Effects-Based Operations in the Cyber Domain

by

Michael J. Weiskopff

A Capstone Project Submitted to the Faculty of

Utica College

May 2017

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

New ways to fight using technology, requires new planning and methodology to fight back. This paper evaluates current Department of Defense doctrine to look at ways to conduct warfare utilizing the cyber domain. In order to maintain a superior military capability, the United States must develop an efficientive means to execute operations in the cyber domain. This research discovered the Department of Defense doctrine lacks planning guidelines for utilizing the cyber domain in current operations. This paper demonstrates how the department of defense can expand on the leveraging of the cyber domain in effects-based operations. Keywords: Cybersecurity, Professor Cynthia Gonnella, cyber targeting.

Acknowledgements

I would like to thank my parents for giving me the motivation and direction in my life, God for guiding me through right and wrong, my Boy Scout troop for showing me how to plan and prepare for the future, my teachers from all levels for giving me the knowledge to succeed, my military leadership for showing me how, and how not, to lead. Last, but not least, I would like to thank my family for allowing me to achieve my goals.

Table of Contents

List of Illustrative Materials vi
Effects-Based Operations in the Cyber Domain 1
Evidence Justifying the Research Problem 2
Deficiencies in Evidence 5
The Audience 6
Literature Review 7
Defining Effects-Based Operations 8
Applying Effects-Based Operations to the Cyber Domain 23
Needing Effects-Based Operations in the Cyber Domain 31
Other Countries Using Effects-Based Operations in the Cyber Domain 39
Discussion of the Findings 42
A Target as a System 45
Target Development Process 48
Orders of Effects 50
Use in Strategic Targeting 53
Future Research and Recommendations 55
Undesired Effects 55
Predictability 56
Probability and Success 57
Recommendations 58
Conclusions 60
References 63
Appendix 67
Appendix A – Russian Primary Goals of Cyber Operations Against Georgia 67

List of Illustrative Materials

Figure 1 A Systems Perspective of the Operational Environment 10
Figure 2 Complexity of Higher Order Effects 17
Figure 3 Phase 5 Targeting Steps.....23
Figure 4 The Three Layers of Cyberspace.....27
Figure 5 Effects Cascades: Bounding Complexity by Pruning 49

Effects-Based Operations in the Cyber Domain

According to Guinness World Records, organized warfare began around 3000BCE, specifically in the land domain (n.d.). Since 3000BCE, warriors have gained several new domains to operate in, including sea, air, and space. As war changes, a warrior's tactics, techniques, and procedures need to change as well. In July of 2016, the North Atlantic Treaty Organization, and its allies had officially declared cyberspace a new domain of warfare (North Atlantic Treaty Organization, 2017). The addition of a new domain, of course, requires the warrior to change, or adapt, their tools for use in the new domain. Military forces heavily used one of these tools, the concept of effects-based operations, from 2003 to 2017, during the wars in Iraq and Afghanistan.

Joint Publication 3-60 stated that "the purpose of targeting is to integrate and synchronize fires into joint operations by utilizing available capabilities to generate a specific lethal or nonlethal effect on a target" (Department of Defense, 2013, p. vii, para. 7). In non-technical terms targeting, in a generic sense, is the process of selecting objectives, and determining how to engage those targets in a way that facilitates and supports the operation. According to the Department of Defense Joint Publication 3-60, the Department of Defense considers effects a "change in the physical or behavioral state of a target system, a target system component, a target, or a target element that results from an action, a set of actions, or another effect" (2013, p. xiii, para. 4). In other words, an effect is a condition that is expected to support the operation if achieved. As Lieutenant Colonel Joshua H. Ho, a Senior Fellow at the Institute of Defence and Strategic Studies at Nanyang Technical University in Singapore, stated, "an effects-based approach to operations seek to marry the means with the ends by identifying the outcomes or strategic objectives desired in a campaign and deriving the means required to achieve those

outcomes" (2006, p. 157, para. 2). This effects-based approach allows nations to leverage non-lethal means of warfare to support the operation, which is helpful with cyber since it mostly helps achieve non-lethal effects.

The purpose of this research was to analyze current practices of effects-based operations in conventional warfare and determine how to apply these practices to effects-based operations in the cyber domain. Specifically, this research focused on four main questions: What are effects-based operations? How do we apply conventional effects-based operations in the cyber domain? Do we need effects-based operations in the cyber domain? Have any other countries successfully employed effects-based operations in the cyber domain?

Evidence Justifying the Research Problem

When a nation declares a new domain of warfare, that nation's military should develop new tactics, techniques, and procedures, or adapt old ones, to make full use of this new domain. According to Dr. Karl Mueller, a political scientist specializing in defense policy issues at the RAND Corporation, when the United States first established air power as a domain in warfare, they spent the next 90 years developing new, and adapting old, tactics, techniques, and procedures for leveraging air power against their adversaries (2010). Now that the North Atlantic Treaty Organization and its allies officially consider cyber as a domain, nations' militaries need to start developing or adapting, tactics, techniques, and procedures to effectively leverage the new domain against their adversaries (North Atlantic Treaty Organization, 2017). Because cyber is conceptually different, and less tangible, from the other four domains, land, sea, air, and space, militaries will have to provide greater detail when they develop the tactics, techniques, and procedures for cyber as opposed to the current level of detail in the Department of Defense

doctrine. Another reason a decision is required is due to how quickly nations have already adapted cyber as another domain of warfare

The United States has maintained an advantage over other nations in air power for the past ninety years due to the resources and technological advantages utilized for developing new and adapting old, tactics, techniques, and procedures for leveraging air power. If different nation's capabilities are compared to each other, the United States' capability to conduct air operations is far superior to any other nations due to the resources and technological advantage the United States had over other nations when the United States started developing its air power. According to NationMaster.com, an organization consisting of statistical professionals from around the world, the United States has over three times the aircraft of the next largest air force, (n.d.). According to Colonel Michael Philbin, an operations officer for the United States Army Cyber Unit, due to the low cost of equipment and the availability of information, developing a capability to operate in the cyber domain is exceptionally cheaper, and therefore extremely easier, than developing a capability to operate in any of the other domains (2013). Due to the reduced initial cost of conducting cyber operations, the existence of the cyber domain creates an even playing field that allows nations with fewer resources to be just as capable, with access to equivalent strategic weapon systems, as nations with greater resources. Therefore, due to a reduced cost of conducting cyber operations, the United States should start developing a targeting process for cyber operations, before other nations obtain an advantage. If the United States wants to achieve the same kind of benefits in the cyber domain it does with air power, then the United States must adapt old and develop new tactics, techniques, and procedures for operations involving the cyber domain.

For proof that nations are leveraging cyber as a domain of warfare, one can easily point to other nations and their use of the different domains. As reported on the *GlobalSecurity.org* website, a trusted source of military information by prominent news agencies, China has only one active aircraft carrier to project air power into naval operations, which is a very stark comparison to the United States who has nineteen aircraft carriers (n.d.). However, when looking at compromises caused by cyber operations, China, according to FireEye, a prominent cyber security firm, is responsible for over 262 compromises (2016). When looking at Russia's naval capabilities, they also currently have only one aircraft carrier (GloblSecurity.org, n.d.). However, F-Secure, a cyber security firm, accredited at least seventeen compromises to Russia from 2008 to 2015 (n.d.). Other countries have lesser capabilities in projecting naval air power, such as Iran, which have no aircraft carriers. Claudio Guarnieri, is the creator and developer of the Cuckoo Sandbox and active member of the Shadowserver Foundation Collin Anderson is a researcher focused on measurement and control on the Internet. Guanieri and Anderson, during their presentation at Black Hat, a popular hackers' conference, discovered Iran conducted at least four major campaigns consisting of numerous compromises (2016).

Ninety years ago, air power was declared a domain of warfare and currently no other nation has a capability equal to the United States in launching aircraft while at sea (n.d.). When comparing nations' capabilities to conduct operations in the cyber domain, even before the North Atlantic Treaty Organization declared cyber a domain of warfare, policy makers discovered that nations conducted cyber operations against each other (North Atlantic Treaty Organization, 2017). A perfect example was the use of the Stuxnet worm, which Kim Zetter, a prominent cyber security researcher for Wired Magazine, attributed to the United States as a part of a successful cyber operation in 2008 to attack the Natanz nuclear complex in Iran (2014). The cyber operation

that utilized Stuxnet occurred seven years before the North Atlantic Treaty Organization declared cyber a domain (North Atlantic Treaty Organization, 2017). The comparison of when cyber operations occurred and when the North Atlantic Treaty Association declared cyber its own domain showed that the international adoption rate of, and the individual nations' capability within the cyber domain is advancing faster than the capability for international organizations to develop policy to utilize the cyber domain. With the adoption rate being so quick, a nation who wants to leverage, successfully, the cyber domain needs to start developing its cyber tactics, techniques, and procedures, which, includes various targeting methodologies, such as the use of effects-based operations to conduct targeting. Not only is the international adoption rate of cyber as a domain fast paced, but so is the changing of technologies used to make up the cyber domain.

Deficiencies in Evidence

Cyber targeting has only initially started development and therefore leaves a large amount of room for improvement. The majority of Department of Defense doctrine on targeting in the cyber domain, based on reviews of Joint Publications 3-60 and 3-12R, is just an extension of the Department of Defense's current targeting practices which, based on these same publications, is typically used primarily in the application of lethal force (2013). Most of the Department of Defense's publications, Joint Publication 3-60, and Joint Publication 3-12R, only add, in an ad hoc style, cyber elements to existing joint doctrine. In 2017, there is not any extensive doctrine for utilizing the cyber domain for conducting effects-based operations.

Joint Publication 3-60, published in January 2013, "provides doctrine for the planning, coordination, and execution of joint targeting" (Department of Defense, 2013, p. i, para. 1). Joint Publication 3-60 described, "the purpose of targeting is to integrate and synchronize fires into

joint operations by utilizing available capabilities to generate a specific lethal or nonlethal effect on a target" (Department of Defense, 2013, p. I-6, para. 2).

Joint Publication 3-12R, published in February 2013, "provides joint doctrine for planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations" (Department of Defense, 2013, p. I, para. 1). Although the focus of this publication is cyber operations, the main concern of the publication is how to integrate cyber operations into existing military operational doctrine to fully optimize cyber operation. Neither Joint Publication 3-60 nor the Joint Publication 3-12R provided detail on how to conduct targeting explicitly in the cyber domain.

Major Steven J. Smart, former Chief of Targeting and Operational Law at United States Cyber Command, took on the most recent endeavor into researching how to update the joint targeting process in 2011. Smart stated that an update to Joint Publication 3-60, was vital because, "Cyber warfare differs fundamentally from traditional armed conflict" (2011, p. 67, para. 3). Although the Department of Defense has updated Joint Publication 3-60 since Smart's criticism, the additions have been minor. An update to these publications could greatly enhance the ability to plan cyber operations to support other operations.

The Audience

The *targeteer* is a person "who has completed formal targeting training in an established Service or joint school and participates in the joint targeting cycle in their current duties" (Department of Defense, 2013, p. GL-9, para. 9). The targeteer and his role in planning is the primary focus for this information. Although targeting, in and of itself, is not intrusive, the follow up actions of conducting operations in the cyber domain, either computer network attacks or computer network exploitation can have negative side effects. The repercussions of these

operations can have detrimental effects to the operator such as the discovery of a capability, previously undiscovered exploit, or specialized techniques. The company that maintains the network, that cyber operations occurred on, will most likely discourage these actions, due to the possible negative effects these actions may have on the company's network. Therefore, the primary audience for this information will include Department of Defense employees and military service members who are involved with the targeting process in cyber, as well as the developers of current military doctrine, as it pertains to cyber targeting.

Literature Review

The sources selected for this research come from various repositories. Since the focus of this research deals mainly with reviewing the military fundamentals of effects-based operations as effects-based operations are currently taught, a review of Department of Defense doctrine was required, and therefore several joint publications were reviewed. However, since effects-based operations doctrine can differ from the actual implementation of effects based operations, several papers, published through the different services' colleges for advanced military studies, were also researched due to their expertise in the usage of effects-based operations in warfare. Another portion of the literature covered comes from a theoretical point of view published by think tanks, which involve their evaluation and theoretical use of effects-based operations in crisis, conflict, or peacetime. Lastly, due to the constantly changing nature of the cyber domain, some of the most recent incidents that involved the cyber domain are evaluated. The research was used to discuss the four main areas that involve the cyber domain. These four main areas include describing what effects-based operations is, how to apply effects-based operations in the cyber domain, what is effects-based operations in the cyber domain, and are any countries currently utilizing effects-based operations currently.

Defining Effects-Based Operations

Major Leonard D Rickerman, a graduate of the United States Army Command and General Staff College, School of Advanced Military Studies, authored *Effects-based Operations: A New Way of Thinking and Fighting*. Rickerman wrote, "transformation ascertains that a new paradigm or way of thinking about warfighting is required due to the changing threat, strategic environment, and new ideas, which continue to challenge the way we think about warfighting" (2003, p. 1, para. 1). One of these new paradigms that Rickerman discussed is effects-based operations. Rickerman described effects-based operations as a process, "which seeks to plan, prepare and execute military operations oriented on what effects must be achieved to bring about the desired strategic outcomes" (2003, p. 1, para. 2). With the concept of effects-based operations, nations are no longer focusing only on lethal capabilities at targets. Instead, nations are now leveraging all elements of national power in order to obtain the desired effect (Rickerman, 2003).

According to Rickerman, "warfighting concepts are evolving because of two primary driving factors" (2003, p. 4, para. 2). Rickerman presented the two primary factors as, the increased ability to collect and process data and the increasingly interconnected and interdependent countries around the globe (2003). This interconnected and interdepended nature of these countries is what allows for, "vulnerabilities of direct and indirect, desirable and undesirable effects" (Rickerman, 2003, p. 4, para. 2). Rickerman continued to discuss how the technologies that allow these different countries to become interconnected and interdependent is achievable because of the vast advances in technology (2003). Rickerman also explained how technology, through "Cyberwar" and "Netwar," would be the future of warfare (2003). Rickerman expressed how this same technology has also caused not just countries, but also

businesses and people to be interconnected and interdependent (2003). Not just interconnected and interdependent to each other, but to the technology that supports the interconnection and interdependence as well.

One of Rickerman's complaints is that effects-based operations have murky and confused origins (2003). With historians tracing the origins of effects-based operations as far back as the origins of war itself, Rickerman wrote, "the confusion associated with the concept of effects-based operations is attributed to its evolution as a concept and the resulting difference of versions and definitions" (2003, p. 10, para. 1). However, Rickerman also correlated the use of effects-based operations to the use of technology, and that technology has allowed militaries to expand the effectiveness of effects-based operations (2003). This technology is what allowed Colonel John Warden, the architect of the Gulf War air operations in 1990, to focus, "on an approach that describes required effects to secure strategic objectives and then conduct military actions that would bring about the required effects" (Rickerman, 2003, p. 12, para. 1). Rickerman continued his discussion about Warden's concept of effects-based operations, which consisted of five concentric rings, leadership in the middle, with production, infrastructure, population, and fielded forces in the outer rings (2003). Targets in the center ring would be fewer than in the outer rings, but simultaneously targeting the multiple targets in the outer rings would cause the same desired effect as targeting in the center of the ring (Rickerman, 2003).

Rickerman discussed how Major General Dave Deptula had continued Warden's work (2003). According to Rickerman, Deptula has, "placed more emphasis on the understanding of the enemy as a system, and the determination of the linkages between cause and effect" (2003, p. 14, para. 2). Rickerman continued, with Deptula's, "expanded concept offers better potential for the military to achieve desired effects through a more holistic and systematic approach to

planning, executing, and assessing results" (2003, p. 14, para. 2). Rickerman assessed this expanded view would provide, "more efficient ways to achieve national goals and allows us to consider shaping the environment to minimize United States interests" (2003, p. 14, para. 2). This approach shows that Deptula's focus is more on control rather than on the attrition and is similar to Warden's five rings (Rickerman, 2003). Deptula focused "targeting not necessarily on the destruction of the enemy systems but rather on the prevention of the intended use as the adversary desires" (Rickerman, 2003, p. 15, para. 1). According to Rickerman, the Joint Forces Command continued Deptula's way of thinking, "which integrates effects-based operations as a holistic and systematic approach to warfare that is applicable across the spectrum of conflict" (2003, p. 15, para. 2). Figure 1 graphically shows how a system's to targeting can be perceived.

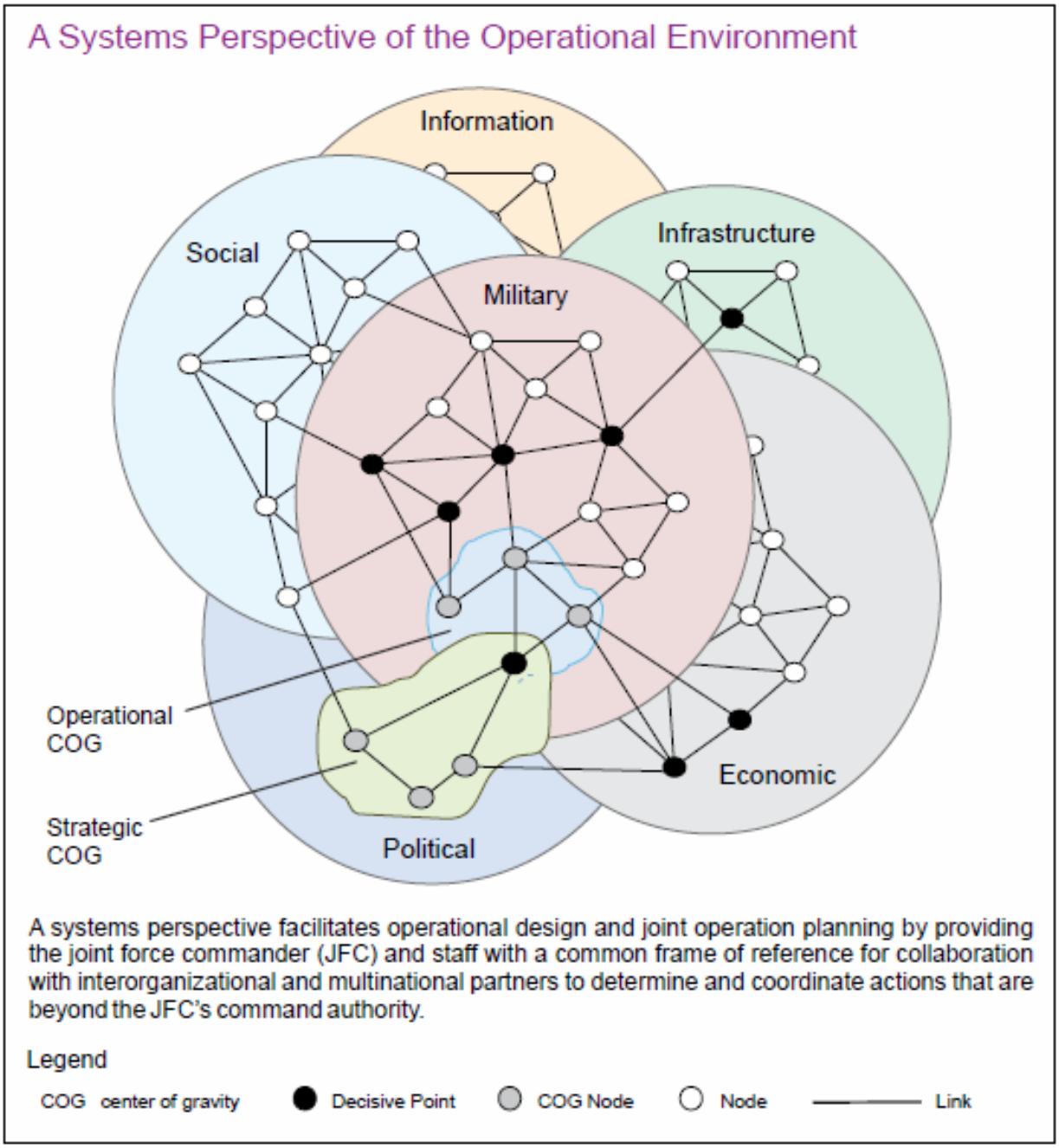

Figure 1. A Systems Perspective of the Operational Environment (Department of Defense, 2013, p. IV-3, para. 2)

Rickerman also revealed how Deptula had modeled effects-based operations. Instead of five rings, Rickerman described Deptula's model as a five-stage cycle (2003). The cycle starts with knowledge, then effects, application, assessment, adaption, and finally returns back to knowledge (Rickerman, 2003). The knowledge stage, according to Rickerman, "requires

comprehensive understanding of the enemy, the operational environment, and ourselves" (2003, p. 19, para. 2). Rickerman also stated, "the effects stage is where planning occurs focused on desired future states or outcomes (2003, p. 19, para. 2). Next, Rickerman explained, "upon execution of the plan, the application stage considered the full range of national powers" (2003, p. 19, para. 2). For the assessment stage, Rickerman noted, "the assessment stage then focuses on the effects by collecting, analyzing, and evaluating results of the effects" (2013, p. 19, para. 2). After completing the assessment stage, the results of the plan are then either validated or modified and made a part of knowledge (Rickerman, 2003).

Lieutenant Colonel Allen W. Batschelet, a targeting and planning officer for the United States Army, provided several examples of effects-based operations in history. The first included Ulysses S. Grant's implementation of the Anaconda Policy (Batschelet, 2002). During his campaign, Grant focused his strategy on targeting both the armies of the Confederacy as well as the resources required for the war that existed in the South. Grant's focus on both the armies and the resources of the Confederacy essentially destroyed the Confederacy's existing armies as well as prevented the building of any new armies. Another example that Batschelet described was Sherman's campaign through Georgia (2002). During Sherman's campaign, as Batschelet explained, Sherman was trying to make the local populace, "feel the hard hand of war, as well as the organized armies" (2002, p. 7, para. 2). Both of these examples show how, "they sought to achieve combined and mutually supporting effects by attacking the enemy's armies, resources, and will" (Batschelet, 2002, p. 7, para. 1).

Batschelet also wrote about examples that took place during World War Two (2002). During World War Two, the United States Government devised war plans that would use land power to engage the German military while utilizing air power to destroy Germany's defense

industrial base (Batschelet, 2002). This two-part strategy did not allow the Germans to continue to build their military machine, forced the German's to utilize their air power to protect their defense industrial base, and weakened their military to be susceptible to an amphibious attack (Batschelet, 2002).

The final example that Batschelet described involves the Gulf War that occurred in 1990 and 1991. Through the commander's intent of General Norman Schwarzkopf's plan, Batschelet described, "six theater objectives: attack Iraqi political/military leadership and command and control; gain and maintain air superiority; sever Iraqi supply lines; destroy chemical, biological, and nuclear capability; destroy Republican Guard forces; and liberate Kuwait City" (2002, p. 9, para. 2). Per Batschelet, this indicated that Schwarzkopf saw the enemy as a system, of which each part of the system Schwarzkopf targeted to achieve the desired effect over the entire system (2002).

In exploring the methodology of traditional targeting, Batschelete revealed that current targeting doctrine, "enables the idea of creating and achieving desired effects" which he refers to as "target value analysis" (2002, p. 10, para. 5). Batschelete continued explaining that conducting target value analysis is already a part of the Army's current military decision-making process (2002). Batschelet continued to further explain both the Army's targeting methodology, as well as the joint targeting methodology. The description that Batschelet gave the traditional targeting methodology included a process of, "Decide, Detect, Deliver, Assess" which "serves as familiar shorthand for this targeting and targeting value analysis process" (2002, p. 11, para. 2). Batschelet clarified that joint targeting methodology does not differ and that, "it prescribes a six-phase process: the commander determines his objectives, guidance and intent; develops,

nominates and prioritizes targets; analyzes friendly capabilities; decides on a course of action; plans and executes the mission; and finally, assesses action taken" (2002, p. 12, para. 1).

Edward Smith, the author of *Effects-based operations: Applying Network Centric Warfare in Peace, Crisis, and War* compared symmetric, or attrition-based, warfare with asymmetric, or cognitive-based, warfare (2006). The understanding that Smith provided is that while attrition-based warfare eventually eliminates the will of the enemy to fight by destroying their means, cognitive based warfare eliminates the will of the enemy to fight by shaping, "the behavior of the foe so that he no longer wishes to continue the struggle, or disorient him so that he can no longer fight or react coherently" (2006, p. 106, para. 1). Smith continued to explain, "while physical destruction remains a factor in effects-based operations, it is the creation of such a psychological or cognitive effect that is the true focus of the effects-based approach" (2006, p. 106, para. 2). Smith also stated that due to the increased capabilities that come with technological advances, the use effects-based operations might overcome the current reliance on attrition (2006).

Smith continued the discussion of an effects-based approach being used "to support our allies and to reassure neutrals, as well as simultaneously deterring other would-be adversaries who might potentially join the foe in opposing us" (2006, p. 107, para. 2). This way of thinking would then be used to, "provide a basis for looking at how military operations might best be orchestrated to shape the behavior of friends and would-be foes alike so as to prevent war and preserve peace" (Smith, 2006, p. 107, para. 3). Fundamentally, Smith is writing about using effects-based operations during wartime, as well as peacetime, and during a crisis. Effects-based operations do not have to be exclusively used in conflict scenarios.

Smith defined effects-based operations as, “coordinated sets of actions directed at shaping the behavior of friends, neutrals, and foes in peace, crisis, and war” (2006, p. 108, para. 4). Smith then split the difference that effects-based warfare is only a small portion of effects-based operations that would solely occur during a time of war (2006). Only after defining effects-based operations, Smith stated that a nation could start developing a process of effects-based operations (2006). Smith then explained that the definition of “actions” and “behaviors” are deliberately left as being broad so as to encompass military, political, economic, actions as well as friend, foe, or neutral’s behaviors, further leveraging the wide scope of how effects-based operations can be utilized (2006).

In detail, “effects” is the word to describe what happens to the larger operation if a unit destroys a target (Smith, 2006). Smith’s definition of “effects is also related to what Smith considered the second and third orders of effect, or the indirect impact of the destruction of the target (2006). Therefore, “an effect is a result or impact created by the application of military or other power” (Smith, 2006, p. 111, para. 3). Smith then implied that “other powers” could consist of power that comes from the elements of national power (2006).

Smith continued his discussion about effects-based operations when he asked, “just how do the actions we take, military and otherwise, influence the behavior of adversaries and other observers” (2006, p. 113, para. 1). Smith’s question becomes more of a psychological question, as psychologists would refer to advisory behavior as cause and effect, or, “stimulus and response interactions” (Smith, 2006, p. 113, para. 1). If this thought of stimulus and response continues, then it is easy to see that killing your foe shapes his future behaviors (Smith, 2006). To this same point, destruction of a foe’s equipment, infrastructure, or any other capability will also prevent the foe from continuing with his behavior (Smith, 2006). As an example, Smith explained how

destroying the SCUD missiles in Iraq prevented the enemy from being able to attack with the SCUD missiles, even though the enemy was still alive (2006). The destruction of this capability prevented the enemy of achieving their mission that required that capability.

Smith continued to integrate the effects-based approach to modern day tactics as he integrated the effects-based approach into the Observe, Orient, Decide, Act loop (2006). In his example, Smith explained that observing an activity, the stimuli, can cause a change of the decision, response, in the decision-making process (2006). The example that Smith gave involved the battle of Midway. During the battle of Midway, as Smith explained, Japanese aircraft were rearming due to the observation of the USS Yorktown (2006). The Japanese rearmed their aircraft with different munitions designed for watercraft, as opposed to aircraft, which is what their original munitions design. The process of rearming the Japanese aircraft prevented the aircraft from immediately taking to the air, which allowed the American bombers to destroy the aircraft, and the exposed munitions, before they could be used (Smith, 2006). The stimuli, observation of the USS Yorktown, caused a response, the rearmament of Japanese aircraft, which allowed the American aircraft to attack unchallenged.

The Department of Defense released, in January 2017, the updated Joint Publication 3-0, which defined joint operations. According to the Department of Defense:

> Joint operations are military actions conducted by joint forces and those Service forces employed in specified command relationships with each other, which of themselves do not establish joint forces. A joint force is one composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (2017, p. I, para. 2)

The Department of Defense then continued to explain that joint forces would use "fires" to, "produce destructive effects, but various other ways and means can be employed with little or no associated physical destruction. This function encompasses the fires associated with a number of tasks, missions, and processes" (2017, p. III-26, para. 3). The Department of Defense defined "effects" as:

1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect.
2. The result, outcome, or consequence of an action.
3. A change to a condition, behavior, or degree of freedom (2017, p. GL-8, para. 10).

All three of those definitions from the Department of Defense build a description of effects-based operations.

These definitions become important because the characterizations start building the framework of how to conduct targeting. Continuing the discussion of effects-based operations, the Department of Defense linked the "desired effect of the fires" to the "actions and tasks at the component level" (2017, p. III-27, para. 1). The Department of Defense's linkages start building the framework of how to conduct effects-based operations by deciding the effect that the commander wishes to achieve, and aligning it to the method of which the targeteer plans to achieve it. The alignment of effect to capability reiterated Smith's discussion about cause and effect, or stimuli and response and did not have to include the use of physical bullets and missiles (2006).

Major T. W. Beagle Jr., a senior pilot with over 3,000 flight hours and assigned to the Air Staff's Checkmate division in Washington DC, explained how effects-based operations are really about understanding the enemy as a system (2000). In Beagle's description, the enemy, in

modern warfare, consists of multiple parts, with each part providing a piece to allow the enemy success in their mission (2000). Each part then can be influenced and will "have effects associated with that influence" (Beagle, 2000, p. 7, para. 2). Considering the enemy as a system and targeting all parts of the system implies that targeting and influencing any one ancillary part of the system may not have the desired effect. However, targeting and influencing several ancillary parts may create the desired effect. Beagle referred to these as indirect effects, in comparison to direct effects, which is a part of the process of targeting the primary target (2000). In an analogy, Beagle talked about targeting the oil refiners as a way to stop a mechanized unit, without fuel, the enemy cannot move (2006). The same targeting strategy could be used by targeteers to target food sources, or ammunition sources, causing the same effect as actually targeting the mechanized unit with conventional munitions. Figure 2 shows how direct and indirect effects can influence each other.

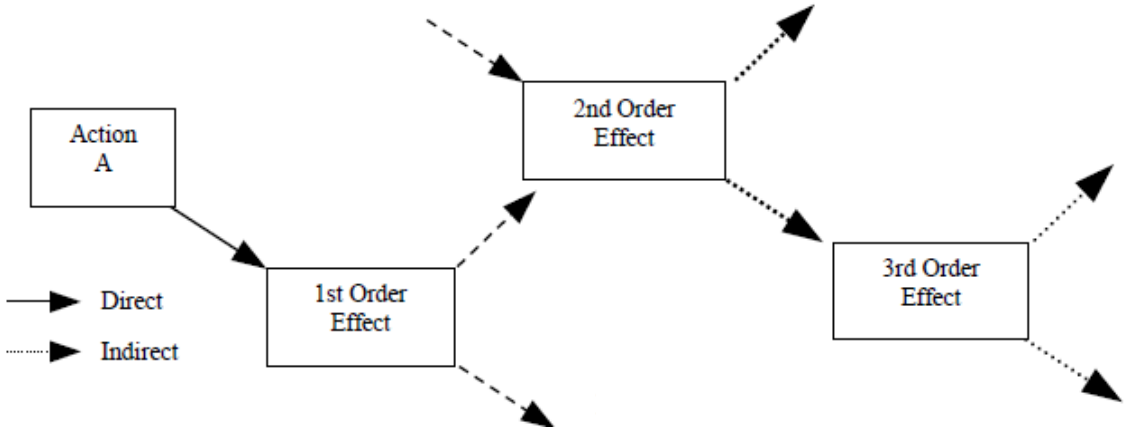

Figure 2. Complexity of Higher Order Effects (Beagle, 2000, p. 11, para. 2).

Beagle also explained that the majority of effects have other qualities and properties. These qualities include duration, or the time it takes for the desired effect to manifest scope of influence, or how much of the system it effects (Beagle, 2000). The properties of these effects, according to Beagle, include cumulative, cascading, and distributive (2000). Cumulative occurs when the aggregate of the effects cause other lower-order effects (Beagle, 2000). Cascading,

which occurs when a ripple of effects travel through the enemy system from higher order to lower order (Beagle, 2000). Lastly, distributive, which means every part of the system feeds, at least to some degree, the effects of the targeting (Beagle, 2000). Beagle also combined several of these effects into categories. The first set of categories that Beagle talks about includes both direct and indirect effects (2000). Where as a direct effect has a straightforward relationship to the target. An indirect effect may have a more obscure relationship to the target. However, Beagle further explains a second set of categories whereby the indirect effects can be broken down further based on the degree of separation from the target (2000). Beagle also explains this when he stated that, "Thus, a first-order effect is synonymous with a direct effect and subsequent orders (second, third, fourth, etc.) are the first, second, third, and so on, layers of indirect effects." (2000, p. 7, para. 1)

As Beagle continued to build out his methodology of effects-based operations, he continued to show the complexity of this concept (2000). While considering an enemy as a complete system, targeteers start to widen their view on how to attack the enemy and achieve the desired effect. This view continues to gain complexity when the targeteer understands that once the targeteers have decided what they are targeting, there are various ways to attack. If you expand upon Beagles example about targeting the oil refinery to stop a mechanized, targeteers could actually target the power station that is supplying power to the oil refinery, which accomplishes the same mission of preventing fuel from reaching the mechanized unit, which achieves the same effect of neutralizing the mechanized unit. However, as Beagle stated, "it becomes increasingly difficult to predict the outcomes of successively higher-order effects" (2000, p. 7, para. 1). This difficulty of predicting the results of the targeted effects is expected as targeteers increase the complexity of what and how they target the enemy.

One of the first things that Smart discussed in his paper *Joint Targeting in Cyberspace* refers to the foundational principles of joint targeting. Smart referred to Joint Publication 3-60 and explained that to conduct an offensive operation, five principles need to be followed (2011). The first principle is that joint targeting in the cyber domain requires military force to achieve the mission goals. The second principle is that no one, civilian or military, experience unnecessary suffering from the use of force, i.e.: chemical weapons. The third principle requires that the employment of force differentiate between combatants and noncombatants (Smart, 2011). The fourth principle that Smart described is proportionality. Smart explained that the military force used has to be proportionate to mission goals as to reduce the amount of collateral damage (2011). The last principle that Smart highlighted is the combatants involved in the conflict must follow a mutually agreed upon code of conduct (2011). Smart followed up with this discussion that following these principles guides targeteers targeting by guiding their use of force (2011).

As Smart continued to look at the use of Joint targeting in the cyber domain, he noted, "applying existing military doctrine (specifically, targeting and law-of-war principles) to operations in cyberspace is easy in theory but may prove extremely difficult in practice" (2011, p. 67, para. 3). Smart also explained that cyber warfare and traditional warfare differ because the actors involved, "(including state actors, criminals, terrorists, and hackers) can wage cyber warfare from far reaches of the globe rapidly, cheaply, anonymously, and devastatingly" (2011, p. 67, para. 3). Another difference between traditional warfare and cyber warfare is that traditional warfare exists exclusively in the physical world whereas cyber exists in both a physical world and a logical one (Smart, 2011). Smart then concluded that, "these variations illustrate the complex challenges of applying current law, policy, and military doctrine to keystrokes and mouse clicks" (2011, p. 67, para. 5). However, Smart did explain there are a few

similarities between cyber warriors and warriors of the other four traditional domains (land, sea, air, and space). These similarities include, "knowledge of the domain, operational environment, and weapon system capabilities" (Smart, 2011, p. 68, para. 2).

In Smart's review of Joint Publication 3-60, he clarified that the Department of Defense publication well explained the concept of joint targeting which consists of, "target development, target engagement, and damage assessment" (2011, p. 69, para. 4). However, as Smart expanded on his analysis, he showed that targeting is a backwards process, where the targeteer took the commander's mission statement and desired end state, determines the applicable targets to the commander's mission statement and desired end state, and finally pairs the appropriate weapon system to the target (2011). Smart then stated that this process, "quickly outlines the who, what, where, when, why, and how of adversary engagement" (2011, p. 69, para. 5). This entire process is what ensures each target is engaged with a capable weapon system, has a successful engagement, all while minimizing collateral damage against unintended enemy targets and civilians (Smart, 2011). According to Smart, this makes Joint Publication 3-60 a versatile guidebook for targeting in any domain if they share similar characteristics (2011).

Due to the nature of cyber, Smart explained it differs greatly from the other domains. The first difference between cyber and the other domains, as Smart described, are all the players involved. In the traditional domains, the main actors are typically state sponsored (2011). However, the cyber domain allows for, "criminals, terrorists, and state actors use the same cyber infrastructure employed by commercial enterprises and individuals to conduct their operations" in an anonymous fashion (Smart, 2011, p. 70, para. 3). The existence of all these actors also provides a, "social context" to the cyber domain (Smart, 2011). All of these actors, according to Smart, are capable of, "pressuring, confronting, or intimidating the United Stated, its allies, and

each other" (Smart, 2011, p. 70, para. 3). As Smart surmised, this makes for a congested and complex terrain that complicates Joint Publication 3-60 guide to targeting (2011). The complications come in, "five key areas: (1) positive identification of targets, (2) location of targets, (3) attribution of attack, (4) capability/target pairing, and (5) assessment of potential collateral damage" (Smart, 2011, p.70, para. 3).

Smart expanded on these five keys stating that due to the fluid nature of the cyber domain, and the duel use capabilities of certain targets, targets in the cyber domain, "demands both consistent updating of the validating intelligence and positive identification in near real time" (2011, p. 71, para. 1). Smart also explained that determining, "the location of a cyber target presents unique challenges" (2011, p. 70, para. 2). Traditional targeting refers to a location as a single point on a map whereas in cyber targeting locations can be both physical and logical allowing it to exist in multiple locations at once (Smart, 2011). As Smart explained, Joint Publication 3-60 does not take into account a target existing in multiple locations at once, which would imply the primary effects on a single target having secondary effects in several different locations (2011). Smart also described the complications that arise with attribution in cyber space. Smart separated attribution and positive identification to, "illuminate differences between offensive and defensive cyber targeting" (2011, p. 71, para. 3). The cyber domain allows for various forms of anonymity that can obfuscate, or even miss-assign, attribution (Smart, 2011). Smart followed up with a discussion of how, "pairing of capability and target in cyberspace entails unique issues" 2011, p. 71, para. 5). Finally, Smart also discusses the requirements needed in order to conduct assessments of potential collateral damage in cyber space. Smart explained that two main requirements were needed (2011). The first requirement Smart mentions consisted of conducting significant intelligence collection, which would require the knowledge

of the interconnectivity of networks (2011). The second requirement that Smart detailed included the redundancies in systems, which would require extensive planning (2011). With this in mind, Smart understood the complications of these requirements when he expressed "At present we have no formal methodology of collateral damage estimation for cyber targeting" (2011, p. 71, para. 6).

Applying Effects-Based Operations to the Cyber Domain

The Department of Defense published Joint Publication 3-60 to provide," doctrine for the planning, coordination, and execution of joint targeting" (2013, p. I, para. 1). During this revision, the Department of Defense did include some new information, as it is related to cyber. The first of these include the description of a virtual target, which is defined as, "an entity in cyberspace that provides a function that contributes to a target system's capability" (Department of Defense, 2013, p. I-1, para. 6). The Department of Defense further explored targeting of virtual targets through capabilities assignments. During capabilities assignments, the Department of Defense explained a process called *weaponeering* that aligns a weapon to the vulnerabilities of the target, once the targeteer discovers the vulnerabilities. (2013). According to the Department of Defense, this process is applicable regardless if it is a lethal or non-lethal weapon, like a weapon used in the cyber domain (2013). Figure 3 depicts the targeting steps as they appear in phase five of the joint targeting cycle.

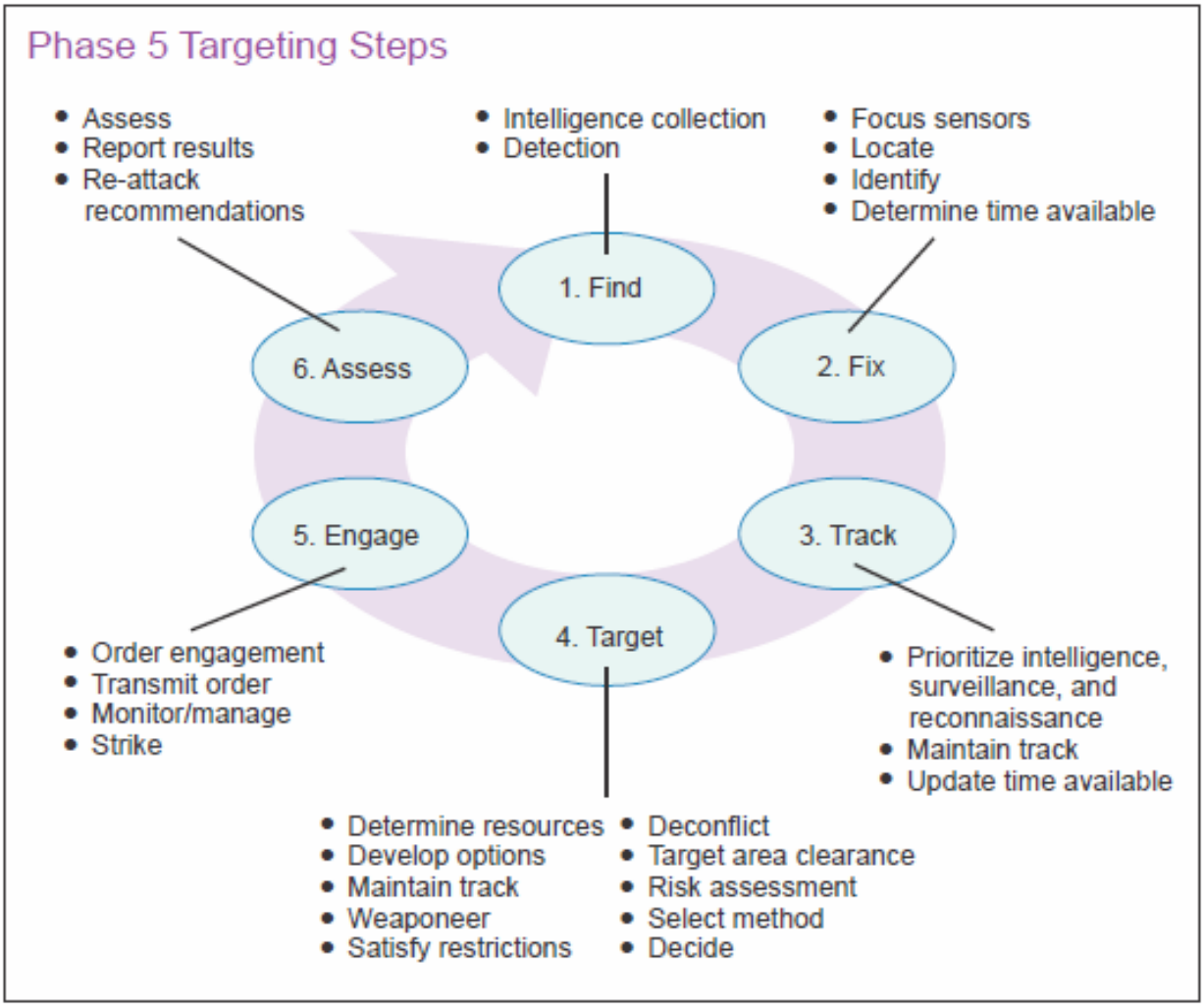

Figure 3. Phase 5 Targeting Steps (Department of Defense, 2013, p. II-23, para. 1).

When referring to non-lethal capabilities, the Department of Defense explained this might be the preferred choice depending on the mission (2013). For instance, "the Joint Forces Commander may require targeteers to prevent enemy flight operations while safeguarding the airfield's capability to support blue force operations once captured" (Department of Defense, 2013, p. II-16, para. 1). The use of non-lethal capabilities, one of which includes the use of operations in the cyber domain, gives the Joint Forces Commander, "scalability, selectability, and responsiveness" to all target types, to include virtual targets (Department of Defense, 2013,

p. II-16, para. 1). The Department of Defense's explanation shows that operations in the cyber domain has several use cases within conventional warfare.

The organization that is the lead in the Department of Defense for executing operations in cyber space has been the United Stated Cyber Command (Department of Defense, 2013). According to the Department of Defense, this organization is a, "subunified command under United Stated Strategic Command" (2013, p. III-18, para. 3). The Department of Defense also explained that the United Stated Cyber Command described their mission as:

> …plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified DOD information networks and prepares to, when directed, conduct full-spectrum military cyberspace operations in order to enable actions throughout the operational environment, and facilitates United Stated/Allied freedom of action in cyberspace while denying the same to our adversaries. (Department of Defense, 2013, p. III-18, para. 3)

United States Cyber Command's mission statement means that United Stated Cyber Command is responsible for everything as it pertains to cyber space.

Within Joint Publication 3-60, the Department of Defense also discussed the concept of integrating operations in cyber space with the joint targeting (2013). In this discussion, the Department of Defense explained that the Joint Forces Commander has the authority, through his mission, to create offensive effects utilizing cyber space (2013). However, the Department of Defense also explained that the targeting process utilizing cyber space has to be coordinated and deconflicted with the commander of Cyber Command in accordance with existing policy (2013). With this in mind, the Department of Defense explains that targeting in the traditional domains and targeting in the cyber domain should be similar, with a few caveats (2013). The first caveat

is that a targeteer must take into consideration the cyber domain's unique nature as compared to the traditional domains. The Department of Defense also explains that another caveat has to be made which includes the unique requirements that arise when a targeteer tries to match a cyber domain capability, or weapon, to targets that exist in cyber space (2013). However, the Department of Defense also clearly stated that, "Cyber Command does much of this targeting work and develops targets in support of its organic planning efforts and as recommendations for the integration of cyberspace targeting efforts with the combatant commands" (2013, p. C-7, para. 3).

The Department of Defense published a joint publication on conducting cyber operations that are referred to Joint Publication 3-12(R). The purpose of this publication, as stated by the Department of Defense, is to provide, "joint doctrine for the planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations" (2013, p. I, para. 1). The Department of Defense used this publication to define operations in the cyber domain as, "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (2013, p. V, para. 1). Specifically, the Department of Defense defined cyberspace as, "global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space" (2013, p. V, para. 2). The definition of the cyber domain then continues to be broken down by the Department of Defense into three main components, physical, logical, and persona (Department of Defense, 2013).

These three components continue to be defined by the Department of Defense. The physical network component is understood by the Department of the Defense as being, "comprised of the geographic component and the physical network" (2013, p. V, para. 4).

Therefore, the physical network component would be described by the tangible equipment, such as routers, switches, laptops, and desktops, and where the equipment resides physically so that one could have direct access to the equipment. The logical network component, as described by the Department of Defense, "consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node" (2013, p. VI, para. 1). The concept of a logical network component exist because information on the Internet may be, "hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator" (Department of Defense, 2013, p. VI, para. 1). The Department of Defense then expanded on what a persona is by stating that it, "represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace" (2013, p. VI, para. 1). The digital representation of an individual or entity is pertinent in order to describe the people who are actually on the network. Figure 4 exemplifies the Department of Defense's understanding to the three layers to cyberspace.

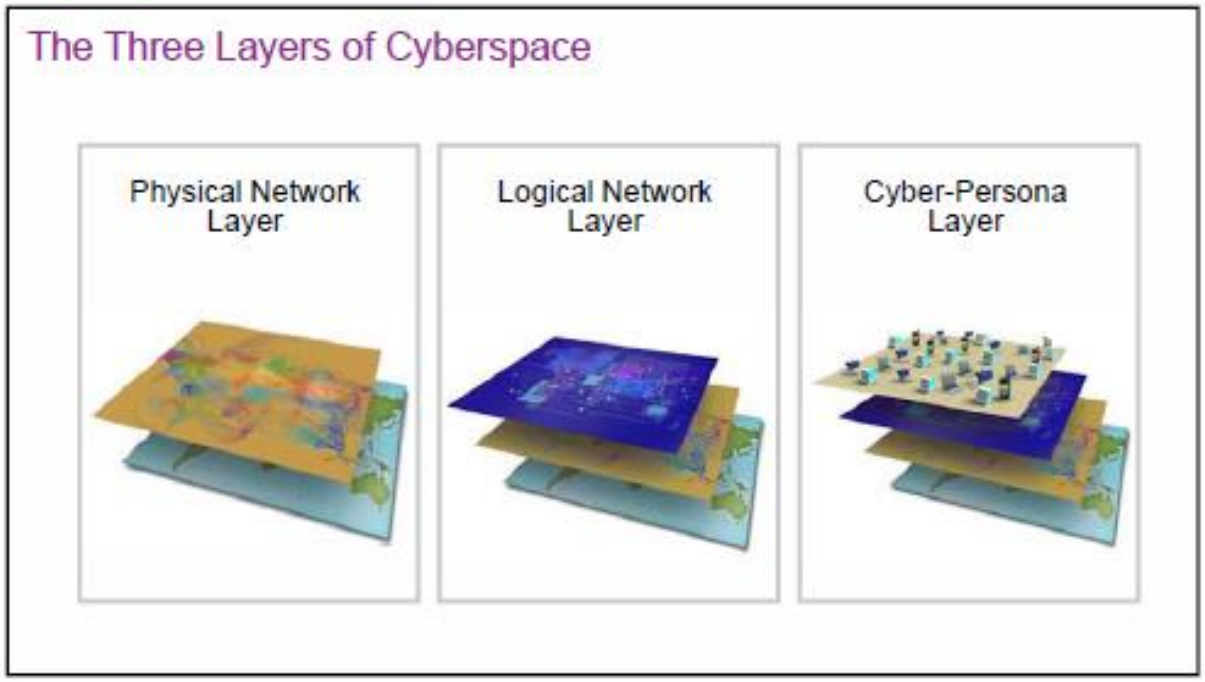

Figure 4. The Three Layers of Cyberspace (Department of Defense, 2013, p. I-3, para. 1*)*.

Cyber operations that are within the Joint Force Commander's purview include offensive operations in the cyber domain, defensive operations in the cyber domain, and Department of Defense information network operations (Department of the Defense, 2013). As their names imply, these operations are offensively orientated, defensive orientated, and maintenance orientated, respectively. However, there is also an intelligence collection proponent involved with operations in the cyber domain, which is mostly handled by national intelligence agencies and support the commanders planning (Department of the Defense, 2013). Each of these types of cyber operations can utilize targeting within each of the listed components.

The Department of Defense discussed one key part of operations in the cyber domain, operational environment. According to the Department of Defense, the operational environment consists, "of the conditions, circumstances, and influences that effect the employment of capabilities and bear on the decisions of the commander" (2013, p. I-4, para. 3). However, the operational environment is complicated by, "the continuing advancement of communications and

computer technology has significantly reduced acquisition costs leading to the rapid proliferation of cyberspace capabilities" (Department of Defense, 2013, p. I-4, para. 4). Understanding the operational environment, including how the physical, logical, and persona layers are all connected, help us understand the information environment. (Department of Defense, 2013).

The Department of Defense stated, "the information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is broken down into the physical, informational, and cognitive dimensions" (2013, p. I-5, para. 2). The physical dimension is important because it consists of command and control systems, infrastructure, decision makers, facilities, and computers (Department of Defense, 2013). The informational dimension is where information flows between being, "collected, processed, stored, disseminated, and protected" (Department of Defense, 2013, p. I-5, para. 4). The cognitive dimension refers to the actual humans who utilize the information (Department of Defense 2013).

After describing the environment, the Department of Defense included a description of the types of threats that one would engage in the operational environment. The first threat to consider is the nation state threat. Due to the access to resources not available to other actors, this actor becomes the most dangerous (Department of Defense, 2013). Nation states have used cyber operations to both attack and conduct espionage (Department of Defense, 2013). A nation state may also outsource its engagements in the cyber domain to other parties that are capable of achieving the nation's stated goals (Department of Defense, 2013).

Although the primary actor is the nation-state that the Department of Defense is worried about, they also discuss non-state actors. The first that the Department of Defense brought up is the transnational actor (2013). The transnational actor, according to the Department of Defense,

is, “formal and informal organizations that are not bound by national borders. These actors use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist actions within cyberspace” (2013, p. I-7, para. 1). Other non-state actors that are discussed by the Department of Defense also included criminal organizations threats, which are described as being either transnational or non-transnational in nature and may be used as surrogates by a nation-state. However, the criminal’s main goals include, “steal[ing] information for their own use or, in turn, to sell to raise capital” (Department of Defense, 2013, p. I-7, para. 2).

Lastly, the Department of Defense considered individuals or small group threats as well. As previously stated, the Department of Defense had made clear that due to the cheap and ubiquitous nature of computer technology, even individuals are able to play a role (2013). The Department of Defense explained that these individuals could illegally obtain access to and disrupt services of various networks and computer systems usually with malicious intent for various reasons (2013).

Conveying all these different threats brings up one of the more challenging difficulties, according to the Department of Defense, which includes attribution (2013). According to the Department of Defense the process of determining attribution, “requires significant analysis and collaboration with non-cyberspace agencies or organizations. The nature of cyberspace presents challenges to determining the origin of cyberspace threats” (Department of Defense, 2013, p. I-7, para. 4). Another challenge with all of these threats is that they are able to conduct their operations from remote locations (Department of Defense, 2013). Conversely, the Department of Defense can also conduct their operations against these adversaries remotely, which requires additional coordination (2013).

Desired effects on a target is another aspect of targeting that the Department of Defense raised within Joint Publication 3-12(R). In this case, the Department of Defense refers to these as deny, "to degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time" and manipulate, which is, "to control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives" (2013, p. II-5, para. 4 & 8). In order to deny a target a resource or asset, targeteers are required to achieve one of three effects. These effects are to degrade; to deny a specific amount of capacity for a specific amount of time, disrupt; to completely deny for a specific amount of time; or destroy, to completely deny for a maximum amount of time (Department of Defense, 2013). To manipulate, the Department of Defense stated that a targeteer has, "to control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives" (2013, p. II-5, para. 8).

Needing Effects-Based Operations in the Cyber Domain

Paul K. Davis, a senior principal researcher at the RAND Corporation, and a professor of policy analysis at the Pardee RAND Graduate School, understood that a new way of conducting operations was needed as the current type of operations was aging against the evolution of warfighting to include the rise of asymmetric warfare, when he authored the work *Effects-Based Operations: A Grand Challenge for the Analytical Community* (2001). In his book, Davis explained,

> effects-based operations are operations conceived and planned in a systems framework that considers the full range of direct, indirect, and cascading effects, which may—with different degrees of probability—be achieved by the application of military, diplomatic, psychological, and economic instruments" (2001, p. 7, para. 2).

This definition is designed in such a way to include both the physical military targets as well as what both Department of Defense and Davis called cognitive and behavioral targets. The definition of effects-based operations that Davis uses means that the effects-based operations system can be used for targets that are either tangible or abstract (2001).

Davis continued to explain that effects-base operations are rather an expansion of existing operations, and not a replacement (2001). Although effects-based operations can incidentally be concerned with destruction of a target, Davis stressed that effects-based operations instead focus on ideas like, "collapsing the will and cohesion of the enemy," "defeating the enemy's strategy rather than his armies" or "convincing the enemy's leader to make decisions favorable to our goals" (2001, p. 12, para. 1). Davis argued, however, that even with the introduction of cyberwar, "some traditional aspects of war will still be necessary" (2001, p. 16, para. 1). Davis then continued that effects-based operations might be better used in smaller conflicts rather than in major theaters of war (2001).

Davis then provided several examples of where effects-based operations were used and were successful:

1. Destroy a functionality of a complex facility (e.g., the ability to generate electricity or to produce aviation fuel).
2. Reduce the functionality of a C2 or C4ISR distributed network or the crucial elements of an integrated air defense system (IADS) (as was done in the first hours of the air attack on Iraq in 1991).
3. Limit the functionality of a combat system by attacking one or more of its critical components (e.g., in World War II, a goal was to kill most of the Luftwaffe pilots, limiting Luftwaffe capability even if aircraft and aviation fuel were plentiful).

4. Limit combat mission capability by degrading support operations (e.g., destroy ammunition or POL stocks, sever lines of communication necessary for resupply, or prevent surveillance).
5. Degrade the effectiveness of enemy operations by demoralizing or tiring enemy personnel (e.g., soften defender infantry by massive artillery fire and bombing prior to one's own offensive into the infantry positions).
6. Degrade the effectiveness of enemy operations by confusing and diverting enemy commanders (e.g., with feints, such as the amphibious forces off the coast of Iraq during Desert Storm; rear area operations, such as the partisan activities in World War II, civil war cavalry raids, or deep missions proposed for U.S. Marine and Army units; and higher-level disinformation, such as deception regarding the landing areas for Operation Overlord).
7. Influence the decisions of the enemy leader by making visible preparations for a large-scale ground offensive (as was arguably accomplished in the later days of the Kosovo campaign).
8. Influence the decisions of the enemy leader by providing him with a convenient way to protect some of his assets (e.g., as when the Iraqi Air Force flew to Iran, which served as a sanctuary during the remainder of the Gulf War, but which also removed the assets from the theater of operations).
9. Influence the attitudes of the enemy population to encourage a revolution or other change of power (as, for example, when Serbians removed Milosevic in the aftermath of the war over Kosovo, arguably as the result of seeing him as the one who had led

the nation into ruin and who—in any case—was an obstacle to recovery from the bombing campaign and continued economic isolation).

Entire list (Davis, 2001, p. 19, para 3)

Davis also included some effects-based operations that did not bode well for the planners. In these events, Davis explained that as effects-based operations apply to the cognitive domain, they have the ability to affect the decisions of political leaders, military commanders, or even whole populations (2001). However, Davis also explained that this becomes exceedingly difficult since individuals do not always react in predictable ways (2001). Individuals do not always react in predictable ways is mostly because, as Davis explained using the Cuban missile crisis as an example, "streams of reasoning were affected by numerous factors such as the vividness of certain facts or images, the order of events, physical fatigue, and random events" (2001, p. 22, para. 1). Another reason why Davis believed that effects-based operations are not always successful is because of the requirement of strategic level intelligence, which tends to be unreliable, to make decisions within an effects-based operation (2001). Davis furthered his discussion that there are sometimes too many variables to keep track of for a targeteer to understand how a target is going to react, thereby increasing the difficulty to predict the actions of the target when acted against (2001).

To help develop the best practices of conducting effects-based operations, Davis provided several principles to follow to conduct effects-based operations. The first principle that Davis indicated that a targeteer should follow is mission-system capability (2001). In this fist principle, Davis explained that not only does an analyst need to understand the capabilities of a system, but an analyst also needs to know what components make up the system and what resources are needed to run the system (2001). The next principle that Davis explained is exploratory analysis

(2001). Here Davis explained that the use of exploratory analysis is to, “confront uncertainty head-on, rather than downplaying its magnitude” (2001, p. 35, para. 3). The third principle of effects-based operations, as Davis understood it, is qualitative modeling (2001). In this principle, Davis explained there are other factors that cannot have a value assigned to them but are still important in predicting outcomes (2001). The next principle, according to Davis, is the use of empirical information (2001). In this principle, Davis explained that minimal effort is used to bring historical experience, or experience gained from training or exercises when conducting analysis (2001). The last principle that Davis expanded on is agent-based modeling (2001). This form of modeling, as Davis explained, is utilizing the command and control element of the system as the central or core element as opposed to command and control being a support element and the fighting force becoming the central or core element (2001).

To provide a working example, Davis started to develop a halt problem type scenario where an attrition-based attack is used to determine how many resources (troops, time) are required to halt an invading force (2001). Under typical considerations, Davis explained, the plan is to use standoff weapons to destroy enough of the invading force until it has reached its breaking point and retreats (2001). However, Davis postulated that a targeteer could employ other planning considerations to reduce the effectiveness of the invading force and force them to hit their breaking point sooner (2001). The first of these included the possibilities that the invading force that the targeteer is encountering is not motivated, cohesive, or first rate (Davis, 2001). If these variables were assessed to be true, then breaking point of the invasion may be much lower than initially expected (Davis, 2001). The rate at which the enemy forces travel may also be subject to re-evaluation. If specific, choke points, as bridges and tunnels are destroyed, it may decrease the rate of travel for the enemy (Davis, 2001). Lastly, Davis also explained that not

all attacking forces would follow the main avenue of approach (2001). If the enemy did split up across several avenues of approach, it would mean that depending on their dispersion and impeded movement, not all of them would reach their objective at the same time allowing for target prioritization where smaller units could successfully engage and destroy the larger invading force piecemeal (2001).

Captain Anthony M. Forestier, a recipient of a Masters in Defense Studies at Canberra as well as a National Security Fellow at Harvard University, authored a thesis called, "Effects-Based Operations: An Underpinning Philosophy for Australia's External Security?" where he described the use of effects-based operations for defending Australia (2006). The first thing that Forestier takes upon himself was describing conflict and how nations deal with conflict. At the base level, Forestier explained that conflict is a part of the human condition (2006). Forestier implied people are the real cause of conflict (2006). When there is a conflict between two nations, Forestier explained, that those nations can use their national power, "exercised through the political, economic, diplomatic and military dimensions" in order to have an effect on the will of the people involved in the conflict (2006, p. 2, para. 1). Ultimately, as Forestier continued, conflict is ended by people, just as it was started by people (2006). Therefore, the will of the people, and thus the people themselves, can be targeted via, "directly or indirectly, his physical, reason and belief domains" (Forestier, 2006, p. 2, para. 3).

Forestier continued to discuss the use of effects-based operations at a national level. With the use of effects-based operations having already been around for several years, Forestier stated it had been repackaged allowing new eyes to see it (2006). Forestier expanded on that idea by writing that "effects-based operations and the concepts of conflict related to it (network-centric warfare, rapid-decisive operations etcetera)" are the result of a new idea that information

operations will enable more conventional forms of conflict (2006, p. 15, para. 2). Forestier also explained that information operations would also help conventional operations "to be prosecuted more effectively and efficiently" (2006, p. 15, para. 2). Ultimately, Forestier explained, over time the concept of information operations will evolve from an enabling operation to a direct weapon (2006). According to Forestier, some of the side effects of utilizing effects-based operations include, "refocusing of intent and commitment, rapid conflict termination, economy of effort, reduced physical destruction, moral authority and so on" as national interests are concerned (2006, p. 16, para. 2). With the execution at the national level, Forestier's understanding of effects-based operations could help resolve conflict before conflict arises (2006).

Forestier also explained that one of the biggest requirements to conduct effects-based operations is the leveraging of intelligence (2006). Understanding that the proper use of effects-based operations would allow an invader to target the mind of the advisory, effectively allowing the advisory to make decisions that would ultimately be in the targeteer's favor (Forestier, 2006). However, to engage, effectively, these physical, and psychological, targets require as much intelligence about the targets in order to know what decisions the advisory will make after being engaged (Forestier, 2006). Forestier surmised that the leveraging of the elements of national power (political, economic, diplomatic, and military) with the proper intelligence about the adversarial people would cause the adversary to make the required decisions to prevent conflict (2006).

Aaron Brantly, Ph.D., Assistant Professor of International Relations and Cyber in the Department of Social Sciences, Cyber Policy Fellow, Army Cyber Institute and Cyber Fellow, Combating Terrorism Center at the United States Military Academy, talks about virtual-physical cyber operations where virtual attacks have effects in the physical world (2015). Conversely,

Brantly postulated, these kinds of effects could also occur in reverse direction (2015). Brantly cited an example from 2014 where a sniper was attacking power stations in California, which could have perceivable effects in the virtual world by powering down computers on the Internet (2015). Brantly referred to these activities as being indirect effects, which he also explained this applies to the majority of cyber operations (2015).

These types of virtual-physical cyber operations, as presented by Brantly, break down into two different categories, standalone effects and enabling effects (2015). Although standalone effects are straightforward, enabling effects can also be considered as "fires" and refers to supporting an operation from a remote location (Brantly, 2015). Brantly then explained a few examples to include the attack on the Natanz nuclear facility as a standalone effect and the corruption of the GPS in a counter artillery radar would serve as an enabling effect (2015). Brantly also explained that he does not include cyber for the purpose of intelligence gathering as either standalone or enabling (2015). Brantly continued his discussion to include the attributes of maneuver in the cyber domain. These attributes include deception, identification defense, movement of forces, mission execution against vulnerabilities to achieve a desired effect, and preparation to defend or relinquish acquired terrain as needed (Brantly, 2015).

Brantly then explained three different situations where cyber operations were used by different nation-states to support larger operations. The first example includes the use of psychological operations against Iraqi forces in 2003. Brantly explained that during the invasion, emails were sent to soldiers in the Iraqi military with instructions on how to surrender (2015). The second example included the use of cyber operations to neutralize Syrian air defense systems in 2007 to allow Israeli air strikes against suspected nuclear sites (Brantly, 2015). The last example that Brantly included was the use of organized criminal gangs to conduct cyber

operations to attack specific targets in Georgia prior to the Russo-Georgian war of 2008 (2015). Because cyber operations are so new, Brantly concluded, there needs to be continued discussion on how to appropriately use cyber operations for direct and indirect support of ongoing military operations (2015).

Other Countries Using Effects-Based Operations in the Cyber Domain

Jamie E. Palagi, served in the 10th Mountain Division and later in the US Army Special forces before joining the United States Department of State where he has had a career in the Foreign Service, wrote about one specific country and their use of cyber, Russia. The first instance of Russian use of cyber offensive operations was against Estonia in 2007 (Palagi, 2015). As Jamie explained, the cyber-attack, "affected the Estonia government, banking systems, and nearly shut down the infrastructure of the country" (2015, p. 15, para. 2). Besides being the first known Russian use of cyber, this incident is important for several other reasons (Palagi, 2015). The first is Russia's use of cyber at not only tactical level but also at a strategic level in defense of ethnic Russians in former Russian states (Palagi, 2015). The direct effects of this operation were on the cyber infrastructure of the country with an indirect effect that Russia proved it could, on a scale never before seen, "influence foreign populations within a sovereign nation" (Palagi, 2015, p. 16, para. 1). This act by Russia, which used both state and non-state assets, sent the message that "we are ready, willing, and able to actuate ethnic Russian populations and tensions, regardless of where the internationally recognized borders are drawn" (Palagi, 2015, p. 16, para. 2).

The following year, Russia utilized cyber operation in conjunction with a conventional attack in Georgia (Palagi, 2015). In this instance, Russia had utilized offensive cyber operations in order to disrupt Georgian's ability to communicate before and during the conventional

military operation (Palagi, 2015). The direct effect was the neutralization of communications capabilities within the country via landlines, cell phones, and the Internet as well as defacement of various Georgian websites with a pro-Russian message (Palagi, 2015). However, the indirect effect was the creation of confusion and the perception of instability within the country, which, "amplified the conventional Russia military forces' freedom of movement" (Palagi, 2015, p. 18, para. 2).

The United States Army War College conducted an even more in depth analysis of the Russian use of offensive cyber operations against Georgia. In this study, the War College details the Russian cyber operation, which began with intelligence gathering (2016). In this case, Russian cyber intelligence units were mapping out important Georgian government, military, and civilian networks (War College, 2016). According to the War College, Russia, "also attacked Georgian hacker forums to pre-empt a retaliatory response against Russian cyberspace targets" (War College, 2016, p. 55, para. 4). The Russian primary goals The War College described are listed in Appendix A.

In a more recent event, Kim Zetter, author of Countdown to Zero Day and cyber security writer for *Wired* magazine, discussed the power outage in the Ukraine in December of 2015. In this incident, Russia used a cyber weapon to take control over the power stations only to lose control a few hours later when the power stations were switched to manual (Zetter, 2016). However, in her report, Zetter also explained that in 2014, Russia annexed Crimea and since then political tensions between Russia and the Ukraine have been high (2016). Zetter then explained that there could have been several reasons for the attacks on the power station in the Ukraine. The first being pro-Ukrainian protesters had physically damaged power stations in the pro-Russian parts of Crimea (Zetter, 2016). However, Zetter explained that the intelligence gathering

for this cyber operation had been going on for several months prior to the attack and that the physical attacks on the power station in pro-Russian areas had "rushed their plans" (2016, p. 10, para. 2). Zetter continued that the initial reason for conducting the reconnaissance required to perform such a cyber operation may have been started due to "the Ukrainian parliament has been considering a bill to nationalize privately owned power companies in Ukraine" (2016, p. 11, para. 2). However, "Some of those companies are owned by a powerful Russian oligarch who has close ties to Putin" (Zetter, 2016, p. 11, para. 2). Therefore, Zetter postulated, the Russians designed the cyber operation to send a message to the Ukrainian government (2016).

The Department of Homeland Security released, on October 7, 2016, a statement about the most recent offensive cyber operation attributed to Russia, the Democratic National Committee hack (2016). In this incident, the Department of Homeland Security stated that, "Russian Government directed the recent compromises of emails from US persons and institutions, including from US political organizations" (2016, p. 1, para. 1). In the statement, the Department of Homeland Security also outlined several pieces of information that they used to attribute the attack to Russia. The tactics, techniques, and procedures, as well as motivations, are consistent with other Russian cyber operations (Department of Homeland Security, 2016). Russia has also utilized similar methods in order, "to influence public opinion" (Department of Homeland Security, 2016, p. 2, para. 1). The Department of Homeland Security also explained that several states had witnessed reconnaissance activities against their election-related systems from Russian based locations. Although this information regarding reconnaissance could not be attributed to Russia directly (Department of Homeland Security, 2016).

Discussion of the Findings

The purpose of this research was to analyze current practices of effects-based operations in conventional warfare and determine how to apply these practices to effects-based operations in the cyber domain. Specifically, this research focused on four main questions: What are effects-based operations? How do we apply conventional effects-based operations in the cyber domain? Do we need effects-based operations in the cyber domain? Have any other countries successfully employed effects-based operations in the cyber domain?

Of all the research that was reviewed, the discussion that involved effects-based operations was solely referencing the use of effects-based operations in conventional warfare. The absence of research in using effects-based operations in the cyber domain is proof that research needs to be conducted to determine if effects-based operations would be effective in the cyber domain. Although the material covered did not specifically apply to the cyber domain, there were several themes that became evident from the research, that are applicable to the cyber domain. These themes include the historical use of effects-based operations as far back as the American Civil war, treating a target as a system of several targetable components, orders of effects and their direct or indirect application, the use of effects-based operations in manipulating elements of national power.

The first theme, the historical use of effects-based operations, shows that both military and national leaders utilized the concept of effects-based operations as far back as the American Civil War. With operations planned and executed by Ulysses S. Grant, as Batschelet explained, showing that he understood the enemy composed of several parts. Batschelet wrote that Grant understood the Confederate Army consisted of several components that needed to run smoothly for them to keep up their offensive. According to Batschelet, Grant also knew that targeting the

industrial base in the South would have several side effects that would affect the main military force. Based on Batschelet's understanding of Grant's strategy, targeting the South's defense industrial base would disrupt logistical support for the South's war effort as well as break the will of the civilian populace in the South, which would have a negative effect to the moral of the Confederate fighting force. Batschelet knew that if the fighting capability of the Confederate forces could be mitigated enough, then the Confederate Armies either would give up, no longer being a viable threat, or be defeated by the Union Armies due to the lack of support and low morale.

Another example of this same tactic involved the bombing campaign of the defense industrial base in Germany during World War Two. However, besides disrupting the supply chain for the German forces and breaking the will of the civilian populace, there was another side effect of conducting bombing campaigns on Germany's industrial base. From Batschelet's analysis, this other side effect caused the German military to prioritize their missions and further divide their resources as required. According to Batschelet, the attacks against Germany's industrial base meant that if the German forces wanted to maintain their supply chain for their forces, they would have to divide further and prioritize their military units to protect their industrial base. As Batschelet explained, since the allied forces were attacking Germany's industrial base with bombing sorties, the German military would have to use aircraft to counter the bombing sorties. With those aircraft performing guard duty protecting the industrial base against the bombing sorties, Batschelet understood that ground operations would not be able to benefit from the use of those aircraft and become susceptible to other attacks like amphibious assault.

The next example that described the use of effects-based operations was Schwarzkopf's mission statement during the first Gulf War in 1990 and 1991. As Batschelet summarized, during this time, Schwarzkopf's mission statement consisted of six strategic Iraqi targets: leadership, air superiority, supply lines, weapons of mass destruction, Republican Guard, and Kuwait City. Batschelet understood that based on Schwarzkopf's mission statement, Schwarzkopf understood the enemy as a system and knew that he could target each component of the system to defeat the enemy.

When analyzing the Ukraine power station hack in 2015, and the more recent Democratic National Committee hacks of 2016, many of the same similarities are observed. High-level leadership utilized an effects-based approach to conducting operations that effect other nations. Zetter's explanation of the cyber operation in Ukraine speculated that the assailant recognized the protesters as a system and when targeting one of those components, the power station, forced the protesters to change their behavior, which reduced pressure against the pro-Russian forces. As for the compromise of the Democratic National Committee, the Department of Homeland Security assesses that a nation conducted a strategic level operation on a single component of the larger system to achieve a desired effect or behavior that benefits the assailant. In this case, as the Department of Homeland Security explains, the Russians targeted the actual voters with information acquired from hacking the Democratic National Committee. The Department of Homeland Security further explained that the information that the Russians had allegedly acquired was then used to sway voter opinion to help the desired candidate to win. Another good example, according to the War College, is Russia's usage of effects based operations in the cyber domain against the Georgian hacking forums in conjunction with the Russian invasion of Georgia in order to prevent possible strikes against Russian cyber targets. In this incident, the

Georgian hacker's communications channels were eliminated when the Russians took out the Georgian hacker's popular forum site.

These examples showed that although the concept of effects-based operations may not have been doctrine during their respective times, it does show that leaders at the strategic level had a higher level of understanding when it involved conducting operations at the strategic level. As it pertains to these cases, all leaders involved understood that enemies are made up of several components that create a system. The leadership also understood that they could win by targeting all components of the system, instead of only targeting the fighting force. The understanding of an enemy being comprised of several different components brings up the second theme, the enemy as a system.

A Target as a System

When talking about the cyber domain, the cyber domain can be observed by the targeteer as a system in of itself, or as part of a larger system. Cyber as itself is easy to see as a system comprised of several different components such as servers and clients. The Department of Defense explained that any computer network could have any number of servers that host different services and all those services work together in concert to provide a service for the clients to use creating an entire system. However, Smith stated that effects-based operations leverage the utility of targeting a system when considering the enemy as a system; therefore, the cyber domain should be considered as one of those components to the enemy system that a targeteer can target. Similarly, the cyber domain can also be described by the targeteer as a system. As the War College explained, multiple components make up the cyber domain to include various servers, workstations, and other specialized devices. If a targeteer targets a single

server on a network, like a domain name server or a dynamic host configuration protocol server, the targeteer could potentially incapacitate the entire network.

According to the Department of Defense, when a targeteer decides to target a portion of an enemy's system in the cyber domain the targeteer first wants to look at what is the effect or behavior that the targeteer wants to achieve. Rickerman continued this explanation by stating that after determining the desired effect, the targeteer needs then to look at all the different components that exist in cyber as it pertains to the target and find out how the different components are linked to the target. Rickerman also explained that once the targeteer establishes the various linkages to the different components of the system is complete, creating a cause and effect type relationship, the targeteer can then make a determination on how manipulating different components to the system, as well as their linkages, could achieve the desired effect or behavior. However, Beagle explained that considering the enemy as a system and targeting only a single part of that system may not yield the desired behavior which would require targeting of all the other parts of the system as well.

There are similarities between the Russian cyber-attack on the Georgian hacker forums, and the targeting process used to target the smaller cyber component in a larger system that caused a desired behavior. The War College considered the Georgian hacker forums as a communications channel between the Georgian hacker groups. A communications channel that the Georgian hackers could have used in order to communicate between the different cyber hacker groups and coordinate strikes against Russian cyber targets. A Russian targeteer could have easily discovered how these Georgian hackers used these forums for communications in-between the Georgian hacker groups in which the Russian targeteer would then understand the linkages between the Georgian hacker forums and the Georgian hacker groups. A Russian

targeteer could then decide that denying access to the Georgian hacker forums could stop any possible counter offensive cyber operation against Russian cyber targets that the Georgian hacker groups could have developed by eliminating the Georgian hackers' communications and coordination capability. During the Russian invasion, denial of the Georgian Hackers' forums obviously had an effect on the Georgian hackers because of the Georgian hackers' reliance on the forums for communications and coordination. Without the capability to communicate and coordinate, the Georgian hackers were unable to mount a cyber offensive operation against any Russian cyber targets.

The Democratic National Committee hack is another good example of effects-based operations in the cyber domain of a larger enemy system. In this example, the linkages are more indirect and deal with the release of information and how the release of that information influenced the populace. Specifically, as the Department of Homeland Security stated, Russia used information operations in the past to influence citizens of foreign countries. In this example, the Department of Homeland Security explained that Russia's intent, when Russia allegedly released the Democratic National Committee information, was to influence the voting public during the United States 2016 presidential election. The information, therefore, links the Democratic National Committee to the United States population by the influence the information created when Russia had allegedly released the information. By hacking the Democratic National Committee and releasing the information collected, the Department of Homeland Security understood that there is a strong possibility that the behavior of the voters had changed, due to the information's influence, from what would have happened if they were not exposed to the information, as Russia had intended. This example also showed how expansive an enemy system could be, which may take a considerable time to map out the enemy system to determine what

targets can be developed and what kind of effect that actions on the developed targets may create.

Target Development Process

One of the key pieces of this research was to discover a process to conduct effects-based operations in the cyber domain. However, none of the literature reviewed talked about how to conduct effects-based operations in the cyber domain. Due to the abstract nature of effects-based operations, this process should not be hard to develop, as long as the targeteer places focus on the core of what effects-based operations are considered. Rickerman explained that the core of effects-based operations is considered as, developing targets utilizing a holistic and systematic approach. The cyber domain is just another dimension to take into consideration when a targeteer is building out a system that is a target. As Rickerman explained, the key is that the targeteer needs to understand the behavior that occurs when one of those components, referring to the cyber domain, in this case, are manipulated. Therefore, developing a target as a system involves systematically discovering all components of that system, to include the linkage of that component to the actual target, and the possible effect on the target if the targeteer manipulated the component or the linkage

The War College believed that in the Georgian hacker forum's incident, the Georgian hackers were the actual target. The Georgian hackers are a system that consists of other components. These components could be their computers, their Internet Service Provider, their email server, or the forums of which they frequently visited. To understand the Georgian hackers as a system, a targeteer builds out the system, and if the Georgian hackers did use some kind of forums for communications, then they needed a server to host the forums. Therefore, denying access to the server that hosted the Georgian hacker's communications, in this case, the Georgian

hacker forums, indirectly affects the Georgian hackers. Smith explained that understanding the cause and effect nature of effects-based operations is how a targeteer can understand how to affect, indirectly, the target through the second and third orders of effects of the targeteer's targeting. However, Rickerman's stance is that this type of targeting may backfire if there are other undesirable effects.

When looking at the Democratic National Committee hack, the election process could also have several different components to it. The targeteer could consider the candidates, the voting machines, and the voters as components of the electoral process. Each of those components also has other sub-components. For instance, the candidates might need the necessities to stay alive, the voting facility might require electricity, and the voters might require information to decide whom they choose to vote. All of these components come together to create a system that is the whole target. In this case, the target is the United States and its election system. After building the system, a targeteer can now determine how each component, when manipulated, can directly, or indirectly affect every other component of the system. After this discovery process is complete, the targeteer can decide which component to target directly, that will cause the desired effect against the component that they are indirectly targeting. As it applied to the Democratic National Committee hack, the Department of Homeland Security explained the Russians possibly targeted the information being received by the voters, to indirectly affect the election results.

Both of these examples show that the targeteer involved first looked at each target as a system. The targeteer then looked at how each component of that system affects each other. As Rickerman stated, after fully understanding the entire system, and its sub-components, the targeteer decided what effect or behavior they wanted to influence on the actual target. The

targeteer then decided what component or subcomponent they were targeting that would cause a second or third order effect to achieve the desired effect or behavior. According to the Department of Defense, the last piece to the target development process would be to determine the tool or weapon used based on what the desired effect or behavior is.

Orders of Effects

As demonstrated with the Ukraine power station and Democratic National Committee examples, the intended target does not have to have a direct association with the actual target, and therefore do not have to have a direct effect, on the intended target. Smith explains that due to these effects not having a direct association with their target, effects-based operations typically involved second and third orders of effects. Smith expanded on the idea of second and third orders of effects by explaining and referring to them as indirect effects, as opposed to direct effects. Smith continued to explain that these orders of effects are also numbered sequentially to indicate which order they occur. The goal in effects-based operations is to maximize the desired effect while minimizing the undesired effects. However, this is what can make effects-based operations somewhat unpredictable, when the targeteer does not take into consideration all the possible effects, or when an effect or behavior is misjudged. Figure 5 exemplifies how complicated effects based operations can get when taking into consideration all the possible effects.

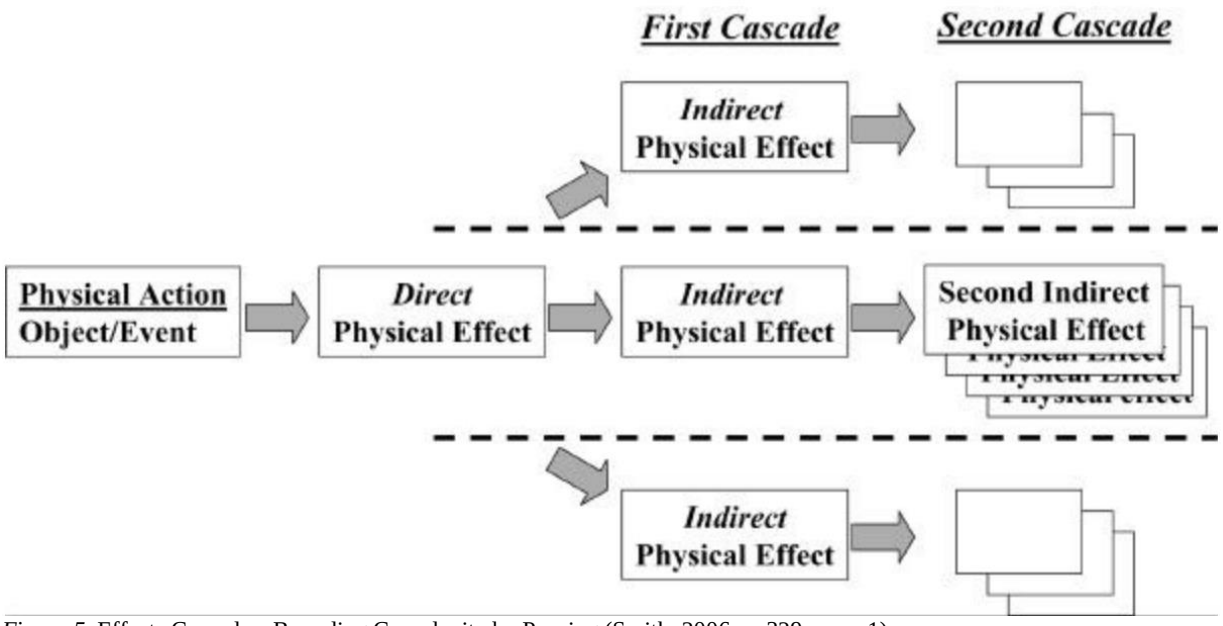

Figure 5. Effects Cascades: Bounding Complexity by Pruning (Smith, 2006, p. 329, para. 1).

When analyzing the situation involving the Georgian hacker forums, the direct approach to neutralizing the Georgian hackers could have included either capturing them with soldiers or killing them with air strikes to stop the Georgian hackers from conducting a retaliatory strike on a target in the cyber domain. However, there is a possibility, due to the global presence the initial invasion had, that the death or detainment of the Georgian hackers would have had negative side effects on the Russian government. The possibility of negative side effects is why the Russians choose a different approach to neutralizing the Georgian hackers. By targeting the Georgian hacker forums with a cyber weapon, one of the indirect effects was changing the behavior of the Georgian hackers by eliminating the communications and coordination channels. The attack on the Georgian hacker forums also provided a message to the Georgian people that the Russians have more than the conventional capabilities and that they are willing to use those capabilities against the Georgian people.

When looking at the Democratic National Committee hack, it is easy to see that the actual target was the United States, not necessarily the election. In this case, according to the

Department of Homeland Security, the Russians hacked the Democratic National Committee to obtain emails that the Russians allegedly released to United States voters to sway public opinion. This use of influencing the public opinion is what Russia wanted to set up a presidential administration that could be friendlier to the Russian Government. One of the other effects is due to the outrage by the Democratic Party, the protests following the election and inauguration caused some instability within the United States. Hypothetically speaking, this instability could have also been one of the intended effects that Russia had wanted. However, why did Russia not just directly target the voting machines in the necessary states? It could have been the lack of ability to hack the electronic voting machines, or maybe the states that Russia needed to turn did not use electronic voting machines. A possible answer is that if United States election officials discovered that Russia had directly interfered with the elections via the electronic voting machines, then the election could have been delegitimized and a revote could have occurred, possibly changing the outcome of the election. Indirectly targeting the voters with an information operation consisting of negative emails directly from the Democratic National Committee allowed the American people to make the choice still, preventing the presidential election from being delegitimized.

Both of the previous examples put into perspective the concept of orders of effects and how they work with effects-based operations. A targeteer can see how distant they can get from the actual target by targeting a component within the system of the target. Smart understood that keeping the targeteer's effects separated from the actual target makes it more difficult for the target or an outside observer, to determine the true target and the motivations of the targeteer for targeting the target. This plausible deniability is why it may be difficult to understand the real motivations for Russia in both of these examples. Another reason to use effects-based operations

is that when the targeteer distances themselves from the target, it increases the difficulty of attributing the targeting. Even though the United States government may be confident in attributing both of these attacks to Russia, the United States has not conclusively identified Russia as the suspect nation.

Use in Strategic Targeting

The elements of national power consist of four different dimensions, which Forestier listed as political, economic, diplomatic, and military. Smith postulates that the proper use of these elements against a nation would force that nation to make a specific decision. Therefore, as Rickerman concurred, if properly leveraged, these dimensions can be used by state leaders to change the behavior of another nation's government. However, by utilizing effects-based operations against the cyber domain, there is a possibility that targeteers can affect another nation's elements of national power.

In a hypothetical situation, another nation-state may want to see Venezuela collapse in order to invade and that the nation-state in this example decides to conduct cyber operations against Venezuela to make the country collapse. As a cyber attack, this nation-state may decide to hack into Venezuela's oil industry. In this case, the goal isn't to destroy Venezuela's oil capability, but rather to temporarily reduce Venezuela's oil production capability to a temporary halt. Instead of hacking the Venezuelan oil industry and disrupting operations completely. The attacking nation-state could obtain entry into the Venezuelan oil industry and subtly start reducing Venezuela's oil production, possibly though various accidents and equipment malfunctions. Over a period of time, as long as the reduction in oil production continued, the effects based operations in this cyber operation could identify how the cyber operation would affect Venezuela's national power in several ways.

The first and most obvious effect would be a reduction in monetary resources. If oil is one of Venezuela's largest exports, not having enough oil would mean Venezuela could not sell enough of their oil to pay for their obligations. There would not be enough money for the Venezuelan government to supply food and water to their people that live below the poverty level. There would also not be any money to pay for any of the national employees of Venezuela, including its military, reducing Venezuela's military capability. Venezuela could also not buy the military equipment it would need to supply its military, due to the lack of money. Without a funded government or a funded military, the political leaders of Venezuela would no longer have any leverage in their country or the rest of the world. The lack of money and a military would eliminate any political power that the Venezuelan leaders once had. Another national power that Venezuela would have diminished due to the lack of oil production is its diplomatic power. Venezuela has, in the past, provided aid to other nations either via oil exports or though monetary aid. By reducing Venezuela's oil production, Venezuela would lose the ability to influence other nations through its oil or money donations reducing a part of its diplomatic power. However, having an unstable country with no money would also prevent Venezuela from having any diplomatic power.

When looking at the Ukraine power station hacking incident, it is observed that there are several elements of national power involved as well, the first being economical. Since the power stations ownership is through companies in Russia, the longer they are down, the less money those Russian companies make. At the same time, however, controlling the power stations creates a beneficial diplomatic situation for the Russians as being able to leverage the power stations against the Ukraine. However, the Ukrainians reduced this boost to national power after the Ukrainian power station operators gained control back. Controlling the power stations also is

a military benefit as it controlled the will of the people to act against the Russian forces in the Ukraine. Even after the Ukrainian people regained control of the power stations, the Ukrainian people have not been as active against the pro-Russian people.

While analyzing the Democratic National Committee hack, a similar assessment can be made. By affecting the elections to have the preferred candidate voted into office, Russia could achieve a boost in all of its elements of national power. A candidate that would make decisions that would be beneficial to Russia would help Russia politically, economically, diplomatically, and militarily. Also, having a pro-Russian candidate in office would not interfere with Russia when they were making decisions that would benefit Russia, regardless if they were detrimental to the United States or not.

Future Research and Recommendations

With the research of effects-based operations in the cyber domain still being in its infancy stages, there is a lot more work that researchers can do. There are still several questions that researchers need to answer that will help develop this process further. These questions will also give the targeteer the needed information to make the proper recommendations to the commander. These questions include: How does the targeteer mitigate undesired effects? How does the targeteer make the desired effects more predictable? How does the targeteer determine the probability and degree of success of an effect?

Undesired Effects

One of the biggest problems with effects-based operations is the existence of ancillary effects. When dealing with second and third orders of effects, they could undermine the desired effect that the targeteer was trying to achieve all along. When looking at the Ukraine power station incident, one of the undesired effects was Russia being caught. This attribution

delegitimizes what Russia was trying to do in support of the pro-Russian people in the Ukraine. Another negative side effect is that since it is the Russian companies that operated those power stations, the amount of time that those power stations were down equated to money lost to those businesses, which hurt the Russian economy. When hacking the Democratic National Committee, affecting the legitimacy of the election would be a concern. However, to mitigate those effects, the Russians decided to use information operations to sway the opinion of the public rather than hack the voting machines directly. If the Russians lacked the capability to directly hack the voting machines, either because the voting machines were not electronic, or the electronic voting machines were not available in the states that needed to be swayed, indirectly targeting the voting population in the United States with an information operation derived from information discovered from a cyber operation creates the same desired effect as directly hacking the electronic voting machines.

As a part of making the effects-based operations more efficient, researchers need to discover methods on how to mitigate unwanted effects. With the different orders of effects, both direct and indirect, some of those effects are desired by the targeteer, while others are undesirable by the targeteer. Being able to find ways to mitigate the undesirable effects would become beneficial to the targeting process. Mitigating, or eliminating, unwanted effects would also make predicting the end behavior more easily.

Predictability

Being able to guarantee the desired effect would also be beneficial. Knowing there is a high probability of success ties into mitigating the undesired effects. As the more predictable an effect is, the higher probability of success becomes, and the lesser chance that undesirable effects occur, reducing the effort of mitigation the targeteer has to implement. In the Ukraine power

station hack, the actual effect on the people could have been the exact opposite. Instead of quieting the people, these attacks on the Ukrainian power stations could have caused the Anti-Russian protesters to step up activities and cause more harm or damage to pro-Russian people or infrastructure. As for the Democratic National Committee hack, although less likely, the people could have voted against then presidential candidate Donald Trump because the United States voters could see the Russian government supporting Trump.

Making the effects-based operations process more predictable would also be beneficial to effects-based operations. By being able to understand all possible outcomes and developing a process to determine the most likely outcome would lessen any negative effects that an operation could cause. Another option would be to develop ways that would prevent other possible outcomes from occurring, thereby removing them from the list of possible outcomes. By reducing the number of possible outcomes, and making the other possible outcomes less likely, targeteers increase the confidence level that the operation will be successful and achieve the desired effect or behavior.

Probability and Success

When understanding a target as a system, targeteers know there are several different parts that they can target that would affect the system. However, a process needs to be developed that can determine how much of an effect the targeteer can have on the target as they target parts of the system and how the probability of success is achieved as the targeteer increases the number of targeted components. The availability of the probability and success assessments would give commanders the necessary knowledge to determine if and how to attack a target. If the chances of successfully targeting a part of the system are low, then a commander may not want to affect that target at all.

In both the Ukraine power station hack and the Democratic National Committee hack, there could have been a chance that the targeteer did not achieve the desired effect. Worse, the targeteer achieves the exact opposite effect. If the probability of achieving the degree of successfulness were too low, then more than likely the commander would cancel the operation. Being able to know the probability and level of successfulness will help the commander decide to conduct an effects-based operation.

Recommendations

Although several different strategists have utilized effects-based operations for a long time, there has not been a formalized process developed for it. All the authors agreed on what effects-based operations is, no one has tried to write it in doctrine. By extension then, there is not any formalized process to utilize effects-based operations in the cyber domain either. The lack of a formalized process means that the documentation to review and compare for learning about effects-based operations, and how to employ it in the cyber domain, is very limited. However, building a foundation that standardizes effects-based operations and creates a doctrine for effects-based operations in the cyber domain.

The Department of Defense should consider creating a doctrine for effects-based operations. Codifying, and teaching, an actual process for effects-based operations through the military would be the first step in implementing a standardized process for effects-based operations in the more familiar domains of warfare, land, sea, air, space. Once this is completed the process could then be adapted to the newer domain, cyber. Further development of effects-based operations and their uses in the military operations would then make effects-based operations more efficient and more predictable as more people became educated on the process.

After the actual process of effects-based operations is complete and made doctrine, the process should be rolled out to those training to be practitioners of warfare in the more familiar domains. After this initial rollout is complete, the Department of Defense needs to expand the process of effects-based operations to those training to be practitioners of warfare in the cyber domain. Since the domains of land, sea, air, and space are more common in use, they are more familiar to their targeteers. Because of the familiarity to these domains, it should be easier to develop and roll out the new doctrine for these domains.

After developing the doctrine across all the domains, and rolling it out to all those in training, the Department of Defense should then systematically apply this effects-based operations doctrine of the cyber domain to all the services. Having uniformity in how to conduct effects-based operations in the cyber domain will ensure understanding of the effects-based operations process between the different services. Understanding each other's processes will allow each of the service's effects-based operations to be planned together using the same steps preventing any problems that may arise with using different procedures. The end effect is that all effects-based operations will be more synchronized and allow the different services to target different components of the same system uniformly making the process more efficient and successful.

Lastly, to guarantee the success of effects-based operations, the doctrine must include a few more components as discussed previously. The doctrine needs to address how to mitigate undesired effects. The doctrine must also address how to make the effects more predictable. The doctrine must include a methodology to determine the probability and degree of success. These extra pieces will help make concrete and legitimize effects-based operations as a useful piece of doctrine that can help leverage the cyber domain.

Conclusions

Effects-based operations are a different way of looking at targeting. Rather than looking at a target as a singular entity that the targeteer is tasked with destroying or neutralizing, the target should be looked at as a system of components that can each be individually targeted to achieve the desired effect. The cyber domain is quickly becoming involved in everything from remote controlling devices to communications between people. , a component that exists in the cyber domain can now be leveraged by a targeteer against the larger system. For the power companies in Ukraine, the cyber domain facilitates the flow of electricity. For the Democratic National Party, the cyber domain is a vital communications system. Both of which were exploited to achieve the desired effect against the anti-Russian protesters and American voters, respectfully. Indirectly targeting a target by directly targeting a component in the system that makes up the target, causing second and third orders of effects to the target, which achieve an end goal.

The easiest way to apply conventional effects-based operations to the cyber domain is to understand that the cyber domain may be a component of a target's system. Now the targeteer needs to understand that there is one more component to the system that he can look at and find a way to exploit. However, this means the targeteer needs to understand all the areas of which the cyber domain now has a presence in the target's system. Due to the widespread possibilities with the cyber domain, this may become overwhelming for the targeteer. However, it does widen the number opportunities to attack the target's system. Instead of an adversary causing permanent physical damage to power stations to quell a population, the adversary can now take power stations temporarily offline. Instead of an adversary trying to force people to vote a specific way, the adversary can now change voter opinion through obtained emails.

Due to the complexity of the cyber domain, there is a need for a different strategy for targeting. Effects-based operations detail a different strategy that allows targets to be engaged in ways that previously the targeteer never considered. Effects-based operations also provide flexibility to targeting that allows the targeteer to leverage the utility of the cyber domain against the advisory. Now innocuous things such as control systems and email can be leveraged by the targeteer within a system to obtain the desired effect against the targeteer's target.

Even though it is very challenging to determine if a nation is utilizing an effects-based operation as a method to conduct targeting against an advisory, it can be understood how they could be doing as such; especially when the operation in the cyber domain is several degrees removed from the target. In this way, an observer or analyst can perceive that Russia utilized effects-based operations to determine a way to target the Georgian hackers and stop their possible counter cyber operations. An observer or analyst can also perceive how Russians utilized effects-based operations to try to change the opinion of voters during the 2016 United States elections. In both examples, an observer or analyst can perceive that the power stations in Ukraine and the e-mail server in the Democratic National Committee are components being targeted separated, sometimes by several orders, from the desired effect of quelling the anti-Russian protesters and changing the opinion of United States voters, respectfully. This separation of a targeted component from the desired effect is the core of effects-based operations.

The cyber domain offers targeteers a new dimension to conduct targeting. Effects-based operations leverage the utility of the cyber domain and offer a flexibility not available in other targeting strategies. Leveraging the effects-based operations approach to targeting in the cyber domain will garner a wider breadth of opportunities to target adversaries that previously were not

targetable. This is a strategy that can be used by other nations, and it can be developed and utilized by the Department of Defense for future operations.

References

Batschelet, A. W. (2002). Effects-based operations: A New Operational Model? [Scholarly project]. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a404406.pdf

Beagle, T. W., Jr. (2000). A391749 Effects-based operations Another Empty Promise? (Master's thesis, School of Advanced Airpower Studies, 2000) (pp. 1-127). Maxwell AFB: USAF. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a391749.pdf

Brantly, A. F. (2015). Strategic Cyber Maneuver. Small Wars Journal, 1-12. Retrieved from http://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver

Davis, P. K. (2001). Effects-Based Operations: A Grand Challenge for the Analytical Community (pp. 1-117, Rep.). RAND. Retrieved from http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR1477.pdf

Department of Defense. (2013). Joint Publication 3-12(R) Cyberspace Operations. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Department of Defense. (2013). Joint Publication 3-60 Joint Targeting. Retrieved from https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf.

Department of Homeland Security. (2016, October 7). Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security. Retrieved from https://www.dhs.gov/news/2016/10/07/jointstatementdepartmenthomelandsecurityandofficedirectornational

F-Secure. (n.d.). THE DUKES: 7 years of Russian cyberespionage (Tech.). Retrieved from https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

FireEye. (2016). / RED LINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE (pp. 1-16, Rep.). Milpitas, CA: FireEye. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

Forestier, A. M. (2006). Effects-Based Operations: An Underpinning Philosophy for Australia's External Security? Security Challenges, 2(1), 1-20. Retrieved from https://www.regionalsecurity.org.au/Resources/Files/vol2no1Forestier.pdf

GlobalSecurity.org. (n.d.). World Wide Aircraft Carriers. Retrieved from http://www.globalsecurity.org/military/world/carriers.htm

Guarnieri, C., & Anderson, C. (2016). Iran and the Soft War for Internet Dominance. Retrieved from https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf

Guinness World Records. (n.d.). First standing army. Retrieved from http://www.guinnessworldrecords.com/world-records/first-standing-army

Ho, J. H. (2006). Waging Effects-Based Operations. Security Challenges, 2(1), 157-168. Retrieved from https://www.regionalsecurity.org.au/Resources/Files/vol2no1Ho.pdf

Mueller, Karl (2010). Air Power. Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/pubs/reprints/RP1412.html

NationMaster.com. (n.d.). All countries compared for Military > Air force > Combat aircraft. Retrieved from http://www.nationmaster.com/country-info/stats/Military/Air-force/Combat-aircraft

NATO. (2017). Cyber defence. Retrieved from http://www.nato.int/cps/en/natohq/topics_78170.htm

Palagi, J. E. (2015). Wrestling the bear: the rise of Russian hybrid warfare (Master's thesis, National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School, 2015) (pp. 1-53). Joint Forces Staff College Joint Advanced Warfighting School. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a622700.pdf

Philbin, M. J. (2013). Cyber Deterrence: An Old Concept in a New Domain (pp. 1-32, Rep.). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a589940.pdf

Rickerman, L. D. (2003). Effects-based operations: a new way of thinking and fighting (Master's thesis, Thesis / Dissertation ETD, 2003) (pp. 1-48). Fort Leavenworth: United States Army Command and General Staff College. Retrieved from http://www.au.af.mil/au/awc/awcgate/sam/ebo_rickerman.pdf

Smart, S. J. (2011). Joint Targeting in Cyberspace. Air and Space Journal, 65-75. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a555785.pdf.

Smith, E. A. (2006). Effects-based operations: applying network centric warfare in peace, crisis, and war. Washington, DC: CCR Publication. Retrieved from http://www.au.af.mil/au/awc/awcgate/ccrp/ebo_smith.pdf.

United States Army War College. (2016). Strategic Cyberspace Operations Guide (pp. 1-152, Rep.). Retrieved from https://csl.armywarcollege.edu/usacsl/Publications/Strategic_Cyberspace_Operations_Guide_1_June_2016.pdf

Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. New York: Crown.

Zetter, K. (2016, March 03). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Appendix

Appendix A – Russian Primary Goals of Cyber Operations Against Georgia

The War College believed that Russia's primary goals were as follows:

d. Deny – Degrade. Russian cyberspace forces attacked civilian sites near the action of kinetic operations with the goal of creating panic in the civilian population. For example, in the town of Gori, Russians disabled government and news websites with DDoS attacks just prior to an air attack. Cyberspace interdiction (attacks concentrated on tactical data links and data fusion centers) degraded and disrupted the Georgians' decision cycle limiting their military response.

e. Deny – Disrupt. The Russian cyberspace operations forces disrupted Georgian government, military, and diplomatic communications.

(1) Government and military communications. When the kinetic battle started on 7 August, Russian government and irregular forces conducted distributed denial-of-service (DDoS) attacks on Georgian government and military websites. These attacks disrupted the transmission of information between military units and between offices in the Georgian government.

(2) International communications. Faced by overwhelming Russian air power, armored attacks on several fronts, an amphibious assault on its Black Sea coastline, and devastating cyber-attacks, Georgia had little capability of kinetic resistance. Its best hope lay with strategic communications: transmitting to the world a sympathetic message of rough treatment at the hands of Russian military aggression. But Russia effectively used cyberspace operations to disrupt the

Georgian government's ability to assemble and transmit such a plea thus removing Georgia's last hope for international support.

f. Deny – Destroy (potential). The Russians were very sophisticated in their target selection. For example, Russians refrained from attacking Georgia's most important asset, the Baku-Ceyhan oil pipeline and associated infrastructure. By holding this target in reserve, the Russians gave Georgian policymakers an incentive to quickly end the war.

g. Manipulate. Although there were no know attempts to manipulate data, the Russian cyberspace operations forces dislocated Georgian data flows, shunting data that normally would have traveled over the Internet into more traditional conduits such as telephone and radio communications. Georgians were trying to transmit more data at a higher rate than the useful capacity of their information network could accommodate because a large proportion was being consumed by cyber-attacks injecting extraneous data into the network. The cyber-attacks effectively jammed Georgia’s overall information network during the early stages of the war when rapid and organized action by Georgian defenses, cyber and kinetic, could have had the greatest impact.

h. In summary, Russian planners tightly integrated cyberspace operations with their diplomatic, information, military, and economic elements of power (i.e. DIME). The Russo-Georgian war provides a case study for joint planners preparing for a future conflict, involving the new domain of cyberspace.

Entire List (War College, 2016. p. 55, para. 5).