resistance forces. SOF operators can initiate virtual relationships from the cyber personas discovered during CIPOE analysis. No longer is SOF restricted by an access limited or denied area, through the use of cyberspace—initial contact can take place in parallel with other phases of UW without leaving CONUS.

The use of cyberspace favors SOF by providing an anonymity and non-attribution. Furthermore, social media operates on the backbone of legitimate state sponsored networks. If state networks block access to the Internet sites, they will disrupt commerce, which delegitimizes their already fragile governance. Using the aforementioned social media tools, SOF operators can exploit the intelligence gathered from CIPOE to identify a resistance leader that is more likely to act in interest of the U.S. strategic objectives. By analyzing a potential resistance movement's network and their online activity, Leahy vetting concerns and human rights violations are potentially identified by their online communiqué and You Tube videos. Once an accurate operational assessment is made of the resistance movement, two-way communication or *initial contact* can occur through a variety of on-line social media platforms such as Skype, Second Life, or even Internet Relay Chat (IRC).[16]

Phase III-VI-Organization, Buildup and Employment

The next three phases will be encapsulated into one section, since through the use of cyberspace, each of the phases can occur analogously to the other. The key tasks accomplished during Phase IV-Organization include, organization and development of resistance movements in order to expand operations. During this phase an insurgency is organized trained and equipped into an auxiliary, underground and guerilla force. SOF units are tasked to develop the capability of resistance movements by creating a command hierarchy that compliments already existing cultural, regional or religious structures. Additionally, SF units are tasked with organizing an area complex that include tactical bases, intelligence systems, communication systems, logistical support

[16] Internet Relay Chat (IRC) is an application layer protocol that transfers messages via one-to-one communication through private messaging in the form of text.

systems and training area (United States Army John F. Kennedy Special Warfare Center and School 2008, 5–3). During Phase-V Buildup, the emphasis is placed on expanding the capabilities of the resistance movement by focusing on recruitment, logistical support and training. As stated in unconventional warfare doctrine, "buildup of forces is counterproductive if the irregular force does not obtain enough resources to support and sustain the buildup," therefore an emphasis is placed on logistics (United States Army John F. Kennedy Special Warfare Center and School 2008, 5–5). Phase VI-Employment typically involves combat operations. During this phase SOF advises and assists resistance movements during kinetic operations and focuses efforts to drain an adversarie's morale and resources through military operations (United States Army John F. Kennedy Special Warfare Center and School 2008, 5–6). Operating outside of the restrictive parameters of the physical domain, *The Ghost in the Machine* is capable of blending UW with cyberspace to improve the efficacy of kinetic military action.

The Islamic State in Iraq and Syria (ISIS) has shown a mastery of technology for coordinating operations, recruiting, dissemination of propaganda and inspiring sympathizers across the globe. The terrorist organization's social media presence topped 46,000 Twitter followers in late 2014 and has almost doubled to 90,000 followers in March of 2015. Two thousand of these accounts are organizers for ISIS (Trujillo 2015). Special Operations Forces are capable of achieving similar on-line presence during an unconventional warfare campaign by embracing digital innovation cyberspace. In order for SOF to organize resistance groups we must modify our mindset of the logical framework of the physical domain to a virtual comprehension of who is considered the guerilla force, underground, and auxiliary. In cyberspace, social media activists and independent bloggers who are capable of reaching the corners of the globe with one Tweet augment the auxiliary. The underground composition shifts from a physical person to a virtual connection; every electronic device and virtual action becomes a sensor. The guerilla force is no longer comprised of astute military aged males armed with 7.62 bullets, soviet era grenades and explosives; they are hackers whose weapon of choice is an OSX or Linux operating system. Despite the importance of unconventional warfare in cyberspace, there is still a requirement to have a traditional presence in the physical domain. For true efficacy, unconventional warfare must be viewed as a confluence between cyberspace and physical space, where operations are synchronous between the two. Cyberspace is used to enhance the Special Operations missions.

Akin to how social media was leveraged throughout the Arab Spring uprising at Tahrir Square, SOF can expand a resistance range of influence across geopolitical borders while reducing risk to exposure in a limited access area through social media. An evolution in communication through technological advances necessitates the employment of social media for unconventional warfare. Furthermore, this section laments that the organizational task of *training* does not need a traditional environment to be successful. The asymmetrical nature of the digital battlefield offers numerous options for virtual training. A scalable training program can be accomplished through the novel use of You Tube, Vine and video game systems. During the organizational phase of UW in cyberspace physical currency and material resources are replaced with the emergence of Bitcoin and crowd funding.

The global popularity of You Tube, Pinterest, and Instagram offer a discrete technique to train resistance movements during an unconventional warfare campaign with marginal risk to exposure. Tactical training videos are uploaded into the public domain by fictitious user profiles, capable of being shared across an entire guerilla force within minutes.

An often-overlooked capability of social media is the ability to use the world's population of over six billion inhabitants as a source of income through crowd funding. A technique reserved for raising funds for start up entrepreneurs can now be used to raise digital currency for a resistance movement. Just like the latest technological innovation—the loftier the donation equals the greater chance of success for resistance movements. Bitcoin mining techniques also showcase the possibility of anonymously raising and allocating funds in cyberspace. The most innovative use of Bitcoin would be to train resistance movements to surreptitiously mine Bitcoin. The Bitcoin mining technique in itself is dubious. In the typical traditional monetary system, governments print money when needed. Bitcoin mining substitutes this process by discovering virtual Bitcoins through a decentralized mining process, placing them into circulation. The mining process is where transactions are verified and added to the public ledger also known as a block chain (Kelleher 2015). Once a transaction is added to a block chain, a new Bitcoin is released into circulation. The profitability of mining is dependent on the price of Bitcoin, block reward for solving the computational puzzle, and the size of the transaction fees (Kelleher 2015). Another possibility is the ability to trade Bitcoins based on the exchange rate of physical and virtual currency. Quintessential to the mining process is the anonymity of Bitcoin.

The possibilities for social media during *Phase V-Buildup* are without bounds. The snowball effect of social media during the Arab Spring is the most notable example of the power of social media. Social media's profundity is linked to its "effect on individuals, and even the idea of individuals, have induced an environment increasingly conducive to digitally-enhanced collective action" (Burnore 2013, 33). Social media is changing how we communicate. When added to a resistance movement, there is a formula for success because people become empowered by a Tweet, invoking a primal desire for social networking. According to Burnore, "mobile technology and digital social media are penetrating the most isolated, autocratic and economically deprived areas in the world, the applicability of social media in UW campaigns increases in a parallel fashion" (Burnore 2013, 60). As previously noted, the use of social media to create a unified network based on common objectives, structure and leadership is worthwhile for use in UW. Social media is the agent to fuse online activities by galvanizing a resistance into a common cause that spills over into the physical domain. The manipulation of an ideology on Facebook has the potential for achieving strategic effects.

During *Phase-VI Employment*, computer network operations (CNO) in the form of computer network attacks (CNA) are to be employed by SOF operators to shape the physical domain. These capabilities are able to disrupt, degrade, or deceive and enemy's command and control (C2), activities essential to a successful UW campaign (Knapp Jr 2012, 17). The previous example of Russian hybrid warfare is a clear example of the physical effects computer networked attacks (CNA) can have on the physical domain. Due to the restrictions of Title-10 activities in cyberspace, these attacks must be within a threshold of unconventional warfare (UW); therefore operations like Stuxnet are not something ARSOF will be conducting. Within the confines of UW, SOF is capable of employing a series of capabilities in cyberspace for localized effects in conjunction with kinetic action.

The first application of SOF employment of cyberspace in UW is characterized by Endgame's *Pinnacle* capability, which allows SOF to operate stealthily anywhere in the mobile world. During the employment phase, the UWOA is generally categorized as a denied environment with a significant risk of discovery from government forces. *Pinnacle* converts your standard commercial off the shelf (COTS) smartphone to avoid tracking near a sensitive location by determining when and where a phone a SIM card will attach to a network and altering the dynamically changing the International Mobile Equipment Identity (IMEI) (Endgame Incorporated 2015). This modification of smartphones makes it possible for any user, whether SOF or from the resistance movement, to disappear from the network through an elaborate use of geo-fencing. The beauty of Pinnacle is not stealth, but the ability to conduct DDoS. Capabilities like *Pinnacle* deserve consideration for adding to the repertoire of SOF in Cyberspace.

An emergence of technological advances can be employed to enhance an UW campaign when the political environment does not permit the presence of U.S forces in combat operations. An example of the cyber persona layer of cyberspace bridging the gap between the operational restraints and limitations on the battlefield and strategic objectives is *Virtual Accompany (VA)*. The intended use of this composite of COTS hardware and software is to "track, communicate, and transmit relevant information" with partnered nation (PN) forces while US forces are operationally limited (Hanlon 2015). In essence, VA augments the *physical* need to advise and assist during kinetic operations. During combat operations SOF is able to monitor PN forces location and remotely assist the operation through the expanded use of technology and cyberspace (Hanlon 2015). Virtual Accompany becomes a PN forces ‘right hand man.’

CHAPTER SEVEN

CONCLUSION

Currently, there are 20 billion devices connected to the Internet, this number is expected to reach 40 billion by 2020 (Turner et al. 2014, 2). The new IPv6 Internet protocol will allow 3.4×10^{38} device connections—essentially everything will be interconnected (Deering 1998). With the number of devices, ranging from automobiles, home appliances, and cell phones being linked to the Internet daily, why should SOF *not* leverage this to their advantage? Special Operations should have the ability to operate freely within cyberspace as part of an unconventional warfare campaign. The research question of this thesis was how can Special Operations Forces (SOF) employ technological advances in cyber tools and networked social media to coerce, disrupt, or deter adversaries, thereby defining their role in cyberspace. This thesis answered the question by displaying a reflection of how cyberspace is being used by adversaries along with the theoretical use of technology in a UW campaign.

As identified earlier, the goal of this thesis was to define *The Ghost in the Machine* by showing a reflection of how cyberspace is currently being used by examining the case study of Stuxnet and Russian hybrid warfare. These bipolar case studies were carefully chosen to illustrate the wide-array of options that cyberspace can be used to achieve effects in support of UW. The Stuxnet case study defines a discrete capability that relied on an exquisite payload, though its success relied on the human domain. On the opposite end of the spectrum, Russian hybrid warfare is a mosaic of information warfare, unconventional warfare and DDoS to achieve strategic effects. Nevertheless, the recent use of social media by ISIS for mobilizing, communicating, recruiting, and disseminating propaganda falls somewhere in the middle of these two case studies.

All of these examples provide an opportunity for SOF in cyberspace. Moreover, this thesis outlined the legal framework in which Title 10 Special Operations Forces are legally able to conduct unconventional warfare and further demystified the physical and virtual framework of cyberspace. By using the aforementioned case studies, legal parameters, capabilities and examples, this thesis has created a tidy container in which SOF can operate within cyberspace. By using Special Forces Unconventional Warfare (TC 18-01) and Army Special Operations Forces Unconventional Warfare (ATP 3-05) this research highlighted the applicability of cyberspace for UW. Never before has SOF possessed the capability to conduct elements of unconventional warfare from the security of a team room—thousands of miles away.

While it was not mentioned, this thesis acknowledges that there is training currently being conducted to allow SOF to operate in cyberspace. However, this training is not part of the SOF repertoire of doctrinal training nor is the software. Further research is needed to explore the legal authorities for the utilization of cyberspace for Special Operations. As revealed by Colonel Knapp in 2012, Special Operations may require their own set of authorities to conduct a offensive cyberspace operations (OCO) in support of unconventional warfare (Knapp Jr 2012, 26). Keeping with Colonel Knapp's assessment and recent comments by the head of the NSA, Admiral Rogers, U.S. policy for operations in cyberspace must parallel technological advances. The legislation that dictates accountability between the DoD and intelligence community is outdated and requires revision to meet the current threat. Through executive orders—a clearer picture of *The Ghost in the Machine* will appear.

BIBLIOGRAPHY

§ 403–5. 2006. *U.S.C.* Vol. 50.

§ 413b. 2006. *50 U.S.C.*

Aftergood, Steven. 2014. "Offensive Cyber Operations in US Military Doctrine." *Federation Of American Scientists*. Accessed November 16. http://fas.org/blogs/secrecy/2014/10/offensive-cyber/.

Alexander, Keith. 2013. "Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee On Armed Services." Senate Committee on Armed Services.

AlSayyad, Nezar. 2015. "Virtual Uprisings: Tahrir Square." presented at the Global Cities Conference, Duke University, February 5.

Ambinder, Marc. 2014. "Russia Masters the Art of Clandestine Warfare against Ukraine." *The Week*. April 8. http://theweek.com/articles/448131/russia-masters-art-clandestine-warfare-against-ukraine.

Ash, Lucy. 2015. "How Russia Outfoxes Its Enemies." *BBC News*. January 28. http://www.bbc.com/news/magazine-31020283.

Blum, Andrew. 2012. *Discover the Physical Side of the Internet*. https://www.ted.com/talks/andrew_blum_what_is_the_internet_really.

Burnore, Nathanael O. 2013. *Social Media Applications for Unconventional Warfare*. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA598982.

Cartwright, James. 2011. "Memorandum for Chiefs of Military Services." Department of Defense.

Cleveland, Charles. 2014. *ARSOF Operating Concept 2022*.

Conti, Gregory, David Raymond, Tom Cross, and Michael Nowatkowski. 2014. "2014 6th International Conference on Cyber Conflict." In *Key Terrain in Cyberspace: Seeking the High Ground*, 357. Talinn, Estonia: NATO CCD COE Publications. www.ccdcoe.org.

D'Agostino, Davi M. 2011. *Hybrid Warfare*. Washington DC: DIANE Publishing. http://www.gao.gov/.

Darczewska, Jolanta. 2014. *Anatomia rosyjskiej wojny informacyjnej: operacja krymska--studium przypadku = The anatomy of Russian information warfare : the Crimean operation, a case study*.

David Talbot. 2014. "A Russian Info-War Is Under Way in Crimea." *MIT Technology Review*. March 14. http://www.technologyreview.com/news/525336/watching-for-a-crimean-cyberwar-crisis/.

Deering, Stephen E. 1998. “Internet Protocol, Version 6 (IPv6) Specification.” December. http://tools.ietf.org/html/rfc2460.

Department of Defense. 2013. *Joing Publication 3-12 (Restricted)*. Washington DC.

Department of the Army. 2011. *FM 3-0 Operations*. Washington DC: Headquarters, Department of the Army.

Duggan, Pat. 2015. “Strategic Application of Special Warfare in Cyberspace.” *Special Warfare* 28 (1): 25–27.

Endgame Incoperated. 2015. “Pinnacle White Paper.” Endgame.

Farwell, James P., and Rafal Rohozinski. 2011. “Stuxnet and the Future of Cyber War.” *Survival* 53 (1): 23–40. doi:10.1080/00396338.2011.555586.

Feakin, Tobias. 2013. “Playing Blind-Man’s Buff.” *International Journal of Korean Unification Studies* 22 (2): 63–90.

Finkle, Jim. 2014. “U.S. Government Probes Medical Devices for Possible Cyber Flaws.” Reuters. http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.

Friedman, Allan. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, USA.

Frizell, Sam. 2015. “Sony Is Spending $15 Million to Deal With the Big Hack.” *Time*, February. http://time.com/3695118/sony-hack-the-interview-costs/.

Gertz, Bill. 2015. “Inside the Ring: Special Ops Targets Social Media.” *The Washingtion Times*. March 18. http://www.washingtontimes.com/news/2015/mar/18/inside-the-ring-special-ops-targets-social-media/.

Hadnagy, Christopher. 2015. “The Official Social Engineering Portal.” *Security Through Education*. Accessed February 9. http://www.social-engineer.org/.

Hadnagy, Christopher, and Paul Wilson. 2010. *Social Engineering: The Art of Human Hacking*. 1 edition. Indianapolis, IN: Wiley.

Hanlon, Kelly. 2015. “Virtual Accompany User Manual.” WinTec Arrowmaker Inc.

Harrington, Anne, and Matthias Englert. 2014. “How Much Is Enough? The Politics of Technology and Weaponless Nuclear Deterrence.” In *The Global Politics of Science and Technology - Vol. 2*, edited by Maximilian Mayer, Mariana Carpes, and Ruth Knoblich, 287–302. Global Power Shift. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-55010-2_17.

Hoffman, Frank. 2014. “On Not-So-New Warfare: Political Warfare vs Hybrid Threats.” *War on the Rocks*. June 28. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Hootsuite Media Inc. 2015. “Listening.” *Hootesuite*. https://hootsuite.com/products/platform/social-media-listening.

Hurley, Matthew M. 2012. *For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance*. DTIC Document.

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA567618.

Joint Publication 3-05.1. 2007. Vol. 2. 3. Department of Defense.

JP 1-02 Department of Defense Dictionary of Military and Associated Terms. 2014. Washington DC: Joint Chiefs of Staff.

Kelleher, John. 2015. "What Is Bitcoin Mining?" *Investopedia*. http://www.investopedia.com/articles/investing/043014/what-bitcoin-mining.asp.

Kent, Allen, Fritz E. Froehlich, and Fritz E. Froehlich. 1990. "ARPANET, the Defense Data Network, and Internet." In *The Froehlich/Kent Encyclopedia of Telecommunications*, 1:341–75. CRC Press. http://books.google.com/books?id=gaRBTHdUKmgC&pg=PA341.

Knapp Jr, Everett D. 2012. *Unconventional Warfare in Cyberspace*. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA561663.

Lee, Doowan, and Glenn W. Johnson. 2014. "Revisiting the Social Movement Approach to Unconventional Warfare." *Small Wars Journal*, December. http://smallwarsjournal.com/jrnl/art/revisiting-the-social-movement-approach-to-unconventional-warfare.

Maron, Dina. 2013. "A New Cyber Concern: Hack Attacks on Medical Devices." *Scientific American*. June. http://www.scientificamerican.com/article/a-new-cyber-concern-hack/.

McCulloh, Timothy, Richard Johnson, and Joint Special Operations University (U.S.). 2013. *Hybrid Warfare*.

McNeilly, Mark R. 2014. *Sun Tzu and the Art of Modern Warfare*. Oxford University Press.

NATO StratCom Centre of Excellence (COE). 2014. *Analysis of Russia's Information Campaign Against Ukraine*. NATO.

Niekerk, Brett van, Kiru Pillay, and Manoj Maharaj. 2011. "The Arab Spring| Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective." *International Journal of Communication* 5 (0): 11.

Nielsen, J. N. 2014. "Hybrid Warfare." *Grand Strategy: The View from Oregon*. October 7. https://geopolicraticus.wordpress.com/2014/10/07/hybrid-warfare/.

Paganini, Pierluigi. 2014. "Crimea – The Russian Cyber Strategy to Hit Ukraine." *InfoSec Institute*. March 11. http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/.

Parker, Tom. 2004. *Cyber Adversary Charcteriszation: Auditing the Hacker Mind*. Rockland, Mass.; Oxford: Syngress ; Elsevier Science.

Paterva. 2011. "Maltego Version 3 User Guide." Paterva.

Peterson, Dale. 2013. “Offensive Cyber Weapons: Construction, Development, and Employment.” *Journal of Strategic Studies* 36 (1): 120–24. doi:10.1080/01402390.2012.742014.

Petit, Brian. 2012. “Information Operations Newsletter.” *Special Warfare*, June, 8.

Privax Ltd. 2014. “VPN: Nuts and Bolts.” *Hide My Ass*. September. https://www.hidemyass.com/how-vpn-works.

Raymond, David, Tom Cross, and Greg Conti. n.d. “The Library of Sparta.”

Rid, Thomas, and Peter McBurney. 2012. “Cyber-Weapons.” *The RUSI Journal* 157 (1): 6–13. doi:10.1080/03071847.2012.664354.

Roger McDermitt. 2014. “Myth and Reality—A Net Assessment of Russia’s ‘Hybrid Warfare’ Strategy Since the Start of 2014 (Part One).” *The Jamestown Foundation*. October 17. http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=42966&cHash=6807c1930eae4cbece171314536d557c.

Rogers, Michael. 2015. “A Cybersecurity Conversation with Admiral Rogers.” Discussion, University of North Carolina, February 9.

Shuler, Rus. 2002. *How Does the Internet Work*. Pomeroy IT Solutions.

Stephenson, Neal. 1996. “Mother Earth Mother Board.” *Wired* 4: 97–160.

“The Future Economic War.” 2015. Text. *Hoover Institution*. Accessed February 13. http://www.hoover.org/research/future-economic-war.

Theohary, Catherine A., and Anne I. Harrington. 2015. *Cyber Operations in DOD Policy and Plans: Issues for Congress*. Washington DC: Congressional Research Service.

Theohary, Catherine A., and others. 2011. *Terrorist Use of the Internet: Information Operations in Cyberspace*. DIANE Publishing. http://books.google.com/books?hl=en&lr=&id=Oqj50TAhhyoC&oi=fnd&pg=PA1&dq=%22Use+of+the+Internet:+Information+Operations+in%22+%22and+tactically,+in+pursuit+of+their+political+agendas.1+This+discussion+covers%22+%22and+network+intrusion+detection+are+outside+the+scope+of+this%22+&ots=LFLeAQsrxy&sig=U3sb6Rafq5ZYClfoeZomKl07gUQ.

Trent, Robert. 2014. “Unconventional Cyber Operations (UCO): A New Force Multiplier for Special Operations Forces.” Washington DC: The College of International Security Affairs, National Defense University.

Trujillo, Mario. 2015. “OVERNIGHT TECH: Report details ISIS’s Twitter reach.” Text. *TheHill*. March 5. http://thehill.com/policy/technology/overnights/234818-overnight-tech-report-details-isiss-twitter-reach.

Turner, Vernon, David Reinsel, John F. Gantz, and Stephen Minton. 2014. “The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things.” EMC Corporation. http://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm.

United States Army John F. Kennedy Special Warfare Center and School. 2008. *FM 3-05.130 Army Special Operations Forces Unconvetional Warfare*. Washington DC: Headquarters, Department of the Army. http://library.outdoorhistory.com/xmlui/handle/123456789/6350.

United States Institute for Peace. 2014. *The National Defense Panel Review of the 2014 Quadrennial Defense Review*. Ensuring a Strong U.S. Defense for the Future. Washington DC: United States Institue for Peace.

United States Senate Select Committee on Intelligence. 2009. *Questions for the Record, Nomination of the Honorable Leon E. Panetta to Be Director, Central Intelligence Agency: Hearing Before S. Select Comm. on Intelligence*. Washington DC. http://www.intelligence.senate.gov/090205/panetta_post.pdf.

USAJFKSWCS (A). 2011. "Special Forces Unconventional Warfare." Department of Defense.

USSOCOM Public Affairs Office. 2013. "USSOCOM FY 2013 Budget Highlights." United States Special Operations Command.

Wall, Andru E. 2011. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/harvardnsj3&section=5.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown.

———. 2015. "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever." *WIRED*. January 8. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

ABOUT THE AUTHOR

MATTHEW E. NORDMOE

.