and employs multiple computers to conduct a DoS.[14] This flood of traffic will cause the system to slow or stop functioning, denying the user function of the target system. To further illustrate a DDoS there are examples of hundreds or thousands of corrupt computers swamping a company or country's networks and preventing them from functioning.[15]

Zero-day vulnerabilities are vulnerabilities in computer software not disclosed publicly, software that cannot be corrected, and that anti-virus products cannot detect. [16] A simpler definition of a zero-day vulnerability is a hazard that is so new that viable protection against it does not yet exist.[17] Zero-day vulnerabilities are rare discoveries. In fact, there are approximately twelve million varieties of malicious code found each year and only a dozen of them are zero-days.[18] Vulnerabilities can be used to access a system in order to use malicious code on that system. Typical software systems operate from millions of lines of computer code and therefore, vulnerabilities may exist for years before being recognized. Identifying a vulnerability before the software producer or user is aware results in zero-days being extremely valuable in cyberspace operations. In fact, some say that zero-day vulnerabilities are the most prized possessions of those conducting nefarious actions in cyberspace.[19]

With the definitions of malicious code, DoS, DDoS, and zero-day vulnerabilities in mind,

---

[14] "Understanding Denial-of-Service Attacks," *United States Computer Emergency Readiness Team*, accessed December 15, 2015, https://www.us-cert.gov/ncas/tips/ST04-015.

[15] Joseph S. Nye Jr., *The Future of Power* (New York, NY: Public Affairs, 2011), 126.

[16] Leyla Bilge and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," *Conferences on Computer and Communications Security* (2012): 833.

[17] Byron Acohido and Jon Swartz, *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity* (New York, NY: Union Square Press, 2008), 5.

[18] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Business, 2014), 7.

[19] Zetter, 6.

the key to using these in cyberspace operations is access. There are really only three types of access in cyberspace: authorized, unauthorized, and other than authorized. Authorized access is a fairly simple concept in that a user of a computer or network system is allowed and expected to access the system. Unauthorized access is access gained on a system through nefarious means such as cracking a password or somehow bypassing authentication controls. Other than authorized access, is access gained on a system or network simply by connecting, navigating, requesting, or unwittingly being granted access. Other than authorized access may be the result of the system not requiring credentials (password), or lack of authentication controls.

A tangible example that helps differentiate the three types of access can be expressed in terms of an individual's home. If the individual invites someone into their home and they enter, they have authorized access. If someone breaks into another's home by picking a lock or breaking a window, this as unauthorized access. Finally, if someone has not been invited into another's home but sees a door has been left open so they enter it, this is considered other than authorized access. This distinction is important in cyberspace because, just as someone does not expect a stranger to enter their home without being invited, even though a door was left open, system owners often do not expect others to access their networks or computer systems, even though there are no credentials required. It is important to realize that some connected systems may allow access without extreme effort, therefore, other than authorized access provides the easiest path to access in cyberspace. It also provides an intruder plausible deniability because no nefarious means were used to gain access.

Gaining access is key in cyberspace operations, regardless of the type, because without access none of the tools defined above are useful. In terms of warfare, no munition can be fired in cyberspace without access to the target networks or systems. Access may take a lengthy amount of time and require specific intelligence to obtain, so preparing for offensive cyberspace operations requires defined targets and desired effects on those targets well in advance of the need for the capability. Therefore, it is reasonable to conclude that the ideal timing for identifying

access points occurs during periods of putative peace and not in the midst of other offensive military operations.[20]

Historical Review of Military Theory

Now that key cyberspace concepts have been defined, and the important of access illustrated, it is useful to look at history to examine the evolution of military theory and doctrine in order to recommend how cyberspace can be integrated. Absent from this review is an analysis of the space domain. Although continued work in the realm of space warfare requires exploration, it is outside the scope of this paper.

Key elements of western military theory and doctrine, regardless of domain, trace back to two individuals – Antoine Henri Jomini and Carl von Clausewitz, who wrote about the phenomenon of war in the 19th century. Significant to both of these theorists were the limited capabilities available to their forces at the time. In the 19th century, land armies mainly had to coordinate and synchronize actions of infantry, cavalry, and artillery. Jomini and Clausewitz had little exposure to the concept of coordinating the capabilities of multiple domains. While their theories focused on the land domain, they did influence later thinking in other domains because of the common application of their ideas.

Land Theory

Jomini, who served under Napoleon Bonaparte, viewed war as having universal principles and saw the conduct of warfare in a linear and practical model. He believed that finding a decisive point to maximize concentration of force was paramount. Jomini also wrote about the importance of initiative, mobility, and movement to support concentrating force along lines of operation.[21] As demonstrated in 19th century wars throughout Europe, using a linear

---

[20] Campen, 5.

[21] Azar Gat, *A History of Military Thought: From the Enlightenment to the Cold War* (New York, NY: Oxford University Press, 2001), 118 – 119.

approach to war by developing lines of operation and concentrating force at a decisive point were routinely successful. The French victory in 1805 at the Battle of Austerlitz is a prime example of the importance of mobility with land forces, integration of artillery, and designation of decisive points in land warfare.[22] This battle undoubtedly shaped Jomini's theory of warfare. While military theory moves away from Jominian principles of warfare because of its reductionism, there are some principles that remain valid in specific contexts and continue to influence theory and doctrine. In fact, for the US military, its doctrine points to principles of war such as offensive, mass, and objective all of which link back to Jominian theory of the 19th century. [23]

Clausewitz, while serving in the Prussian Army against Napoleon, presented himself as a critic of Jomini's military theory believing it was characterized by rules and principles.[24] Clausewitz believed war fit more in the realm of art than in science, however, he professed that it should not be thought of as only one or the other. Instead, he advocated war as fitting into the human social existence similar to commerce, but saw it best compared to politics.[25] In other words, Clausewitz viewed the phenomenon of war through a much wider aperture than Jomini. Clausewitz viewed rules and principles as legitimate only as long as their values and limits were understood correctly.[26] Like Jomini, Clausewitz searched for fundamental laws of war, but insisted that in practice the laws are subject to an infinite number of variations. Instead of focusing efforts on decisive battle, he believed it necessary to look at the nature of war and the

---

[22] R. Ernest Dupuy and Trevor N. Dupuy, *The Harper Encyclopedia of Military History: From 3500 BC to the Present*, 4th ed. (New York, NY: Harper Collins Publishers, 1993), 818.

[23] Joint Publication 3-0, *Joint Operations* (Washington DC: Government Printing Office, 2008), I-2.

[24] Gat, 167.

[25] Clausewitz, 149

[26] Gat, 199.

political end intended from conflict. He looked past the integration of arms to achieve military end states and advocated that military means should all serve to meet a political end. After all, Clausewitz claimed warfare to be an extension of politics carried out by other means.[27]

Clausewitz was opposed to any effort to write doctrine based on laws of war, afraid of rigid application of abstract rules on the battlefield.[28] He wrote about theory, but stressed that it not be used as doctrine or as a manual for action.[29] In Clausewitz's view, theories on warfare should be more descriptive than prescriptive. While there are similarities between Jomini and Clausewitz, the key difference is the prescriptive nature of Jomini and his more systematic view of warfare. Just as Jomini's theories have persisted through time, so have Clausewitz's. Current US military doctrine includes Clausewitz's ideas of maneuver, economy of force, and unity of command as the other principles of war.[30] While Jominian ideas are being minimized because they are reductionist, his concepts had some influence and evolved through Clausewitz, and both theorists found a place in current US military doctrine.

Maritime Theory

The writings of Jomini and Clausewitz influenced many other writers and thinkers on war. As technologies advanced and capabilities improved, many saw the benefit of actions in various domains supporting one another to reach common strategic objectives. The turn of the century saw the creation of the modern battleship, which greatly influenced both theory and doctrine of sea power. Alfred Thayer Mahan, an American sailor, in the beginning of the 20th century was a leading military theorist and became known as the Jomini of maritime theory.[31]

---

[27] Clausewitz, 605.

[28] Dupuy, 810.

[29] Clausewitz, 141.

[30] JP 3-0, 2008, I-2.

[31] Dupuy, 899.

Mahan studied Jomini and wanted to develop a systematic approach to naval warfare.[32] In Mahan's view, naval doctrine would place importance on battleships in order to defeat an adversary's fleet by direct confrontation or decisive battle. He believed in the concentration of force and his theory of sea power became known as "Jomini turned sea".[33] Mahan did not foresee the need to coordinate actions on the sea with actions on land. In fact, Mahan argued that once a naval force had command of the sea, everything else would follow making land forces unnecessary.[34] While this theory was disproved, the idea of a new capability dominating in war persisted. Jomini influenced Mahan's approach to naval warfare and his insistence on systematic approaches, decisive battle, and concentration of force are products of this influence.

Another theorist, Sir Julian Corbett, was a prominent British historian whose theories on naval warfare helped shape the Royal Fleet in the 20th century. In contrast to Mahan, Corbett saw the inherent limitations in naval warfare mainly due to the vastness of the sea.[35] He agreed with Clausewitz's work, specifically his ideas on absolute versus limited war.[36] While Corbett concurred with Mahan that command of the sea was an aim, to Corbett it was not the only one. Corbett viewed naval warfare as only one branch of the phenomenon of war as the whole, helping to evolve the theory of sea power. [37] As a historian, Corbett studied past wars fought with sea power and concluded that the majority of failure could be traced to the insufficient number of troops available to conduct follow on land operations. He wrote, "men live on land, not upon the

---

[32] Gat, 448.

[33] Ibid, 458.

[34] Ibid, 477.

[35] Julian S. Corbett, *Principles of Maritime Strategy* (New York, NY: Dover Publications, Inc, 2004), 56.

[36] Gat, 482.

[37] Ibid, 487.

sea…it is impossible that war be decided by naval action alone."[38] Corbett's influence could illustrate the first genuine push for combined military operations in western military culture; the idea that operations in various domains were needed to meet an objective.

J.C. Wylie summarized an example of Corbett's theory in *Military Strategy*. Wylie wrote that maritime theory was the establishment of control of the sea and exploitation of such control towards the establishment of control of the land.[39] Both Corbett and Wylie viewed sea power as complementary to operations on land. These ideas directly countered Mahan's on many levels. Just as Jomini preceded Clausewitz on land, Mahan preceded Corbett on the sea. The advance of military theory from each expanded the original ideas of a more scientific and systematic approach to a more creative and flexible approach to war. In both domains, early theories were matured without completely disregarding the original principles.

Air Theory

The next major advancement in technology that opened an entirely new domain was that of the aircraft. The first military aircraft flew operations in World War I (WWI), and by its end, aircraft served as bomber, pursuit, and observation platforms. The end of the war offered a period to reflect on the use of aircraft in military operations and to develop theories on air power. It was quickly recognized that air power would play an essential role in future warfare.[40] Ironically, the development of air power theory follows that of sea power. The most prominent air power theorist, who followed in the footsteps of Jomini and Mahan, was Italian Colonel Giulio Douhet. Upon retiring in 1921, Douhet wrote, *The Command of the Air*, which was praised as doctrine of

[38] Gat, 487.

[39] J.C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, NJ: Rutgers University Press, 1967), 39.

[40] John Andreas Olsen and Martin van Creveld, eds., *The Evolution of Operational Art: From Napoleon to the Present* (Oxford: Oxford University Press, 2011), 143.

winning wars by the use of air power.[41] Douhet believed that through air power alone the enemy's will could be broken by violent and destructive bombardments. He insisted that air power be independent of, and coequal with, land and maritime forces. Douhet believed that air power presented the most promising strategy for victory. Success lay in the ability to concentrate mass munitions onto decisive points for a grand air offensive.[42] It is as though Jomini himself could have written the same had the technology of aircraft been available. One of Douhet's disciples was Brigadier General William Mitchell, former chief of US Army's Air Corps. Mitchell challenged traditional American military hierarchy and influenced current US military doctrine through his advocacy of Douhet theory.[43]

Douhet's theory of the exclusive use of air power proved ineffective in a number of wars. One example was the Battle of Midway in 1942. During this battle, fifty-five sorties of bombers dropped three hundred and fourteen bombs over a three-day period, only to have a direct hit on one Japanese battleship.[44] Clearly, the Battle of Midway was not going to be won through air power alone. Regardless of countless examples of air power alone being ineffective at obtaining decisive victories, Douhet's theory of air power continued to garner positive views in western military circles throughout the 20th century.

The US military had two schools of thought concerning air power; the bombers and the fighters. While Douhet and Mitchell were clearly bomber supporters, one theorist who supported fighters in air power was Colonel John Boyd. Boyd was a fighter pilot who flew for the US Air Force in the Korean War. He is most famous for the Observe, Orient, Decide, Act (OODA) loop,

---

[41] Dupuy, 1089.

[42] Gat, 577.

[43] Dupuy, 1147.

[44] Thomas Wildenberg, *Billy Mitchell's War with the Navy: The Interwar Rivalry Over Air Power* (Annapolis, MD: Naval Institute Press, 2013), 182.

which he developed in a presentation he titled *Patterns of Conflict*. Boyd detested the air power theories espousing the use of bombers and bombers alone to decide conflicts. Instead, Boyd advocated for lighter and more agile fighter aircraft so the US Air Force could gain air superiority and negate threats to their bombers, naval vessels, and land forces. He developed his OODA loop based on his experience as a tactical fighter pilot, but it has influenced many modern military theories outside of the air domain. For example, his OODA loop is referenced a number of times in the US Marine Corps Doctrine Publication 1 (MCDP-1), *Warfighting.*

Boyd's theory is aligned with Clausewitz and Corbett. Some themes contained within *Patterns of Conflict* are tempo, initiative, speed, and maneuver. Included in Boyd's work was direct reference to Clausewitz. While Clausewitz and Corbett did not benefit from the technological advances in aircraft, they both would have supported incorporating new technology to complement current capabilities in the conduct of warfare. Boyd, like Clausewitz and Corbett, did not see war in a linear, systematic, scientific manner. Rather, their theories stressed flexibility and adaptation, viewing war as more of an artform or realm of human interaction.

Synthesis of Theories

Throughout history, theories of warfare have evolved due to technologic innovation or increases in capability. While there are some striking differences between early theories and later ones in each domain, it is paramount to appreciate the similarities and influence early theories had as each domain matured. The intent to review past theories of warfare is not to discredit any one theory. In fact, all past theories have merit and still influence theory and doctrine today. As an example, during the interwar period between the first and second world wars, the US military viewed center of gravity and culminating points as key elements of warfare. These elements directly tied back to Clausewitz's writings, and are still used today. In addition, the US military

uses decisive points and lines of operation in its doctrine linking back to Jomini's original principles of warfare.[45]

An early amalgamation of military theories introduced three principles of war: concentration of forces, security, and objective.[46] Although Clausewitz was hesitant to list a finite set of principles regarding war, he did articulate similar factors to consider.[47] These principles continued to influence US military doctrine and were introduced in Training Regulation No. 10-5, published in 1921 by the US War Department. In this publication principles of war included: objective, offensive, mass, economy of force, movement, surprise, security, simplicity, and cooperation.[48] Nearly a century later, the US military maintains strikingly similar principles of war in its joint doctrine. The key is that these past theories of warfare have all influenced modern theories. Although certain elements of each military theory have been discredited, such as the belief that conducting warfare in one domain will lead to success in war, one should not discount an entire theory or its influence.

Emergent from all the theories discussed is the concept of integration of arms or combined arms operations, wherein one domain does not inherently dominate and win decisive battles. As the evolved theories of warfare have shown, in order to be most effective, capabilities in each domain must be coordinated and synchronized with all capabilities available. Helmuth von Moltke, Chief of Staff of the Prussian Army in the 19th century, mirrored Clausewitz's ideas and stressed the cooperation of infantry, cavalry, artillery, and engineering in an integration of

---

[45] Olsen, 143.

[46] Charles A. Willoughby, *Maneuver in War* (Harrisburg, PA: The Telegraph Press, 1939), 25.

[47] Ibid, 31. Principles of war were listed as objective, offensive, concentration, economy of force, and mobility.

[48] Ibid, 26.

arms.[49] As witnessed in the 20th century in WWII, air power came into its own at sea.[50] This idea is illustrated in the effective use of aircraft carriers during WWII and the additional capabilities it offered the military through the integration of the two domains. The idea of having mutually supporting capabilities in each domain has direct links to the contemporary US military theory of maneuver warfare and combined arms operations.

Maneuver warfare stresses the primacy of gaining positions of relative advantage of an adversary. Combine arms operations incorporate different capabilities or arms so the strength of each is brought to bear in order to expose an adversary's weakness to another capability.[51] The ideal scenario in modern warfare is to gain positions of relative advantage through the implementation of combined arms in order to deliver an adversary a dilemma, where they are faced with a no-win situation.[52] Dr. Steve Biddle wrote about maneuver warfare, believing it to be an "adept fighting technique making greater use of combined arms integration." Maneuver warfare stressed tempo, not speed, where the focus should be transitioning from one mode of action to another before an adversary can react.[53] Maneuver warfare and combined arms operations clearly demonstrate that military power increases when integrating capabilities in various domains and synchronizing them in time and space order to deliver desired effects or outcomes.

Cyberspace offers another domain in which to operate, wherein desired effects may be realized without land, sea, and air forces actually being present. The concept of forces being absent yet still delivering effects can be illustrated by the initial employment of artillery, which

---

[49] Daniel J. Hughes and Harry Bell, eds., *Moltke on the Art of War: Selected Writings* (New York, NY: Ballantine Books, 1993), 154.

[50] Martin Van Creveld, Steven L. Canby, and Kenneth S. Brower, *Air Power and Maneuver Warfare* (Montgomery, AL: Air University Press, 1994), 193.

[51] Creveld, 193.

[53] Ibid, 5.

may have directly influenced Clausewitz and Jomini. Instead of infantry or cavalry coming within striking distance of one another, artillery created depth not seen before on the battlefield and allowed commanders increased flexibility with their forces to maneuver.[54] Cyberspace increases depth exponentially compared to other domains, but the concept remains of having military forces at a distance from the target while having an effect on the target. This comparison is valid with artillery, sea power, air power, and other evolutions in military capability. As history has shown, evolutions in capabilities require evolutions in theory or doctrine.

It seems increasingly probable that the first battles in any future conflict involving technically advanced adversaries will be waged in cyberspace.[55] What may separate this domain from others is the pace and breadth of its effects when included in military operations.[56] Therefore, it is imperative that US military planners seek to identify, understand, and utilize all of the resources available to them, including cyberspace, in order to execute tactical actions with a clear connection to the strategies of the nation.[57] Operational success or failure in one domain influences operations in the others, therefore the domains have become so interconnected that they are interdependent on one another.[58]

---

[54] Walter Schulte, "Lecture: Evolution of Operational Art," September 2, 2015.

[55] Robert Miller and Daniel Kuehl, "Cyberspace and the 'First Battle' in the 21st Century," *Defense Horizons* 68 (September 2009), 2.

[56] Adams, 305.

[57] Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly*, no. 68 (1st Quarter 2013), 53-58.

[58] Olsen, 150.

Evolution of Cyberspace Theory

As early as 1999, cyberspace capabilities were viewed as potentially the most powerful weapon in the 21st century.[59] This sentiment is strikingly similar to the initial reactions to the theories of sea and air power. The National Military Strategy for Cyberspace Operations, published in 2006, declared cyberspace as the fifth domain of warfare, joining land, sea, air, and space in US military doctrine.[60] This strategy acknowledged cyberwar and suggested that cyberspace was "the edifice of modern warfighting capability."[61] The evaluation of the theory of cyberspace warfare could begin with this recognition, but in order to fully appreciate the development of cyberspace warfare theory it requires going back further in history. There are many ways of looking at the dawn of cyberspace theory; however, to get to the core of the theory it is beneficial to start with the dawn of the contemporary Information Age.

The Information Age is thought to have started around 1970; however, it is only in the last few decades that the computer and the microchip have truly revolutionized so many aspects of daily life on a personal, national, and global level.[62] Increasingly the world is becoming more connected. As it becomes more connected concepts such as the Internet of Things (IoT) are being developed. The IoT describes twenty-five billion connected devices or things by 2020.[63] These include everything from the household microwave to jet engines. Cyberspace and the Internet are

---

[59] Byard Clemmons Q. and Gary D. Brown, "Cyberware: Way, Warriors, and Weapons of Mass Destruction" *Military Review* 79, no. 5 (September/October, 1999), 35.

[60] U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Washington DC: U.S. Joint Chiefs of Staff, December 2006), 3

[61] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York, NY: Harper Collins, 2010), 44.

[62] Campen, 35.

[63] Christy Pettey, "The Internet of Things and the Enterprise," *Smarter with Gartner*, August 31, 2015, accessed November 22, 2015, gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise.

related, but should not be confused with one another. Cyberspace is not just the Internet, but instead represents all computer networks in the world, everything they connect to and control, as well as other networks not intended to be accessible from the Internet.[64] The entire world is linked to a degree unthinkable only a few decades ago.[65]

Militaries across the globe are not exempt from becoming connected. The Pentagon alone has an estimated seven million computers connected to over 15,000 networks.[66] Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, and air.[67] By declaring cyberspace as the fifth domain, the US military has taken steps towards accepting the reality of being connected. While cyberspace may be a new military domain by declaration and doctrine, the principles of war such as objective, offensive, mass, economy of force, maneuver, unit of command, security, surprise, and simplicity, developed throughout history, still apply. These principles have been included in US joint doctrine since its inception and their roots can be traced back to the earlier theorists discussed.[68]

In the case of cyberspace, there are examples throughout history of adversaries exploiting telecommunication technologies in wartime through interception of messages and disrupting communication in order to gain positions of relative advantage.[69] While the themes and principles of war still apply, and telecommunication network attack may not be new, there is evidence that

---

[64] Clarke, 70.

[65] Campen, 34.

[66] Nye, 132.

[67] Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 1 (February 2012), 6.

[68] JP 3-0, 2008, II-1.

[69] Healey, 27. Examples the authors offer include telegraph station captures to intercept and send false messages in American Civil War, interception of signals in World War (WW) I, and the advanced signals intelligence of WWII.

the concept of “ground”, which in the past was fairly simple to define, may be changing as human activity increasingly migrates from Earth to cyberspace. In an extreme case, some believe that if this migration continues, then the dominance of future battlespace will be a result of bytes not bullets.[70]

To illustrate this notion of “ground” morphing, think about the global interconnectivity and difficulty it creates in discerning which lanes of this networked world are purely civilian or military.[71] One could argue that the world is so interconnected that there is little or no separation. Some believe it impossible to target via cyberspace without including civilian facilities.[72] In order to tie back to earlier theories in other domains, it is useful to think about how ground is viewed in other domains. For example, sailors and airmen usually think in terms of the entire world, while the soldiers thinks in terms of theaters or battles, almost literally limited to their immediate terrain.[73] One can speculate that Jomini viewed decisive points as physical space that if lost would ruin the enemy. Emile Simpson, author of *War from the Ground Up*, described this struggle between physical ground and other space when discussing the need to see a battlespace and not a battlefield.[74]

Cyberspace skips the battlefield.[75] For cyberspace, the view of terrain is global. This global view is hard to appreciate because in cyberspace and more specifically the Internet, connections are constantly changing making the terrain of cyberspace fluid. While it is seemingly

---

[70] Adams, 14-17.

[71] Campen, 4.

[72] Clarke, 202.

[73] Wylie, 49.

[74] Emile Simpson, *War from the Ground Up: Twenty-First Century Combat as Politics* (London: C Hurst & Co Publishers, 2012), 6.

[75] Clarke, 31.

fluid, it is not impossible to map the geography of the Internet and it generally reflects the geography of Earth.[76] Mapping of the interconnectivity of the Internet is an interesting topic for those conducting military operations and considering systems to target. While the connectivity of the globe is vast, complicated, and complex, it is generally focused around geography and there are a limited number of dense connection points around the world. The battlespace in cyberspace is vast, but it is not unknown. Military leaders must understand cyberspace as global terrain, but they should also not be overwhelmed by thinking it is so fluid no one can ever map it or target dense connection points.

While the separation of civilian and military networks may be a topic of debate, the fact is that vulnerabilities exist in the more connected nation-states via cyberspace more than ever before. There remains an intricate balance in cyberspace power in that the nation-states with the most effective capabilities in this domain may also be the most vulnerable to attack.[77] In his monograph for the School of Advanced Military Studies, Albert Olagbemiro argues that due to an increasing level of vulnerability, the United States has no choice but to move towards a more offensive model in terms of cyberspace.[78] The United States needs to accept its vulnerabilities as in continues to pursue both advanced defensive and offensive national, including military, capabilities in cyberspace.

As the US military operates in cyberspace and theories in this domain mature, it is imperative to look at current frameworks that can assist in ensuring actions in cyberspace are integrated with actions in other domains in order to support military operations. Instead of arguing if cyberspace warfare is the standard for all future military operations, it better to

---

[76] Andrew S. Blum, *Tubes: A Journey to the Center of the Internet* (New York: Harper Collins, 2012), 28.

[77] Adams, 15.

[78] Albert O. Olagbemiro, "Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyber Warfare" (School of Advanced Studies Monograph, US Army Command and General Staff College, 2014), 6.

appreciate the long-standing themes and principles of war, which cyberspace operations still follow. Current frameworks such as JP 3-60 *Joint Targeting*, JP 3-12 *Cyberspace Operations*, and other concepts such as Effects Based Operations (EBO) offer valuable methods of integrating actions in all domains, to include cyberspace, in order to support, enable, and conduct military operations.

Frameworks to Support Operating in Cyberspace

Frameworks exist within US military doctrine that allow complete integration of cyberspace operations and would support a mature cyberspace theory of warfare. The key is to focus on targeting and desired effects. Within JP 3-60 *Joint Targeting*, there is a defined targeting process that starts with defining the objective or end state. Even the early discussions on cyberspace warfare stressed the importance of focusing on an end state or objective.[79] Too often, cyberspace operations are thought of as over-complicated and specialized, and terms like cyber-target or cyber-effect are born. Instead of treating cyberspace differently, the US military would do well to focus more on the targeting cycle as defined in JP 3-60 and less on understanding the intricacies of capabilities available within cyberspace.

Taking an agnostic approach to domains (i.e. land, sea, air, space, and cyberspace) military leaders should focus on the objectives. Once defined, capabilities in each domain can be considered and developed to reach the desired objective. This process is important because too often in cyberspace operations, access-based objectives are developed. In other words, military leaders will define objectives according to the access or capabilities already available in cyberspace. Creating desired effects that accomplish target-related tasks and meet objectives rather than simply servicing a list of targets on the availability of particular weapons systems,

[79] Clemmons, 38.

platforms, or systems misplaces the focus of targeting.[80] In other words, the focus should be maintained on the objective so that specific targets can be identified, effects against the targets defined, and capabilities in various domains developed in order to match objective with capability. This focus follows the phasing offered in JP 3-60, in which capability analysis does not occur until Phase 3 (see Figure 1). As cyberspace doctrine matures, there is an opportunity to correct current deficiencies in an integrated approach through deliberate planning and the joint targeting cycle.[81]

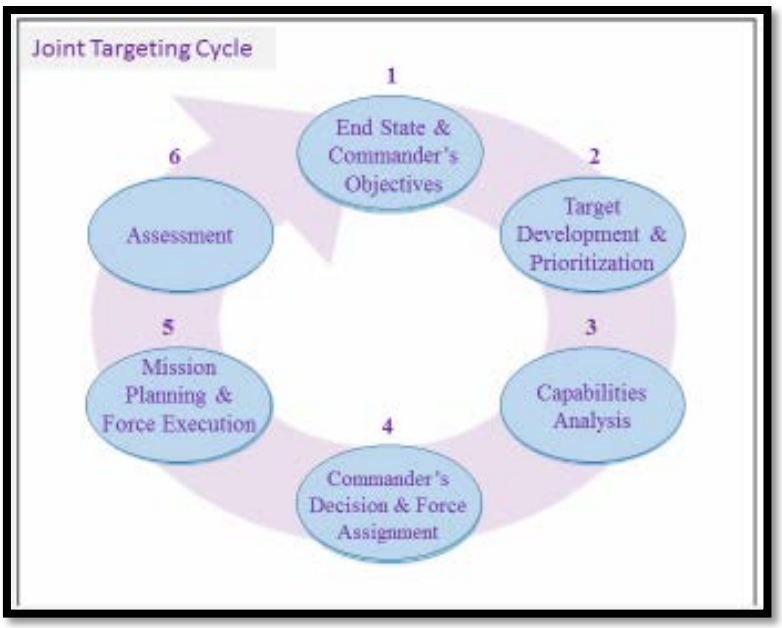

Figure 1. The Joint Targeting Cycle

Source: Joint Publication 3-60, *Joint Targeting* (Washington, DC: Government Printing Office, 2013), II-4.

In addition to JP 3-60, JP 3-12 *Cyberspace Operations*, offers a complementary framework to employ cyberspace capabilities to support military operations. JP 3-12 includes fires in and through cyberspace as a form of power projection that requires inclusion in the joint

[80] Joint Publication (JP) 3-60, *Joint Targeting* (Washington, DC: Government Printing Office, 2013), ix.

[81] Rosemary Carter, Brent Feick, and Roy Undersander, "Offensive Cyber for the Joint Force Commander," *Joint Forces Quarterly*, no. 66 (3rd Quarter 2012), 27.

planning and execution process.[82] While JP 3-12 does not directly reference *Joint Targeting*, the doctrine does align with it stating, "Target development and selection are based on what the commander wants to achieve rather than on the available ways and means to achieve them…focus should be on creating the desired target effects that accomplish targeting-related tasks and objectives."[83] This statement reiterates the dangers of access-based versus effects-based targeting.

Joint doctrine clearly focuses on an effect, result, or objective through the targeting process. As recently as 2008, the term Effects Based Operations (EBO) was in vogue, but has recently become unmentionable in military planning. Ironically, *Joint Targeting* still lists "effects-based" as the second principle of targeting.[84] EBO was a relatively "new idea" in military planning at the turn of the 21st century and some defined it as attacking an adversary's capabilities and thinking, specifically to accomplish the commander's objectives.[85] Other authors argue that EBO is not new at all arguing the concepts of EBO are much as much part of Clausewitz's writings 200 years ago as they are of Sun Tzu's 2,500 years ago.[86] Clausewitz saw the requirement for leaders to define the aim and purpose of an operation so that a series of actions can be determined to achieve the desired aim.[87] EBO is coordinated sets of actions directed at shaping the behavior of friends, foes, and neutrals in peace, crisis, and war.[88] A key

---

[82] JP 3-12r, *Cyberspace Operations* (Washington DC: Government Printing Office, 2013), viii.

[83] JP 3-12r, II-9

[84] JP 3-60, ix.

[85] Paul Davis, "Effects-Based Operations: A Grand Challenge for the Analytical Community" (Santa Monica, CA: RAND Corporation, 2001), 1.

[86] Edward Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War* (Washington DC: DOD Command and Control Research Program, 2002), 504.

[87] Clausewitz, 177.

[88] Smith, ix.

tenant of EBO is the inclusion of a full range of direct, indirect, and cascading effects achieved by the application of military, diplomatic, psychological, and economic instruments.[89] The inclusion of a full range of effects aligns with current doctrine, specifically targeting, by focusing on the effects and not on availability of particular capabilities. Most importantly, EBO focuses on ends rather than means and looks for outcomes that might be obtained by kinetic military actions in concert with other elements of national power.[90]

EBO became taboo in military lexicon when the Commander of Joint Forces Command (JFCOM) published his memorandum stating that JFCOM will no longer use, sponsor, or export the terms and concepts related to EBO.[91] In addition, prior to General James N. Mattis' memorandum in 2008, a year earlier the US Army concluded that EBO had no place in Army doctrine.[92] A case can be made that EBO focused too much on kinetic capabilities to reach desired effects and discounted non-kinetic capabilities. While General Mattis directed EBO be removed from the lexicon, he did offer that certain aspects of effects-based thinking are useful. He admitted that certain concepts within EBO remain relevant to military operations, such as holistic views to understand the operating environment, importance of the commander's intent to create unity of action, nodal analysis as it relates to targeting, and periodic assessments to determine progress towards achieving objectives.[93] While this paper does not argue the importance of continuing to use the term EBO, it does argue the usefulness of the tenants of EBO in incorporating cyberspace capabilities in targeting and planning military operations to achieve

---

[89] Davis, 7.

[90] Smith, 502.

[91] James Mattis, "USJFCOM Commander's Guidance for Effects-Based Operations," *Parameters: US Army War College Quarterly* XXXVIII, no. 3 (Autumn 2008), 23.

[92] US Army Doctrine Update #1, Combined Arms Doctrine Directorate, US Army Combined Arms Center (Fort Leavenworth, Kansas, 24 February 2007).

[93] Mattis, 23.

effects. Similar to theorists, EBO should be viewed as a former theory of warfare that should not be completely discounted as it has valid tenants and continues to influence doctrine.

In direct response to General Mattis' memorandum, Tomislav Ruby offered, "Desired effects are nothing more than desired results from the actions we take in support of objectives and guidance."[94] He concluded that never before has EBO been so necessary. Ruby argued that the tenets of EBO should remain in doctrine and be practiced in warfare. While EBO has been struck from the lexicon, effects-based remains as the second principle of targeting in current joint doctrine. In addition, there are traces of EBO in both joint and Army doctrine, whereas a primary element of operational art is the end state. In general terms, EBO was looking for an effect, objective, or an end state and its tenets may need modified, but it should be studied in the context of warfare.

The term cyberpower has also appeared with the idea of cyberspace capabilities supporting military operations. This idea of cyberpower is characterized by producing preferred outcomes within cyberspace or using cyber instruments to produce preferred outcomes in other domains. [95] The use of cyberspace actions to realize effects in other domains is in concert with EBO. The tenants of EBO, including understanding the desired objective, targeting systems that will achieve the effect, and matching a capability to the target system and objective, remain valid. Regardless whether the term EBO will continue to be banished from military language, the tenants should be studied and applied; especially in the conduct of cyberspace operations.

The need for capabilities in and through cyberspace is not only required to conduct, but also support military operations to attack and paralyze an adversary's military capacity or the

---

[94] Tomislav Ruby, "Effects-Based Operations: More Important Than Ever," *Parameters: US Army War College Quarterly* XXXVIII, no. 3 (Autumn 2008), 26.

[95] Nye, 123.

adversary's ability to control its own forces.[96] Some argue that targeting and decimating an adversary's infrastructure is about as close to war as one can get using capabilities in and through cyberspace.[97] While some view actions in cyberspace as acts of war, others argue that cyber-attacks are merely sophisticated versions of sabotage, espionage, and subversion.[98] Three separate case studies will be analyzed in this paper that have all been deemed the first cyberwar. Regardless of what is determined to be an act of war through cyberspace, the fact remains that today nation-states and their militaries must become practitioners integrating and operating in the cyberspace domain.

Case Studies

> The development of cyber weapons are simply the next evolutionary step in warfare. I'm sure there were huge reactions to the development of mass fire power in the 1800's as a new kind of warfighting implement.
>
> — ADM Michael Rogers, 2015

Military Operations in Cyberspace

While there are various definitions of cyberwar and cyberspace warfare there are also different points of view regarding the first cyberwar, and the concepts of conflict versus war in and through cyberspace. Many authors point to the first conflict in cyberspace being as early as 1986 when German nationals gained access to thousands of US computer files and sold stolen

[96] Xu Rongsheng, Chief Scientist at the Cyber Security Lab of the Institute for High Energy Physics of the Chinese Academy of Sciences, told a Chinese news reporter that "cyber warfare may be carried out in two ways: in wartime, to disrupt and damage the networks of infrastructure facilities, such as power systems, telecommunication systems, and education systems in a country; or in military engagements, the cyber technology of the military forces can be turned into combat capabilities." Larry Wortzel, "China's Approach to Cyber operations: Implications for the US." Testimony before the committee on Foreign Affairs, House of Representatives, March 10, 2010, accessed November 24, 2015, http://www.internationalrelations.house.gov/111/wor031010.pdf, 4-5.

[97] Campen, 3.

[98] Rid, 5.

information to the Komitet Gosudarstvennoy Bezopasnosti (KGB).[99] However, a number of critics look for violent military actions to constitute war and therefore claim that the Russian military operations against Georgia in 2008, which was preceded by a significant cyberspace attack, was the first cyberwar. Other authors, believe the US operations in Iraq in 2008, which had various cyberspace operations supporting military forces, was the first cyberwar. Although this paper argues against using the term cyberwar, it will focus on Russian operation against Georgia and US operations in Iraq as case studies to illustrate the use of cyberspace to support, enable, or carry out military operations in order to achieve desired objectives. The following paragraphs will attempt to illustrate how cyberspace was effectively used in these operations. A third case study, Stuxnet, is examined to further show the use of cyberspace operations in supporting desired objectives to the extent that the need for other military action was unnecessary. While some writers argue that the first battles in the 21st century may well be in cyberspace, they also readily admit that the first battle in cyberspace may have already occurred.[100]

Russian Attack on Georgia

In August 2008, the Russian Army invaded Georgia during the South Ossetia War. Preceding this invasion was the first large scale computer network attack conducted in tandem with a military campaign in history.[101] Many claimed the era of cyberspace warfare had begun.[102] Those investigating the initial event said that the country of Georgia was obviously under DDoS

[99] Healey, 10.

[100] Miller, 1.

[101] Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* 91, no. 6 (November-December 2011), 63.

[102] David Smith, "The Fourth Front: Russia's Cyber-Attack on Georgia," *Tbilisi* 24 (March 24, 2009), 1.

attack and that it was political in nature.[103] The combination of cyberspace attacks in conjunction with traditional military operations and the political nature of these attacks attributed to the account of Russian actions in cyberspace to be viewed as the first cyberwar. Many authors have used this attack as an example of a DDoS attack.[104] In order for this attack through cyberspace to have been successful, targets must have been identified in advance and actions in cyberspace coordinated with other military operations.

Russia successfully targeted the infrastructure of Georgia, specifically their connectivity to the outside world. Instead of accepting the vastness of Georgia's connectivity as too large, they found that Georgia's internet infrastructure had very few land routes, a vulnerability, and therefore the infrastructure could be targeted. [105] In addition, many of the service providers to Georgia were dependent on network infrastructure in Russia. The DDoS attacks began weeks before the Russian invasion and continued after Russia announced hostilities had ceased, which had many saying the attacks were too well coordinated to not have been planned in concert with the invasion.[106] In addition, the element of surprise was crucial to achieve Russia's desired effect. Two factors that produce surprise are secrecy and speed.[107] Surprise was evident in these actions in cyberspace in that it was quite some time before anyone recognized the attack.[108] These cyberspace incidents went hand in hand with a significant conventional military operation by

---

[103] Lucian Constantin, "Georgian Cyber Attacks Online Saga Continues," *Softpedia* (September 13, 2008), 1.

[104] Nye, 126.

[105] Eneken Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," *Cooperative Cyber Defence Centre of Excellence* (November 2008), 4.

[106] Smith, 1.

[107] Clausewitz, 198.

[108] Smith, 1.

Russian forces and were primarily focused on eliminating the people of Georgia's ability to access the outside world in order to tell its side of the story.[109]

Since the attacks, researchers have identified different phases of the cyberspace operations. Phase one was defined as a DDoS attack against specific Georgian government and media sites. Phase two witnessed an expanded target list to include Georgian financial, education, and business sites.[110] The desired effect throughout the phases was to isolate and silence the Georgian government and people. Through the successful execution of cyberspace operations, using surprise, Georgia suffered a psychological defeat before ever seeing Russian forces invade. An element of this success, surprise, as Clausewitz posited creates an intense physiological effect in gaining superiority.[111] In the aftermath of the Russian offensive on Georgia, many were convinced it was increasingly probable that the first battles in any future conflict involving technologically advanced adversaries would be electronic and waged via cyberspace.[112]

This example provides links back to various theories of warfare and contemporary frameworks for the US military. Antoine Bousquet, a lecturer on International Relations at the University of London, wrote about the distributed nature of computer network attacks as swarming tactics. He thought that a swarming network attack as a rule should have little or no mass.[113] There is direct correlation between a DDoS and swarming as described by Bousquet. However, while the individual computer systems or cyberspace munitions of a DDoS have no mass, the collective swarming of hundreds or thousands of systems creates virtual mass against

---

[109] Miller, 3.

[110] Constantin, 1.

[111] Clausewitz, 198.

[112] Miller, 2.

[113] Antoine Bouquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York, NY: Columbia University Press, 2009), 213.

an adversary. Therefore, a DDoS attack on targeted systems can be compared to Jomini's concept of massing of forces. Although Jomini may be disinterested in the nonlinear and indirect approaches offered through cyberspace, he would likely be intensely interested in DDoS providing a method to mass virtual force.

This case study provides direct links to the integration of arms. The attack on Georgia's networks and systems were coordinated with military operations in other domains. Cyberspace capabilities were combined with other arms in order to reach desired effects, illustrating elements of EBO in practice. In addition, surprise was a key factor in the attack on Georgia providing Russia a significant psychological advantage, which ties back to Clausewitz's writings over a century ago as well as the principles of war described in current US doctrine.

US Surge in Iraq

US military operations in Iraq during 2007 have also been identified as the first cyberwar. Some believe the 2007 "surge" marked the first time US military and intelligence agencies tested the capabilities of cyberspace warfare in the battlespace.[114] The Director, National Security Agency (DIRNSA) worked alongside the US military to develop methods to attack targets in a way never attempted.[115] DIRNSA was interested in developing capabilities in cyberspace, delivered by NSA, that were synchronized to support military operations. Specifically, DIRNSA was interested in providing the military with a new weapon, particular capabilities the NSA had developed.[116] NSA was in an exceptionally advantageous position to support the US military because, as an intelligence agency, it had "electronic ears on its targets".[117]

---

[114] Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York, NY: Eamon Dolan/Houghton Mifflin Harcourt, 2014), 25.

[115] Harris, 7.

[116] Ibid.

[117] Ibid, 26.

The key to support military operations would be to match targets being tracked by NSA and ones which NSA had access to those being targeted by the military for strikes with other arms. Military leaders were well-versed in the idea of integrating arms in various domains in order to achieve better results. In this case, military leaders saw cyberspace capabilities as another instrument of warfare that should be combined with other arms. Instead of falling into the trap of access based targeting, military planners worked to incorporate the NSA into the planning and the targeting cycle so they understood the target systems and desired effects against the targets identified. Ironically, as the NSA and military worked through identifying target and desired effects against them, many of the access points required for cyberspace operations were within switching stations of the US's major telecommunication network carriers.[118] This realization is evidence that the line between civilian and military networks is either blurred or perhaps non-existent.

During execution, the partnership between NSA and the US military was so successful their actions in cyberspace were credited with aiding US troops on the capture or killing of at least ten senior leaders of Al Qaeda.[119] The successful capture or killing of these senior leaders was said to have the effect of "cutting the head off a snake".[120] As the partnership grew and more objectives were realized, the NSA and military team began targeting not just the top man in an Al Qaeda cell, but also the designated number two, and then the third and fourth man in succession.[121]

Like the Russia-Georgia example, this case study ties back to numerous theories and frameworks. This case provides an exemplar of the integration of arms. Although the capabilities

[118] Harris, 18.

[119] Ibid, 22.

[120] Ibid, 23.

[121] Ibid, 15.

were present with an intelligence arm of the military, there was quick acceptance that the accesses maintained by NSA could be used to conduct offensive operations in cyberspace to support military operations in other domains. Cyberspace became another arm of the military.

Elements of EBO were present in this case as well. As targets were identified, it was up to the military to prioritize the targets and define the desired effects against the targets so the NSA could develop the appropriate cyberspace munition. In addition, there is evidence that principles of maneuver warfare, gaining a relative advantage over an enemy, and surprise were present in these operations.

Attack on Iran Nuclear Facility

Another example of using capabilities in cyberspace to conduct or support military operations is what became known to the world as Stuxnet. Stuxnet is an alias created from the systems file in a Microsoft Windows operating system, mrxnet.sys, which was exploited by the attack.[122] Ironically, this case study can also be traced back to the same time period as the previous two examples. Israel's concern with the Iranian nuclear program reached a crescendo in 2008.[123] In 2008, Israel requested bombs from the US that would destroy underground nuclear facilities as well as aircraft refueling equipment to extend the reach of their aircraft. Israel also requested permission to traverse Iraqi airspace.[124] It had not one, but at least half a dozen Iranian sites designated as targets.[125] Although many in the US presidential administration at that time supported the idea of air strikes, the US denied Israel both requests. [126]

---

[122] Zetter, 14.

[123] Healey, 216.

[124] Ibid.

[125] Zetter, 193.

[126] Ibid, 191.

Even though these requests were denied, history has shown that the United States did support Israel in delivering the desired effect on one of the identified targets. The target was the Natanz nuclear facility and the specific targets in the system were two models of Siemens Programmable Logic Controllers (PLC), S7-315 and S7-417.[127]. This attack was directed against highly specific targets.[128] For the United States plausible deniability was crucial in that the United States did not want start a war.[129] Instead of supporting air strikes, the United States considered methods to silently damage the targets without being detected.[130] Putting covert forces on the ground in Iran was ruled out just as the air strikes were previously.[131] Instead the United States in cooperation with Israel, chose a digital bunker buster as the preferred weapon, which provided the same effect as a kinetic strike.[132]

Stuxnet contained four zero-day vulnerabilities of the PLC's operating system.[133] These vulnerabilities were delivered via separate packages of malicious code with specific targets for each package.[134] The zero-days were shrewd, exploiting vulnerabilities with intentions to propagate across networks and devices.[135] Designed to propagate, it was hoped that Stuxnet would not require access to the target elements locally; instead it was let loose in the "wild" or in

---

[127] Zetter, 166.

[128] Rid, 17.

[129] Zetter, 196.

[130] Ibid.

[131] Ibid, 194.

[132] Ibid.

[133] Shakarian, 2014, 233.

[134] TED, "Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon," March 29, 2011, accessed December 15, 2015, https://youtube/CS01Hmjv1pQ.

[135] Zetter, 6.

other words, into the commercial Internet.[136] Once released the cyberspace weapon put millions of systems running the Microsoft Windows operating system at risk, but Stuxnet was so sophisticated that it did not harm any other system than the ones it targeted.[137] While millions of systems were at risk, the number actually infected by the malicious code was estimated at over 100,000 by the end of 2010.[138]

Once discovered those who analyzed the code found that it did not work in a laboratory setting or closed network system, because the lab was not the target.[139] The malicious code was so complex that it was deemed the most sophisticated ever and the first digital weapon.[140] This keen focus on a specific target and the effect on that target can be directly correlated to the first two principles of targeting in JP 3-60, focused and effects-based. Due to its precision, some have dubbed Stuxnet a surgical strike on specific machines.[141]

Those that have investigated Stuxnet believe that due to the preciseness of the malicious code the attackers must have had full inside knowledge of the nuclear facility and its systems. In June 2009, after propagating across the commercial Internet, Stuxnet was introduced into the Natanz nuclear facility's industrial control room and unknown to anyone at Natanz, it transmitted onto the critical target systems.[142] It was not until January 2010, that the International Atomic Energy Agency (IAEA) noticed anything abnormal at the Natanz facility at which point the

---

[136] TED, "Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon," March 29, 2011, accessed December 15, 2015, https://youtube/CS01Hmjv1pQ.

[137] Zetter, 6.

[138] Rid, 18.

[139] TED, "Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon," March 29, 2011, accessed December 15, 2015, https://youtube/CS01Hmjv1pQ.

[140] Zetter, 3.

[141] Ibid, 194.

[142] Ibid, 3.

effects on the target had been successful.[143] The malicious code was designed to go unnoticed while it slowly cracked centrifuge rotors. Once it was discovered, the damage had been done. The desired effect was met without ever including additional arms of any military force. Stuxnet could be used as an example of cyberspace being the dominant domain in modern warfare. Instead, Stuxnet should be viewed as an example of warfare capabilities being employed as part of a broader military operation that never materialized because of its effectiveness.

Stuxnet is a unique example of cyberspace warfare and ties back to aforementioned theories and frameworks. Because there is still no admittance from the United States or Israeli authorities that they were behind the attack, one could argue it was not a politically motivated action with militarized capabilities through cyberspace. Instead, Stuxnet can be viewed through the lens of the other previous cases. There is no doubt that the Natanz facility was targeted and more specifically the PLC's that would destroy centrifuges. In addition, there is evidence that the Natanz facility was targeted by military means with capabilities in other domains such as air and land, but the risk associated with other domains was too high. Therefore, capabilities in cyberspace were developed to meet the same desired effects with less risk and complete surprise. It is almost as if one could point to the injection of cyberspace capabilities in phase three of the joint targeting cycle with the target being the Natanz facility. In other words, there were not capabilities being considered prior to the end state being considered and targets being developed first. Clearly, elements of EBO can be found in the case of Stuxnet. Most would also agree that because Stuxnet was a surprise, it worked. Stuxnet changed the way cyberspace was viewed as part of a broad military strategy.[144]

[143] Zetter, 1.

[144] Rid, 15.

Analysis of Case Studies

These case studies are interesting in that they all occurred in roughly the same time period, and each are credited by various authors and critics as the first cyberwar. While it may appear that the labeling of these events as cyberwar contradicts the ideas presented in this work, by conducting an analysis of these events it supports the claim that cyberwar does not exist. Instead, what these case studies show is the independent approach to domains taken in military operations. The wars or conflicts discussed illustrate how an identified political strategic objective can be achieved by integrating capabilities across various domains to deliver desired results. These cases reinforce the argument for expunging the terms cyber-target and cyber-effect because the targets identified or the desired effects in each case were not specific to cyberspace.

The case studies augment a discussion on operational art. In each case, tactical actions were arranged in particular ways to get to desired results contributing to the achievement of some strategic objective. The Russian and Iraq case studies revealed tactical actions in cyberspace preceding actions in other domains. Stuxnet also showed the consideration of actions in multiple domains before deciding to execute actions in cyberspace. Additional analysis may determine the extent of operational art in each case, but the tactical actions made available through cyberspace and the employment of these actions in coordination with other domains is evident.

These cases also presented concepts that may be unique to cyberspace, and require further analysis to fully appreciate. The first is the idea of attribution. In the other military domains, attribution for military action has been fairly straightforward. In cyberspace, attribution for an action is not always evident or desired. Russia had a strategic goal in mind when coordinating cyberspace actions with other military arms, but they valued the fact that attribution of the actions in cyberspace would take time or may not be confirmed. Likewise, in the Stuxnet case, the United States pursued actions in cyberspace above other military options due to the inability to attribute the attacks to the United States. While many authors have published their thoughts on Stuxnet, there is still no confirmation from the United States that it was responsible

for the attack. The lack of attribution complements some of the inherent principles of war such as surprise, economy of force, and security.

Another concept unique to cyberspace is the repurposing of munitions. This idea is not as concrete, but important for military leaders to comprehend. Stuxnet, as an example, was an extremely sophisticated piece of malicious code. As the case study illustrated, Stuxnet put millions of systems at risk. Although the sophistication was such that only the targets were affected, there were inherent risks of releasing Stuxnet. There was a chance that the malicious code would not work as intended and it would infect systems that were not targeted. In addition, there was the risk that an adversary may obtain the malicious code, study it, and repurpose or adjust the code to fire back, compromising friendly systems. The idea of repurposing munitions is a unique concept in warfare. There are no munitions in other domains that once fired have a risk of an adversary returning fire with the same munition. In cyberspace this concern is legitimate because munitions are focused on vulnerabilities. Once a munition is fired in cyberspace against a vulnerability, the one firing must ensure they do not have the same vulnerabilities. The concepts of attribution and repurposing of munitions require more in depth analysis to fully realize the implications they present in cyberspace warfare.

Conclusion

The phenomenon of war is not new. Although new technologies continue to enhance the capabilities available to conduct warfare, the nature of war endures. War will remain a violent clash of wills between belligerents using all available capabilities. The idea that one domain will dominate war has been disproved a number of times as each domain of warfare has matured. For this reason, the term cyberwar needs to be expunged from contemporary military lexicon. It simply is not plausible that a war between two or more belligerents could be carried out in cyberspace alone. Cyberspace warfare, on the other hand, merits further integration into military operations, but this integration will not govern the phenomenon of war.

Similarly, terms such as cyber-effect and cyber-target need removed from the current lexicon of military leaders and planners. These terms offer the idea that targets and effects in cyberspace are different than in other domains. An effect should be looked at as a desired condition or result of an action or operation. It should not be looked at as domain specific, risking the exclusion of capabilities in other domains. Likewise, cyber-target should be purged from any doctrine or practice of military operations, because it specifies the domain in which the target resides. A target should remain autonomous of domain through the process of target identification, prioritization, and evaluation. Once the process is complete, capabilities in all domains can be developed as needed to obtain the desired effect on a specific target.

In all military operations, it is imperative to consider the coordination and synchronization of all available instruments of warfare.[145] For cyberspace capabilities to be integrated into military operations, the aperture of possibilities must be open. Again, adherence to the current doctrine on targeting is necessary in order to consider end state or objective prior to moving on to target development and prioritization. Only after targets have been developed should military leaders begin to consider all instruments of military power, to include kinetic and non-kinetic capabilities. Using the tenets of EBO, but removing the primacy of kinetic effects is important and should inform the current United States targeting doctrine. Just as there are some tenets of EBO that should be considered, looking back at past theories to identify elements that remain valid is valuable to integrating all available arms of military power. While future wars may be fought with the initial strikes occurring in cyberspace, it hard to perceive a future war being carried out in only one domain.

[145] Alexander, 64.

Bibliography

Acohido, Byron and Jon Swartz. *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity*. New York, NY: Union Square Press, 2008.

Adams, James and Adams James. *The Next World War: Computers are the Weapons and the Front Line is Everywhere*. New York, NY: Simon & Schuster, 1998.

Alexander, Keith B. "Warfighting in Cyberspace." *Joint Force Quarterly*, no. 46 (3rd Quarter, 2007): 58-61.

Andress, Jason, Steve Winterfeld, Lillian Ablon, and Technical. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. Waltham, MA: Syngress, an imprint of Elsevier, 2013.

Axelrod, Robert M. and Michael D. Cohen. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York, NY: Basic Books, 2001.

Bateman, Robert L., ed. *Digital War: A View From the Front Lines*. New York, NY: Presidio Press, 1999.

Bell, Harry, Gunther E Rothenberg, Helmuth von Moltke, and Helmuth Karl Bernhard Graf von Moltke. *Moltke on the Art of War: Selected Writings*. Edited by Daniel Hughes. New York, NY: Random House Publishing Group, 1996.

Bilge, Leyla and Tudor Dumitras. "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World." *Conferences on Computer and Communications Security*, 2012: 833.

Blum, Andrew S. *Tubes: A Journey to the Center of the Internet*. New York, NY: Harper Collins, 2012.

Bouquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York, NY: Columbia University Press, 2009.

Campen, Alan D. and Douglas H. Dearth. *Cyberwar 2.0: Myths, Mysteries & Reality*. Fairfax, VA: AFCEA Intl Pr, 1998.

Carter, Rosemary, Brent Feick, and Roy Undersander. "Offensive Cyber for the Joint Force Commander." *Joint Forces Quarterly*, no. 66 (3rd Quarter 2012), 24-32.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About It* (New York, NY: Harper Collins, 2010).

Clausewitz, Carl von. *On War*. Translated and edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Clemmons, Byard Q. and Gary D. Brown, "Cyberware: Way, Warriors, and Weapons of Mass Destruction" *Military Review* 79, no. 5 (September/October, 1999), 30-38.

Constantin, Lucian. “Georgian Cyber Attacks Online Saga Continues.” *Softpedia* (September 13, 2008).

Corbett, Julian S. *Principles of Maritime Strategy*. New York, NY: Dover Publications, Inc, 2004.

Davis, Paul. “Effects-Based Operations: A Grand Challenge for the Analytical Community.” Santa Monica, CA: RAND Corporation, 2001.

Dupuy, R. Ernest and Trevor N. Dupuy. *The Harper Encyclopedia of Military History: From 3500 BC to the Present*. 4th ed. New York, NY: Harper Collins Publishers, 1993.

Galvin, John R. *Maneuver Warfare: An Anthology*. Edited by Richard D. Hooker. New York, NY: Presidio Press, 1994.

Gat, Azar. *A History of Military Thought: From the Enlightenment to the Cold War*. New York, NY: Oxford University Press, 2001.

Harris, Shane. *@War: The Rise of the Military-Internet Complex*. New York, NY: Eamon Dolan/Houghton Mifflin Harcourt, 2014.

Healey, Jason and Karl Grindal, eds. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, VA: Cyber Conflict Studies Association, 2013.

Hughes, Daniel J. and Harry Bell, eds. *Moltke on the Art of War: Selected Writings*. New York, NY: Ballantine Books, 1993.

Joint Pubication 3-0, *Joint Operations.* Washington, DC: Government Printing Office, 2008.

Joint Publication 3-12r, *Cyberspace Operations.* Washington, DC: Government Printing Office, 2013.

Joint Publication 3-60, *Joint Targeting.* Washington, DC: Government Printing Office, 2013.

Kaiser, Robert. “The Birth of Cyberwar.” *Political Geography* 46 (May 2015): 11–20.

Kallberg, Jan and Bhavani Thuraisingham. “Cyber Operations: Bridging from Concept to Cyber Superiority.” *Joint Forces Quarterly,* no. 68 (1st Quarter 2013), 53-58.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009.

Mattis, James. “USJFCOM Commander’s Guidance for Effects-Based Operations.” *Parameters: US Army War College Quarterly* XXXVIII, no. 3 (Autumn 2008): 18-25.

Miller, Robert and Daneil Kuehl. “Cyberspace and the ‘First Battle’ in 21st-Century War.” *Defense Horizons* 68 (September 2009): 1-6.

Nye, Jr. Joseph S. *The Future of Power*. New York, NY: PublicAffairs, US, 2011.

Olagbemiro, Albert O. “Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyber Warfare.” School of Advanced Studies Monograph, US Army Command and General Staff College, 2014.

Olsen, John Andreas and Martin van Creveld, eds. *The Evolution of Operational Art: From Napoleon to the Present*. Oxford: Oxford University Press, 2011.

Parmenter, Robert. “The Evolution of Preemptive Strikes in Israeli Operational Planning and Future Implications for the Cyber Domain.” School of Advanced Studies Monograph, US Army Command and General Staff College, 2013.

Pettey, Christy. “The Internet of Things and the Enterprise.” *Smarter with Gartner* (August 31, 2015). Accessed November 22, 2015. gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise.

Rattray, Gregory. *Strategic Warfare in Cyberspace*. Cambridge, MA: Massachusetts Institute of Technology Press, 2001.

Rid, Thomas. “Cyber War Will Not Take Place.” *The Journal of Stategic Studies* 35, no. 1 (February 2012): 5–32.

Ruby, Tomislav. “Effects-Based Operations: More Important Than Ever.” *Parameters: US Army War College Quarterly* XXXVIII, no. 3 (Autumn 2008): 26-33.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. “How Cyber Attacks Augmented Russian Military Operations.” *Introduction to Cyber-Warfare* (2013): 23–32.

Shakarian Paulo Ruef Andrew Shakarian Jana. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham, MA: Morgan Kaufmann Publishers, an imprint of Elsevier, 2014.

Shakarian, Paulo. “The 2008 Russian Cyber Campaign Against Georgia.” *Military Review* 91, no. 6 (November-December 2011): 63.

Simpson, Emile. *War From the Ground Up: Twenty-First Century Combat as Politics*. London: C Hurst & Co Publishers, 2012.

Smith, David. “The Fourth Front: Russia’s Cyber-Attack on Georgia.” *Tbilisi* 24 (March 24, 2009).

Smith, Edward. *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. Washington DC: DOD Command and Control Research Program, 2002.

TED. “Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon.” Posted March 29, 2011. Accessed December 15, 2015. https://youtube/CS01Hmjv1pQ.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. “Cyber Attacks Against Georgia: Legal Lessons Identified.” *Cooperative Cyber Defence Centre of Excellence*. (November 2008).

Understanding Denial-of-Service Attacks. United States Computer Emergency Readiness Team. Accessed December 15, 2015. https://www.us-cert.gov/ncas/tips/ST04-015.

Van Creveld, Martin. *The Evolution of Operational Art: From Napoleon to the Present*. Edited by John Andreas Olsen and Martin van Creveld. Oxford: Oxford University Press, 2010.

Van Creveld, Martin, Kenneth S Brower, and Steven L Canby. *Air Power and Maneuver Warfare*. Montgomery, AL: Air University Press, 1994.

Van Evera, Stephen. *Guide to Methods for Students of Political Science*. 1st ed. Ithaca, NY: Cornell University Press, 1997.

Wildenberg, Thomas. *Billy Mitchell's War with the Navy: The Interwar Rivalry Over Air Power*. Annapolis, MD: Naval Institute Press, 2013.

Willoughby, Charles Andrew. *Maneuver in War*. Harrisburg, PA: The Telegraph Press, 1939.

Winterfeld, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham, MA: Syngress, 2013.

Wortzel, Larry. "China's Approach to Cyber operations: Implications for the US." Testimony before the committee on Foreign Affairs, House of Representatives, March 10, 2010. accessed November 24, 2015, http://www.internationalrelations.house.gov/111/wor031010.pdf.

Wylie, J C. *Military Strategy: A General Theory of Power Control*. New Brunswick, NJ: Rutgers University Press. 1967.

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