National Defence / Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

WARDEN'S CONCENTRIC RING THEORY APPLIED TO APPLEGATE'S OFFENSIVE CYBER MANEUVER STRATEGY

By Major D.G. Wood
Par le major D.G. Wood

JCSP 40

Master of Defence Studies

PCEMI 40

Maîtrise en études de la défense

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 40 – PCEMI 40

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

WARDEN'S CONCENTRIC RING THEORY APPLIED TO APPLEGATE'S OFFENSIVE CYBER MANEUVER STRATEGY

By Major D.G. Wood
Par le major D.G. Wood

Word Count: 18,392

Compte de mots: 18,392

ABSTRACT

Cyber has become an essential element for governments, militaries and societies. This importance makes it a target when planning a military campaign. The targeting model developed by Colonel John Warden has been shown to be a successful model in several recent conflicts, and has demonstrated flexibility in that it can be applied to any entity that can be analyzed as a system. Scott Applegate has accurately described three different strategies that can be employed when waging offensive cyber warfare. The targeting model developed by Colonel John Warden can be applied to each of these cyber maneuver strategies to analyse and attack an opponent's cyber capabilities. There is anecdotal evidence that these different cyber strategies have been employed in recent world conflicts. Real world examples accessed from open source literature have been analysed using Warden's theory, to demonstrate that countries have already started basing their attacks against their opponent's cyber capabilities using this model.

TABLE OF CONTENTS

CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

With the evolution of airpower, the achievement of air superiority became a necessary requirement in warfare. Once achieved, airpower would then support the troops on the ground and warships on and under the sea in order to achieve land and sea superiority. Colonel John Warden took the notion of airpower one step further with the introduction of his concentric ring theory. It was first demonstrated during the Gulf War in 1992. His theory categorized an enemy as a system of concentric rings; with the fielded fighting forces on the outside ring and leadership at the center ring.[1] By attacking as far into the ring system as was possible, Warden demonstrated that one did not have to fight all of the fielded fighting forces found on the outside ring. Once could attack further in to the ring system, and end the conflict far sooner than normally anticipated.[2] Warden described the Gulf War as being the "…first true 'inside to outside' war, beginning with the most important central ring in Baghdad and working its way to the outermost ring of fielded forces".[3] The success of Gulf War I was stark evidence of this theory in action, with the ground component of the war being measured in metrics of either hours or days.[4] Warden's concentric ring theory was an effective targeting model when applied to Iraq as a system.

---

[1] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 108.

[2] Colonel John A. Warden III, "Employing Air Power in the Twenty-first Century," in *The Future of Air Power in the Aftermath of the Gulf War*, ed. Richard H. Shultz and Robert L. Pfaltzgraff, Jr., (Air University Press, 1992), 69.

[3] Ibid., 78.

[4] Center of Military History, *United States Army, War in the Persian Gulf – Operations Desert Shield and Desert Storm August 1990 – March 1991*, (Washington, D.C., CMH Pub 70-117-1, 2010), 34

What airpower was to military planners in the 20th Century, cyber power is now taking this role on in the 21st Century. There is anecdotal evidence that in recent conflicts involving Israel, Russia and the United States, that achieving cyber dominance or cyber superiority at the outset of a conflict is a necessary component of their warfighting strategy. Cyber is emerging as an important area of warfare. Notably, prior to commencing a conflict with Georgia, Russia launched cyber attacks in conjunction with their military operation.[5] Bonner noted that the "…2008 Russia-Georgia war marks the only public incidence of cyber power integrated with traditional kinetic military operations."[6] There is debate in the literature as to whether cyber is a domain unto itself or not. McGuffin and Mitchell compared and contrasted cyber with the space, land, air and sea domains, and after noting a number of differences, concluded that cyber does not possess enough of the attributes that would warrant it being classified as a domain.[7] Applegate concluded that cyber did warrant being classified as a domain.[8] Regardless, in recent conflicts we are seeing cyber dominance or cyber superiority being pursued as part of military strategy, and that cyber superiority is being pursued first, prior to achieving air superiority, when part of a planned campaign.

How would one define cyber superiority? American Joint Doctrine Publication 3-12, Cyberspace Operations defines cyber superiority as having been achieved when there exists "…dominance in cyberspace by one force that permits the secure, reliable conduct

---

[5] NATO Review Magazine, n.d, Cyber Timeline, last accessed August 14, 2016, http://www.nato.int/docu/review/2013/cyber/timeline/ /index.htm.

[6] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 103.

[7] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014): 411.

[8] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations." 2012 *4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 2.

of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary."[9] Bryant makes use of American doctrine when defining cyber superiority, however he goes further in describing its nature. Due to the nature of cyberspace and the entities operating within it, Bryant assessed that cyber superiority would be "…local and transient."[10] For example, in 2008, Russia achieved cyber superiority against Georgia by suppressing "… Georgia's cyber defenses through diversion and direct attack".[11] Russia did not achieve cyber superiority throughout the entire internet. They did, however, achieve cyber superiority within the country against whom they were commencing a military campaign. Bryant described cyber superiority as being not "…global and comprehensive…",[12] instead being more "…relative to what the attacker in a conflict attempts to accomplish."[13] As an example, he described a scenario whereby a cyber attack was used to disrupt an enemy's logistics system, in order to divert fuel away from an area against which the attacker planned on commencing an operation.[14] With this example, the attacker possessed local cyber superiority, and exploited it in a limited manner in support of a larger purpose. Bonner notes that cyber superiority is similar to air superiority in terms of the benefits it provides to an attacking force, namely exploiting cyber for "…reconnaissance, communication (that is, information mobility), and attack—in addition to orientation (that

---

[9] Director, Joint Staff, 2013, *Joint Publication 3-12 (R) Cyberspace Operations*, Washington: Joint Chiefs of Staff, GL-4.

[10] William D. Bryant, 2013 Cyberspace superiority: a conceptual model, Maxwell AFB: Air University, 39.

[11] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 106.

[12] William D. Bryant, 2013 Cyberspace superiority: a conceptual model, Maxwell AFB: Air University, 39.

[13] *Ibid*.

[14] *Ibid*., 40.

is, information/computer processing) and command and control—without prohibitive interference by the enemy."[15] Secondly, he states that as with the "…early days of airpower, cyber power today is critical to victory…"[16] Further, he notes that in modern conflicts, cyber superiority should be sought *before* pursuing air superiority.[17]

Applegate applied maneuver theory to cyber warfare, and proposed different forms of maneuver that an attacker could incorporate into their overall strategy. For offensive cyber maneuver,[18] he described three different approaches:

a. Exploitive Maneuver – securing information for advantage at the tactical, operational or strategic level;[19]

b. Positional Maneuver – compromising or outright seizing of key nodes in the cyber environment, and then utilizing these nodes for your benefit;[20] and

c. Influencing Maneuver – Applegate describes an influencing maneuver as "…the process of using cyber operations to get inside an enemy's decision cycle or even to force that decision cycle though direct or indirect actions."[21]

Has Applegate defined different strategies that can be conducted when waging cyber warfare? Does his model make sense? Recent cyber conflicts do appear to match the different approaches presented in Applegate's model. In some cases, the attacker

---

[15] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 103.

[16] *Ibid*., 107.

[17] *Ibid*., 109.

[18] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations." *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 7.

[19] *Ibid*., 7 - 8.

[20] *Ibid*., 8.

[21] *Ibid*., 9.

wanted to deny the internet to the country under attack. This was demonstrated in 2007 with Russian aggression against Estonia,[22] and in 2008 during the Russian invasion of Georgia.[23]These strategies correspond most closely with Applegate's definition of Influencing Maneuver.[24]

The United States is not following this strategy, however, in its war against the Islamic State. In this case, the Americans are allowing their opponent access to the internet. This example most closely correlates with Applegate's definition of Exploitive Maneuver, whereby an attacker captures "…information resources in order to gain a strategic, operational or tactical competitive advantage."[25]

In the final type of example, cyber was used in a manner similar to that noted by McGuffin and Mitchell, that being as a supporting capability to a larger military operation.[26] Applegate referred to this as being Positional Maneuver, whereby "…key physical or logical nodes in the information environment…"[27] are captured or compromised. Applegate used as an example the 2007 Israeli attack on a Syrian reactor, which was preceded by an apparent electronic and cyber attack.[28]In keeping with

---

[22] Stephen Herzog, 2011 "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2): 51.

[23]Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins. Kindle Edition, 19.

[24] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations." *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

[25] *Ibid*., 7.

[26] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014): 411.

[27] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations." *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8.

[28] *Ibid*.

McGuffin and Mitchell's thinking that cyber would be supporting a larger operation,[29] Applegate notes that using "…positional maneuver prior to the initiation of actual kinetic combat operations set them up for success and illustrates the potential decisive nature of this form of cyber maneuver,"[30]

Given the importance of cyber for individuals, militaries and societies, and the paradigm shift going on between the timing for achieving air superiority versus the timing for achieving cyber superiority; the question must now be asked - how would cyber warfare be fought in a modern conflict? Analysis of recent cyber conflicts will show that certain countries appear to have already developed detailed cyber strategies, and they are employing these strategies. This paper will argue that Applegate has accurately described three different strategies that can be employed when waging offensive cyber warfare, and that the targeting model developed by Colonel John Warden can be used to analyse and attack an opponent's cyber capabilities. Real world examples accessed from open source media will be analysed, to demonstrate that countries have already started basing their attacks against their opponent's cyber capabilities using this model.

---

[29] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014): 411.

[30] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations." *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

CHAPTER 1 – WHY WARDEN?

The principles of war can be applied to any environment, any type of conflict, and any level of conflict.[31] Of these, the first principle – *selection and maintenance of the aim* – is described as the "arch" principle of war.[32] In warfare, even at the highest strategic level, one requires "…a single, attainable and clearly defined aim that remains the focus of the operation and towards which all efforts are directed."[33] Selecting the aim is crucial in military planning. Secondly, selecting how to go about achieving that aim is important as well. The search for a "…general theory of war…"[34] has interested both academics and military leaders for centuries.[35] Of note, Clausewitz spoke critically of the "…endeavour to establish maxims, rules, and even systems for the conduct of war".[36] He felt that those who chose to develop these models and systems did so "… without taking into view the endless difficulties which the conduct of war presents in that respect."[37]

COLONEL JOHN WARDEN

Colonel John Warden developed a unique targeting model that analysed an enemy as a system, and then attacked key elements of that system.[38] The Gulf War was the first time that Warden's theory was formally applied. The air campaign employing targeting

---

[31] Department of National Defence, *B-GL-300-001/FP-001 Land Operations (English)*. (Ottawa: Edited by Director of Army Doctrine, Chief of Land Staff, 2008), 3-6.

[32] *Ibid*.

[33] *Ibid*.

[34] Azar Gat, *The Origins of Military Thought From the Enlightenment to Clausewitz* (New York: Oxford University Press, 1989), 139.

[35] *Ibid*.

[36] The Clausewitz Homepage, "On War – Carl von Clausewitz," last accessed 6 August 2016, http://clausewitz.com/readings/OnWar1873/BK2ch02.html#a

[37] *Ibid*.

[38] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 108.

based on his theory was conducted over many weeks, however the resulting ground campaign against a softened Iraqi military was measured in hours.[39] Gordon and Trainor note that several factors came together to result in Warden's theory actually being used in planning for the Gulf War.[40] Soon after the Iraqis detained American citizens in Iraq and Kuwait, General Schwarzkopf began assessing retaliation plans that Central Command (CENTCOM) staff had developed.[41] Gordon and Trainor note that he was not satisfied with these plans, nor the fact that his Air Component Commander, Lieutenant-General Charles Horner "…had not taken air-war planning very far."[42] This was mainly due to his (Horner's) "…overseeing the deployment of American forces…"[43] having been assigned by General Schwarzkopf to be his "…acting CENTCOM commander, forward…"[44] in Saudi Arabia. As a result, General Schwarzkopf called General Colin Powell, and requested "…help from the air staff at the Pentagon…"[45] A request such as this at the Pentagon would normally have been directed to Lieutenant-General Jimmie (sic) V. Adams, an adherent of employing airpower to support the ground war.[46] However due to his being on leave, the request was instead sent to Colonel John Warden in the Checkmate office, who produced a plan ten days later.[47] While General Schwarzkopf disagreed with

---

[39] Center of Military History, United States Army, *War in the Persian Gulf – Operations Desert Shield and Desert Storm August 1990 – March 1991*, (Washington, D.C., CMH Pub 70-117-1, 2010), 34.

[40] Michael R. Gordon and General Bernard E. Trainor, 1995, *The generals' war: the inside story of the conflict in the Gulf*, Toronto: Little, Brown and Company, 76.

[41] *Ibid*., 75.

[42] *Ibid*., 76.

[43] *Ibid*.

[44] H. Norman Schwarzkopf, *It Doesn't Take a Hero: The Autobiography of General H. Norman Schwarzkopf* (New York: Bantam Books, 1993), 355.

[45] Michael R. Gordon and General Bernard E. Trainor, 1995, *The generals' war: the inside story of the conflict in the Gulf*, Toronto: Little, Brown and Company, 76.

[46] *Ibid*.

[47] *Ibid*.

part of Warden's overall theory - namely that war could be won by airpower alone,[48] he was sufficiently impressed with the detailed targeting plan that Warden presented, and chose to employ it to execute the air war.[49] Notably, General Schwarzkopf overrode the protests of his Air Component Commander at the time, Lieutenant-General Chuck Horner, who did not appreciate an interloper from Washington (Warden) telling him how to run his air war.[50]This indicated the level of confidence that Schwarzkopf had for Warden's plan. When Warden presented the plan to Lieutenant-General Horner, he (Horner) was hostile and argumentative.[51] Shortly after the briefing, he sent Warden back to Washington.[52] Lieutenant-General Horner later assigned Brigadier-General Buster Glosson to develop a plan with more of his (Horner's) mark on it.[53] Keaney and Cohen note, however, that Horner kept several members of Colonel Warden's planning team, and that the final targeting plan put forward by Lieutenant-General Horner retained Warden's ideas and target sets. Notably, his plan had "…the same focus on Iraqi leadership, and the same intent of isolating Saddam Hussein from the Iraqi people and his forces."[54]

Warden's plan utilized both his targeting model and the tremendous air capabilities possessed by the Americans. Simultaneously, it minimized both the strategy

---

[48] H. Norman Schwarzkopf, *It Doesn't Take a Hero: The Autobiography of General H. Norman Schwarzkopf* (New York: Bantam Books, 1993), 369.

[49] *Ibid*., 371.

[50] *Ibid*.

[51] Michael R. Gordon and General Bernard E. Trainor, 1995, *The generals' war: the inside story of the conflict in the Gulf*, Toronto: Little, Brown and Company, 92.

[52] *Ibid*., 93.

[53] Thomas A. Keaney and Eliot A. Cohen, 1993, *Gulf War Air Power Survey Summary Report*, Washington, D.C., US Government Printing Office, 37.

[54] *Ibid*., 38.

of Iraqi President Saddam Hussein and the power of his "…very capable army."[55] The main center of gravity in Colonel Warden's plan was Iraqi President Saddam Hussein.[56] Warden's plan focused on command and control and communications facilities, in order to "…isolate him from the Iraqi people and his armed forces."[57] In addition, the plan focused on national infrastructure, "…Iraq's nuclear, chemical and biological facilities and its national air defense system and airfields."[58] Saddam Hussein's strategy was to engage the United States in a ground battle, maximizing the use of his ground forces. He reasoned that a drawn-out war of attrition would weary coalition populations, who would then force the end of the war.[59] That was not the war that the Americans chose to fight, however. The American's employed Colonel John Warden's targeting model, and fought the war on their terms. The result was "…one of the most operationally successful wars in history, a conflict in which air operations played a preeminent role."[60]

Chun states that Warden's "…theories had a major impact on Operation DESERT STORM and the air campaign. Warden's ideas on precision guided munitions, stealth, parallel attack, and other air power features did create some strategic paralysis among the

---

[55] Colonel John A. Warden III, "Employing Air Power in the Twenty-first Century," in *The Future of Air Power in the Aftermath of the Gulf War*, ed. Richard H. Shultz and Robert L. Pfaltzgraff, Jr., (Air University Press, 1992), 77.

[56] Thomas A. Keaney and Eliot A. Cohen, 1993, *Gulf War Air Power Survey Summary Report*, Washington, D.C., US Government Printing Office, 36.

[57] *Ibid*.

[58] *Ibid*.

[59] Colonel John A. Warden III, "Employing Air Power in the Twenty-first Century," in *The Future of Air Power in the Aftermath of the Gulf War*, ed. Richard H. Shultz and Robert L. Pfaltzgraff, Jr., (Air University Press, 1992), 77.

[60] Thomas A. Keaney and Eliot A. Cohen, 1993, *Gulf War Air Power Survey Summary Report*, Washington, D.C., US Government Printing Office, ix.

Iraqi government."[61] Further, he states that despite the fact that "…Hussein's government did not collapse, it was affected significantly during the strategic bombardment campaign."[62]Post-Gulf War, Chun assesses that Warden's overall impact on military planning is that his "…Five Ring model gave campaign planners the ability to focus on a framework to paralyze a foe. Warden linked his ring attack to a plausible scheme against a modern nation-state."[63]In addition to air superiority, a commander would require extensive information on an enemy in order to implement Warden's theory.[64] Provided those conditions, along with resources are met, Chun assesses that "…the focus on what factors make an enemy operate as a system is a valuable way to think about an adversary."[65] He concluded that "…Warden helped integrate technology and strategic concepts that supported a major change in how nations use air power in war."[66]

WHY USE WARDEN'S MODEL?

Why choose Warden's targeting model over other theories that have been put forward before? What advantages does Warden's theory convey that make it distinct from other models and theories? Warden's targeting theory, or variations of it, has been applied in several recent conflicts. While no theory to date could be described as being perfect,

---

[61] Clayton K.S. Chun, "John Warden's Five Ring Model and the Indirect Approach to War, in *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy*, ed. J. Boone Bartholomees, 295 – 307, (Carlisle: Strategic Studies Institute, 2012), 305.

[62] *Ibid*.

[63] *Ibid*.

[64] *Ibid*., 306.

[65] *Ibid*.

[66] *Ibid*.

the targeting model proposed by Colonel John A. Warden III has been employed several times since it was first employed during the Gulf War. Then, it was employed to startling effect against the Iraqi regime and its military. Following the success during the first Gulf War, Warden continued to shape his theory,[67] and his protégé, Lieutenant-Colonel (eventually Lieutenant-General) David Deptula would incorporate Warden's theory into Air Force doctrine.[68] Lieutenant-General Deptula felt that a key component of Warden's targeting theory – parallel warfare could "…offer alternatives to the attrition and annihilation strategies of older-style warfare."[69] Warden's theory was employed with questionable success in Kosovo, where NATO conducted an air-only war against the Serbs.[70] High altitude, low risk (for the bombing aircraft) operations initially had limited effect.[71] Biddle assesses that diplomatic pressure from Russia (fearing an eventual NATO ground campaign) along with an intensified bombing campaign (targeting the electrical grid, bridges and railways) led to the Serbian defeat.[72] Lambeth states that the world "…may never know for sure what mix of pressures and inducements ultimately led Milosevic to admit defeat…"[73] He notes that the "…78-day bombing effort was [crucial] in bringing Milosevic to heel…,"[74] while recognizing that "…there is ample reason to be wary of any intimation that NATO'S use of airpower produced that ending without any

---

[67] Tami Davis Biddle, 2012, The Airplane and Warfare: Theory and History, in *U.S. Army War College Guide to National Security Issues*, *Volume I: Theory of War and Strategy,* edited by J. Boone Bartholomees, Jr., 273 – 294, Carlisle Barracks, PA: Strategic Studies Institute, 287.

[68] *Ibid*.

[69] *Ibid*.

[70] *Ibid*.

[71] *Ibid*.

[72] *Ibid*.

[73] Benjamin S. Lambeth, 2001, *NATO's Air War for Kosovo: A Strategic and Operational Assessment*, Arlington, VA: Rand Corporation, 68.

[74] *Ibid*.

significant contribution by other factors."[75] Grant, however, made note of a quote from military historian John Keegan, who said that the "…the capitulation of President Milosevic proved that a war can be won by airpower alone."[76]She noted that following the start of the intensified bombing campaign around 22 May 1999, which targeted military forces, utilities infrastructure and command and control nodes, "…the combined effect had brought the war home to Belgrade and restricted Milosevic's ability to employ his fielded forces effectively."[77]She felt this concentrated targeting and air war campaign directly led to Milosevic acceptance of NATO's conditions on 9 June 1999.[78]

In the next decade, doctrine strongly influenced by Warden's theory was published for the United States Air Force in 2003, and was used by military planners for the wars both in Afghanistan and Iraq.[79] Two statements from this 2003 doctrine stand out as reflecting Warden's influence on American military thinking post 9/11, notably that the "…aggressive use of air and space power can also reduce the size of forces needed for conflict termination, risking fewer American lives…;"[80]and, "…strategic attack builds on the idea that it is possible to directly affect an adversary's sources of strength and will to fight without first having to engage and defeat their military forces."[81] These ideas very much reflect Warden's theory. Biddle noted that United

---

[75] Benjamin S. Lambeth, 2001, *NATO's Air War for Kosovo: A Strategic and Operational Assessment*, Arlington, VA: Rand Corporation, 68.

[76] Rebecca Grant, 1999 "Airpower Made it Work," *Air Force Magazine*, http://www.airforcemag.com/MagazineArchive/Documents/1999/November%201999/1199airpower.pdf, 37.

[77] *Ibid*.

[78] *Ibid*.

[79] Tami Davis Biddle, 2012, The Airplane and Warfare: Theory and History, in *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy,* edited by J. Boone Bartholomees, Jr., 273 – 294, Carlisle Barracks, PA: Strategic Studies Institute, 288.

[80] *Ibid*., 289.

[81] *Ibid*.

States Air Force doctrine that was used in planning the wars in Afghanistan and Iraq post 9/11 "…echoed elements of Warden and Deptula…".[82] When analysing the targeted killings programme conducted by Israel against Hamas leadership, Avi Kober relied heavily on Warden's targeting theory, noting that targeted killings "…usually aims not only at a terror organization's leadership, in accordance with Warden's preference, but also at terror operatives who could be considered military targets."[83] He cites an example where even just the threat of targeted killings directly influenced Hamas leadership. Following a series of rocket attacks into Israel in 2005, the Israeli Defence Minister openly threatened two senior Hamas leaders that if the rocket attacks did not stop, that they would end up joining two former Hamas leaders who had been dispatched by Israel's targeted killings programme.[84] The attacks stopped, with Kober concluding that this result seems "… to support John Warden's view on the effectiveness of the decapitation of political leadership."[85] Perhaps most interesting, however, Kober notes that targeted killings of "…military leaders and operatives proved to be ineffective…",[86] however the "… decapitation of Hamas's political and spiritual leaders, on the other hand, seemed to be rather effective."[87] In his analysis of Operations Unified Protector and Odyssey Dawn in Libya, Distelzweig concludes that the "…planning and execution of Operations Odyssey Dawn and Unified Protector followed Colonel John A. Warden's theory of

---

[82] Tami Davis Biddle, 2012, The Airplane and Warfare: Theory and History, in *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy,* edited by J. Boone Bartholomees, Jr., 273 – 294, Carlisle Barracks, PA: Strategic Studies Institute, 288.

[83] Avi Kober, "Targeted killing during the second intifada: The quest for effectiveness." *Journal of Conflict Studies* 27, no. 1 (2007), https://journals.lib.unb.ca/index.php/JCS/article/viewArticle/8292/9353, n.p.

[84] *Ibid*., n.p.

[85] *Ibid*., n.p.

[86] *Ibid*., n.p.

[87] *Ibid*., n.p.

warfare, based on the importance of air superiority and attacking the enemy as a system, even if this was not the intended methodology."[88] Essentially, what Distelzweig is saying is that in general, if planners incorporate most of the elements of Warden's model, they are following his theory, whether they intended to do so or not.[89] Finally, although few are privy to the planning and methodology for the campaign against the Islamic State, it could be argued that coalition targeting against ISIS is also following Warden's theory, as demonstrated by the Coalition attacks on leadership,[90] oil[91] and money[92]. Warden's theory has demonstrated success repeatedly in recent modern conflicts. Colonel Warden's theory is still taught to United States Army War College students, and as of 2012 was included in their *Guide to National Security Issues Volume I*.[93] It is still very much a relevant theory, as demonstrated by its being taught to developing senior and general officer candidates to this day.[94]

WARDEN'S MODEL

Others have begun noting the flexibility and utility in Warden's model as well in that his theory can be applied to systems other than those that can be influenced by

---

[88] Kurt Distelzweig, "Operations Odyssey Dawn and Unified Protector: Another Win for Warden's Theory" (School of Advanced Military Studies Monograph, School of Advanced Military Studies. 2014), 2.

[89] *Ibid*.

[90] National Public Radio, "We're Taking Out" About 1 ISIS Leader Every 3 Days", 29 June 2016, last accessed 4 August 2016, http://www.npr.org/2016/06/29/484058317/u-s-envoy-were-taking-out-about-1-isis-leader-every-3-days

[91] The Rand Corporation, "The Islamic State's Money Problems," 5 March 2016, last accessed 4 August 2016, http://www.rand.org/blog/2016/03/the-islamic-states-money-problems.html?utm_source=t.co&utm_medium=rand_social.

[92] *Ibid*.

[93] Clayton K.S. Chun, "John Warden's Five Ring Model and the Indirect Approach to War, in *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy*, ed. J. Boone Bartholomees, 295 – 307, (Carlisle: Strategic Studies Institute, 2012), 295.

[94] *Ibid*.

airpower. In their paper applying Warden to Cyberspace, Arwood et.al. referred to the usefulness of the targeting model that he (Warden) had developed; noting that it was a systematic method to "…break complex systems down into subsystems that are more manageable and understandable."[95]Warden's theory has been extrapolated to other organizations that could be categorized as systems as well, both by Warden himself, and by other authors; sometimes for systems for which effects cannot be generated by air power. In his own examples of system attributes, Warden applied his model to the human body, an electric company, a drug cartel and a state government.[96] An example of how Warden applied his model to these systems can be found at Table 1.1.

[95] Sam Arwood, Robert Mills and Richard Raines, Operational art and Strategy in Cyberspace, *International Conference* (2010), 18.

[96] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 107.

Table 1.1 – Warden's Model Applied to Various Systems

	Body	State	Drug Cartel	Electric Company
Leader	Brain -eyes -nerves	Government -communication -security	Leader -communication -security	Central Control
Organic Essential	Food/oxygen -conversion via vital organs	Energy (electricity, oil, food), money	Coca source plus conversion	Input (heat, hydro) Output (electricity)
Infrastructure	Vessels, bones, muscles	Roads, airfields, factories	Roads, airways, sea lanes	Transmission lines
Population	Cells	People	Growers, distributors, processors	Workers
Fighting Mechanism	Leukocytes	Military, police, firemen	Street soldiers	Repairmen

Source: Colonel John A. Warden III, "Air theory for the twenty-first century", 107.

Chappel applied Warden's targeting model to a generic terrorist organization,[97] and Arwood et.al. have adapted and applied it to cyber.[98]It has been shown to be a flexible targeting model, and has been applied to various systems. Thus, although Warden himself was an airpower advocate and his targeting model has been used with airpower to great effect, his model is not airpower exclusive.

---

[97]George G. Chappel, Jr., "A Terrorist Organization as a System: Unleashing Warden's Five Ring Model" (Final Report, Joint Military Operations Department, Naval War College, Newport, R.I., 2002), 2.

[98] Sam Arwood, Robert Mills and Richard Raines, Operational art and Strategy in Cyberspace, *International Conference* (2010), 18.

What is Warden's model, and how does his theory compare to the works of other military scholars? His theory is that the primary aim in warfare is "…(c)ontrol of the enemy command structure, civil and military…".[99] Warden proposed a theory whereby an opposing force is viewed as a system of five concentric rings, with the fielded fighting forces serving as the outermost ring, and leadership serving as the innermost ring.[100] Figure 1.1 shows Warden's concentric ring theory model.

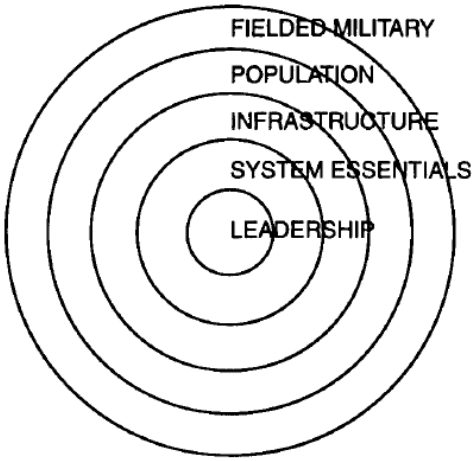

Figure 1.1 – Warden's Concentric Ring Theory

Source: Colonel John A. Warden III, "Air theory for the twenty-first century," 108.

---

[99] Colonel John A. Warden III, "Employing Air Power in the Twenty-first Century," in *The Future of Air Power in the Aftermath of the Gulf War,* ed. Richard H. Shultz and Robert L. Pfaltzgraff, Jr., (Air University Press, 1992), 63.

[100] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues,* ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 108.

Warden was highly methodological in his approach. With his model, one first studied the enemy as a system, both politically and technologically.[101] In order to build his definition of a system, Warden modelled biological (a human), industrial (an electrical utility) and natural (the solar system, with the sun at the center) constructs when developing his definition of a system.[102] In general, his model observed that most systems were comprised of the following elements:

a. "central leadership or direction;

b. organic essentials;

c. infrastructure;

d. population; and

e. a fifth component that protects the system from outside attack or general degradation."[103]

One then determined what were the political goals that your nation sought to achieve from the engagement, followed by a determination of how to go about forcing the enemy to do what you want. Warden identified three mechanisms to force an enemy to do your will – paralyzing him, completely destroying him, or making the cost of continued engagement simply too onerous for one's enemy to continue.[104] The enemy was then

---

[101] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues,* ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 117.

[102] John A. Warden, 1995, "The Enemy as a System." *Airpower Journal* 9 (1). Accessed September 11, 2016. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

[103] *Ibid*.

[104] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 117.

modelled using the five-ring system shown at figure 1.1, and centers of gravity would be identified for each ring. If one could attack the center ring (leadership) immediately, that situation would be optimal. Warden states that an attacker may not need to expend effort fighting an opponent's forces or destroying their infrastructure and resources, "…if we can capture, kill, or isolate the enemy leader."[105] Barring that, Warden argued that the centers of gravity for each ring should be attacked in parallel, in order to completely overwhelm and paralyze an opponent.[106]

Warden argued that parallel warfare results in "…so many parts of the enemy system under near-simultaneous attack that the system simply cannot react to defend or to repair itself."[107] Warden likened parallel warfare as being similar to a "…death of a thousand cuts…"[108] Despite this strategy of overwhelming parallel assault, however, Warden did not feel that one had to completely destroy an enemy's fielded fighting forces. Notably, he cited the World War Two examples of Japan and Germany, who finally surrendered with large components of their fighting forces still intact,[109] and that of Iraq, who surrendered Kuwait "…while its army occupied all of the contested area."[110] In Warden's opinion, the significance of all three examples was that each country

---

[105] Colonel John A. Warden III, 1992 "Employing Air Power in the Twenty-first Century," Edited by Richard H. Shultz and Robert L. Pfaltzgraff, Jr., in *The Future of Air Power in the Aftermath of the Gulf War* (Air University Press), 69.

[106] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 117.

[107] *Ibid*., 116.

[108] *Ibid*.

[109] Colonel John A. Warden III, "Employing Air Power in the Twenty-first Century," in *The Future of Air Power in the Aftermath of the Gulf War*, ed. Richard H. Shultz and Robert L. Pfaltzgraff, Jr., (Air University Press, 1992), 63.

[110] *Ibid*.

surrendered before their fighting forces were totally destroyed. In all three examples, national leadership was influenced to seek terms for surrender.

When one compares these conflict outcomes to all of the other wars which have been fought throughout human history (many of which were wars of annihilation), and noting that in these recent cases capitulation occurred regardless, Warden's arguments begin to make sense. Throughout history, suffering and carnage during war were terrible. For example, the during the Peloponnesian Wars which were fought in ancient Greece, Wolf states that those "…under siege were starved. Revolutionary elements were liquidated. Large groups of captured prisoners were executed in revenge for acts of savagery by the enemy."[111] Further, there was significant collateral damage, with Wolf describing how mercenaries "…employed by Athens lay(ing) waste to towns not involved in the combat, killing all inhabitants. As in any war, combat meant brutality."[112] Hanson notes that for most of history, the "…Western style of warfare puts a premium on the idea of annihilation, of head to-head combat rather than ritualistic fighting."[113] Further, he states that from the ancient wars of early Greece to "…the industrial wars of the 20th century, there is a certain continuity of Western military practice."[114] Secondly, he notes that a common theme was "…Hellenic characteristics of battle: superior discipline, matchless weapons, egalitarian camaraderie, individual initiative, tactical flexibility and a preference for shock battle."[115]

---

[111] John D. Wolf, 1983, The Military and Moral Implications of the Peloponnesian War, Newport, R.I.: Naval War College, 9-10.
[112] *Ibid*., 10.
[113] Victor Davis Hanson, 2004, "The western way of war." *Australian Army Journal* 2 (no. 1): 159.
[114] *Ibid*.
[115] *Ibid*.

The three examples cited by Warden give weight to his theory that the principle aim in war is to control the opposing force's command structure in order to have them accept concessions imposed by the aggressor,[116] not when their forces are completely destroyed. This circumstance can result in a situation where full scale war does not have to be fought. Throughout, Warden's focus is "…against the mind of the enemy command…",[117] not on the fighting forces. This thinking correlates with that of Chinese General and tactician Sun Tzu who, centuries earlier, stated that "…the best thing of all is to take the enemy's country whole and intact…".[118] Further, he states that "…it is better to recapture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them."[119] According to Sun Tzu, the aim of warfare is to achieve victory with minimal effort on your part. While this stratagem, in part, correlates with Clausewitz's idea of minimizing friction within your own forces,[120] it goes further, and advocates minimum destruction be applied against your opponent. Clausewitz divided friction into two components, incidental friction (also known as chance),[121] and general friction, comprised of "…danger, physical exertion, uncertainty…".[122] By exerting minimal effort on the attacker's part, both general and incidental friction is minimized.

---

[116] Colonel John A. Warden III, "Employing Air Power in the Twenty-first Century," in *The Future of Air Power in the Aftermath of the Gulf War*, ed. Richard H. Shultz and Robert L. Pfaltzgraff, Jr., (Air University Press, 1992), 63.

[117] *Ibid*., 67.

[118] Sun Tzu, Sun, *The Art of War, The Original Authoritative Edition*, Edited and translated by Lionel Giles (Sweden: Chiron Academic Press, Kindle Edition, 2015), page 37.

[119] *Ibid*.

[120] Antulio J. Echevarria II, *Clausewitz and Contemporary War* (Kindle Edition. Oxford University Press, 2007), 130.

[121] *Ibid*., 103.

[122] *Ibid*.

WARDEN'S DETRACTORS

Warden's theory has its detractors, however. Their opposition to some of his potentially paradigm shifting ideas often takes away from a widely applicable targeting model. General Schwarzkopf himself was not impressed with Warden's advocacy that one could win wars with airpower alone.[123] Prior to his first meeting with Warden and his planning team, Schwarzkopf stated the he was "…leery of Warden, who was from the Curtis LeMay school of Air Force planners – guys who think strategic bombing can do it all and that armies are obsolete."[124] General Schwarzkopf quickly changed his opinion of Colonel Warden, however, upon meeting him and noting both the quality of his targeting plan and the flexibility in his thinking.[125]Lieutenant-General Horner, Air Component Commander during the Gulf War took issue with Warden's targeting plan, assessing that it was "…seriously flawed in its operational aspects and disapproved of its relative neglect of the Iraqi forces in Kuwait."[126]Gordon and Trainor note that at that period of time, Horner was serving as both the Air Component Commander and the "…acting theater commander pending Schwarzkopf's arrival in Riyadh…".[127] While serving in the latter capacity, he continuously had the threat from Iraqi forces on his mind, and now a "…colonel from the Pentagon had arrived to tell him to stop worrying so much about the

---

[123] H. Norman Schwarzkopf, *It Doesn't Take a Hero: The Autobiography of General H. Norman Schwarzkopf* (New York: Bantam Books, 1993), 369.

[124] *Ibid*.

[125] *Ibid*.

[126] Thomas A. Keaney and Eliot A. Cohen, 1993, *Gulf War Air Power Survey Summary Report*, Washington, D.C., US Government Printing Office, 37.

[127] Michael R. Gordon and General Bernard E. Trainor, 1995, *The generals' war: the inside story of the conflict in the Gulf*, Toronto: Little, Brown and Company, 91.

Iraqi forces in Kuwait and to start planning strikes against downtown Baghdad."[128]Horner initially felt that Warden's plan was "…shockingly theoretical and naïve, and competed with the more traditional plan he had sketched to attack the invading Iraqi forces."[129]What is interesting, however, is that after replacing Colonel Warden with Brigadier-General Buster Glosson, Lieutenant-General Horner chose to retain several members of Warden's planning team to assist Glosson.[130] The resulting plan they developed "…retained the same target sets, the same focus on Iraqi leadership, and the same intent of isolating Saddam Hussein from the Iraqi people and his forces."[131]The plan implemented under Lieutenant-General Horner was quite similar to the one that Colonel Warden had presented to him originally.

Warden himself contrasted his theory from the writings of Clausewitz, stating that his plan differed from the latter's in that the "…destruction of the enemy military is not the essence of war; the essence of war is convincing the enemy to accept your position, and fighting his military forces is at best a means to an end and at worst a total waste of time and energy."[132]

---

[128] Michael R. Gordon and General Bernard E. Trainor, 1995, *The generals' war: the inside story of the conflict in the Gulf*, Toronto: Little, Brown and Company, 91-92.

[129] *Ibid*., 92.

[130] Thomas A. Keaney and Eliot A. Cohen, 1993, *Gulf War Air Power Survey Summary Report*, Washington, D.C., US Government Printing Office, 37-38.

[131] *Ibid*., 38.

[132] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 109.

WARDEN AND THE GREAT THINKERS

We have heard Warden's own contrast of his work against the writings of Clausewitz. What were Clausewitz's main teachings on the aim of warfare? Prussian Major-General Carl Philipp Gottfried von Clausewitz wrote that the "…destruction of the enemy's fighting power is, therefore, always the means to attain the object of the combat".[133] Later, he argues that the "…destruction of the enemy's armed force appears, therefore, always as the superior and more effectual means, to which all others must give way.[134] If one focused on those statements, it would appear that Clausewitz's theory was focused upon the destruction of the fighting forces of an opponent. More specifically, he stressed the importance of attacking the centers of gravity of an opponent (those points, which if attacked would result in the complete collapse or disruption of an adversary).[135]

Many military scholars have made an effort to summarize the diverse works of Clausewitz. Antulio Echevarria states that according to Clausewitz, the aim of warfare was to "…destroy the combat capacity of one's adversary…".[136] Echevarria further amplifies Clausewitz's use of the word "destroy" to imply the "…the complete or partial destruction of the adversary…",[137] damaging an opponent "…at a rate proportionally greater than that suffered by friendly forces"[138] (attrition). Gat similarly notes this thinking in Clausewitz's writing, by his quoting that "…direct annihilation of the enemy's

---

[133] The Clausewitz Homepage, "On War – Carl von Clausewitz," last accessed 6 August 2016, http://clausewitz.com/readings/OnWar1873/BK1ch02.html#a

[134] *Ibid*.

[135] Antulio J. Echevarria II, *Clausewitz and Contemporary War* (Kindle Edition. Oxford University Press, 2007), 185.

[136] *Ibid*., 133.

[137] *Ibid*., 134.

[138] *Ibid*.

forces must always be the *dominant consideration*."[139] Hence, one would begin to surmise that there is stark disagreement between Warden's theory (even, as noted, by Warden himself) and the writings of Clausewitz, with Clausewitz supposedly advocating that one should completely destroy an enemy's military forces.

This is not the case, however. There are parallels in thinking between Clausewitz and Warden. Clausewitz himself noted that the "…object of a combat is not the destruction of the enemy's force, that is, of the force opposed to us, but that this only appears as a means. But in all such cases it is no longer a question of complete destruction…"[140]Later, he notes that "…a whole campaign may be carried on with great activity without the actual combat playing any notable part in it."[141]This idea that one could win a war without destroying your enemy's fighting forces is very similar to what Warden was arguing. Gat picked up on these aspects of Clausewitz's writing, noting that while it was advisable to be prepared to fight, nevertheless "…the perfection of strategy was therefore to achieve such favourable conditions as to render battle unnecessary."[142]Later, Gat notes that in Book VI, "…Clausewitz realizes that the war of destruction is not the exclusive form of war, and that by ignoring that which does not conform to it, theory becomes cut off from historical reality."[143]Gat notes that writers often attribute the complete destruction dogma as being Clausewitz's sole mantra, and

---

[139] Azar Gat, *The Origins of Military Thought From the Enlightenment to Clausewitz* (New York: Oxford University Press, 1989), 207.

[140] The Clausewitz Homepage, "On War – Carl von Clausewitz," last accessed 6 August 2016, http://clausewitz.com/readings/OnWar1873/BK1ch02.html#a

[141] *Ibid*.

[142] Azar Gat, *The Origins of Military Thought From the Enlightenment to Clausewitz* (New York: Oxford University Press, 1989), 210.

[143] *Ibid*., 219.

that it is a common misinterpretation of his overall ideas.[144] Hence, the idea that Clausewitz only advocated complete destruction is erroneous. As a result, there are aspects of Clausewitz's writing which do correlate to that of Warden's theory.

Clausewitz recognized that annihilation was not the only strategy that a commander could adopt. The idea that a commander was not bound solely to a simple annihilation strategy, but instead could select from different strategies "…goes back at least to Clausewitz, but its most famous proponent was German military historian and critic Hans Delbrück."[145] Delbrück described two forms of strategy; the first, he called "strategy of attrition, or bipolar strategy"[146] The second strategy he felt stood "…in opposition to the other one…",[147] that being "…annihilation."[148] Delbrück's attrition (or exhaustion) strategy sought to "…reduce enemy capability over time".[149] With respect to maneuver, Delbrück noted that Turenne, during the Thirty Years' War (1600's)[150], was "…considered more or less as the creator of a maneuver strategy that is clever and active but avoids combat."[151]When describing maneuver strategy during the Seven Years War (1700's), Delbrück noted that the theory had evolved to the point where "…one could turn completely away from the decision by battle, and the method of pure maneuver was

---

[144] Azar Gat, *The Origins of Military Thought From the Enlightenment to Clausewitz* (New York: Oxford University Press, 1989), 229 - 230.

[145] J. Boone Bartholomees Jr., 2010, "The issue of attrition," *Parameters* 40 (1): 6.

[146] Hans Delbrück, 1975, English language edition published 1985, *History of the Art of War Within the Framework of Political History*, Translated by Walter J. Renfroe, Jr., Vol IV, Westport: Greenwood Press, 108.

[147] *Ibid*., 109.

[148] *Ibid*.

[149] J. Boone Bartholomees Jr., 2010, "The issue of attrition," *Parameters* 40 (1): 9.

[150] Hans Delbrück, 1975, English language edition published 1985, *History of the Art of War Within the Framework of Political History*, Translated by Walter J. Renfroe, Jr., Vol IV, Westport: Greenwood Press, 299.

[151] *Ibid*., 335.

developed."[152]He quoted an English General Lloyd, who wrote that a commander "…who had an understanding of these things can initiate military operations with geometric strictness and can constantly wage war without ever finding it necessary to be forced to fight."[153]This idea of fighting war differently is quite similar to Warden's theory.

This thinking also correlates with the writings of Swiss officer Antoine-Henri Jomini, who sought to describe the fundamental principle of war. His first maxim was to not engage an opponent force upon force. Instead, he wrote that a commander should direct the "…mass of an army, successively, upon the decisive points of a theater of war, and also upon the communications of the enemy as much as possible without compromising one's own."[154] By doing so, a commander only has to attack those necessary decisive points of an enemy, with the result that maximum effect is achieved against an opponent, with the minimum of effort by one's own force. In describing what he meant by decisive points, Jomini refers to any persons, places or things which "…are capable of exercising a marked influence either upon the result of the campaign or upon a single enterprise."[155] He provides examples common to soldiers of the nineteenth century, such as "…geographic points and lines whose importance is permanent and a consequence of the configuration of the country,"[156] along with what he described as

---

[152] Hans Delbrück, 1975, English language edition published 1985, *History of the Art of War Within the Framework of Political History*, Translated by Walter J. Renfroe, Jr., Vol IV, Westport: Greenwood Press, 387.

[153] *Ibid*., 388.

[154] Baron Antoine Henri De Jomini, *The Art of War,* ed. by Andrew McNab, trans by Captain G.H. Mendell and Lieutenant W.P. Craighill (Apostrophe Books Ltd, Kindle Edition, 1862, 1910 edition), Kindle locations 1118 – 1119.

[155] *Ibid*., Kindle locations 1372 - 1373.

[156] *Ibid*., Kindle location 1375 – 1376.

being "…decisive geographic points…"[157] such as junctions for communications and valleys. Notably, Jomini defines national capitals as being strategic decisive points. This is due to their dual nature as being both communications centers, but also being the location of national leadership and government.[158] Hence, Jomini does not simply advocate the destruction of an enemy's fighting forces, instead, he advocates attacking key decisive points (such as command and leadership centers), to cause an opponent's entire force to topple. This focus on leadership is significant, and will be the focus of later thinkers on this subject. While Jomini's decisive points bear similarity to Clausewitz's centers of gravity, Jomini's decisive points do not necessarily focus on the complete nor partial destruction of an enemy's fighting forces. Jomini is focused on decisive points that might topple a force, not attriting them. This thinking is similar to that proposed by Warden.

WARDEN AND BOYD

Years later, USAF Colonel John Boyd also focused on the leadership element when developing his "observe-orient-decide-act (OODA) loop sketch."[159] With this model, Boyd mapped out the decision cycle as being a continuous, cyclical process of observing, orienting, deciding and acting (see figure 1.2).[160]

---

[157] Baron Antoine Henri De Jomini, *The Art of War,* ed. by Andrew McNab, trans by Captain G.H. Mendell and Lieutenant W.P. Craighill (Apostrophe Books Ltd, Kindle Edition, 1862, 1910 edition), Kindle location 1383 – 1384.

[158] *Ibid*., Kindle location 1389 – 1390.

[159] John R. Boyd, 13 March 2006. "Boyd's OODA Loop." Slideshare.net. Accessed August 6, 2016. http://www.slideshare.net/Mewthom/boyds-ooda-loop.

[160] *Ibid*.

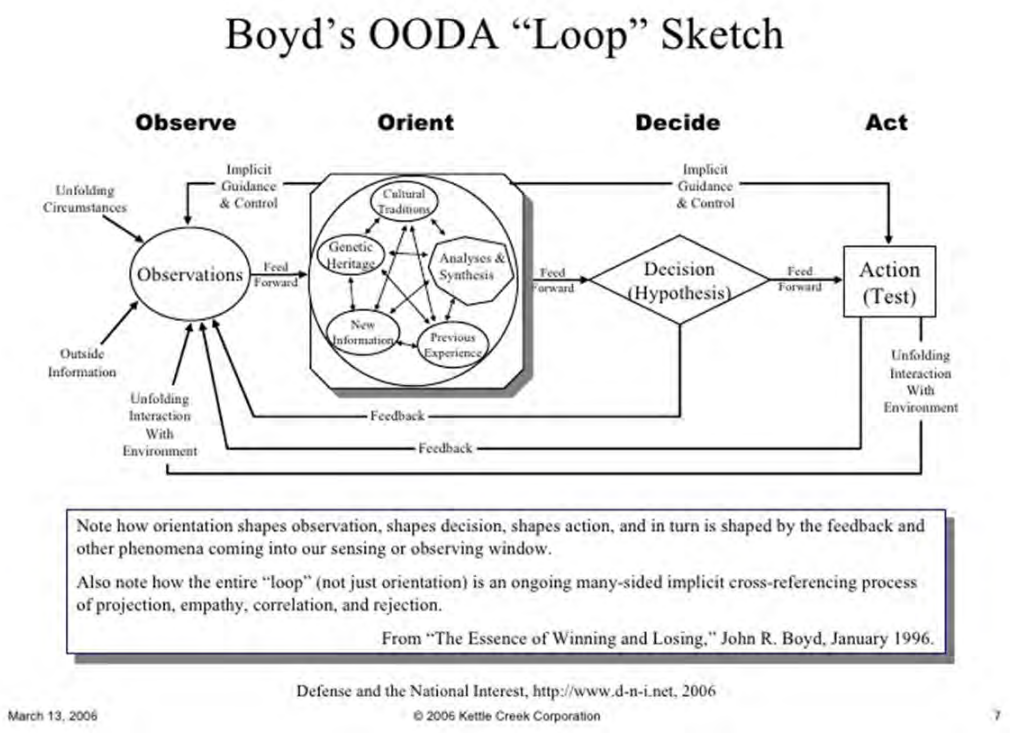

Figure 1.2 – Boyd's OODA Loop

Source: Boyd's OODA Loop, http://www.slideshare.net/Mewthom/boyds-ooda-loop

In his presentation, *Patterns of* Conflict, Boyd highlighted the goal of the theory of warfare he was proposing. With this strategy, the aim is to "Collapse (sic) adversary's system into confusion and disorder by causing him to over and under react to activity…".[161] Boyd advocated achieving this state by creating a "…rapidly changing environment…"[162] and by inhibiting "…an adversary's capacity to adapt to such an environment…"[163]

---

[161] John R. Boyd, December 1986, "Patterns of Conflict," *Air Power Australia*. Accessed August 6, 2016. http://ausairpower.net/APA-Boyd-Papers.html, 7.

[162] *Ibid*.

[163] *Ibid*.

With this strategy, Boyd stressed the importance of obtaining and maintaining the initiative against one's opponent. He argued that if you could conduct military operations within an adversary's OODA loop, you could paralyze both the commander and his forces.[164] To get inside an opponent's OODA loop, Boyd argued, one accomplished this by either "…"tightening" friendly OODA loops and/or "loosening" enemy OODA loops."[165] Clausewitz similarly recognized the need to minimize what he described as "…natural friction…"[166] within one's own forces, by drilling and training one's own troops to a very high standard. If one's forces were faster and more agile than one's opponents, this could permit a force to operate within the OODA loop of an opponent.[167] Hence, there are similarities in thought between Boyd and Clausewitz. Boyd goes further, however. By focusing on the psychological (by getting inside the decision loop of the enemy commander) and temporal (by operating at a faster operational tempo than the opposing forces)[168] aspects of warfare, Boyd has developed a model where one can create battlefield situations faster than one's opponent can react.[169] Boyd's focus is on the mind of the opposing military commander, and paralysing him.[170] This idea of leadership paralysis correlates well with the thinking of Warden.

---

[164] David S. Fadok, Air Power's Quest for Strategic Paralysis (thesis, Faculty of the School of Advanced Air Power Studies, Maxwell Air Force Base, Alabama: Air University Press, 1995), 2.

[165] *Ibid*.

[166] Antulio J. Echevarria II, Antulio J, *Clausewitz and Contemporary War* (Kindle Edition. Oxford University Press, 2007), 130.

[167] David S. Fadok, Air Power's Quest for Strategic Paralysis (thesis, Faculty of the School of Advanced Air Power Studies, Maxwell Air Force Base, Alabama: Air University Press, 1995), 14.

[168] *Ibid*.

[169] *Ibid*.

[170] *Ibid*., 2.

WARDEN'S THEORY OF AIRPOWER WINNING WARS

Robert Pape disagreed with Warden's argument that one did not have to destroy an opponent's military forces (namely the land forces), although he did acknowledge that "…in some circumstances, theater air power may be able to do most of the work."[171]He also disagreed with Warden's controversial argument that airpower alone could win a war, noting that air power "…slaughtered British, German, and Japanese civilians in the Second World War; threatened Egyptian civilians in the 1970 Egyptian-Israeli war of attrition along the Suez Canal…,"[172]yet still these populations did not press their leaders for a surrender. Warden countered Pape in a subsequent article, stating that his targeting plan (approved by General Schwarzkopf) was not based on Pape's war model of "…punishment, risk, denial, and decapitation…,"[173] instead, the targeting plan was to "…attack Iraq in order to change Iraq, the system, so that it would be compatible with the envisioned postwar peace."[174] The "…postwar peace…"[175] envisaged by Warden was "…Iraq out of Kuwait, and an Iraq that would not be a threatening regional superpower for an extended period of time…"[176]Warden's plan to achieve this was based upon his Concentric Ring Theory, and the goal was to"…. reduce the energy level of the entire system enough to reach our peace objectives."[177]Admittedly, however, while Warden's theory successfully dismantled the Iraqi regime, the longer term objectives of the

---

[171] Robert A. Pape, "The Limits of Precision-Guided Air Power." *Security Studies* 7, no. 2 (Winter 1997/98), 95.

[172] *Ibid*., 98.

[173] John A. Warden III, "Success in Modern War - A Response to Robert Pape's Bombing to Win." *Security Studies* 7 no. 2, Winter 1997/98, 173.

[174] *Ibid*., 175.

[175] *Ibid*.

[176] *Ibid*.

[177] *Ibid*.

Americans with respect to Iraq were not realized, namely building a stable regime that could "…make substantive progress in engendering a degree of legitimacy and administrative capacity…(and)…convince a sizeable proportion of the Iraqi population that it is ruling in their interests, furthering their collective ideas of what Iraq is and what it is to become."[178] Dodge notes that the longer term American plan with respect to Iraq "…failed spectacularly to build even the foundations of the infrastructural power needed to achieve this."[179]

Biddle also disagreed with the notion that airpower alone could win wars, in his analysis of the "Afghan model."[180]While this model was effective against poorly trained and poorly motivated ground forces who chose to remain in the open, its weakness was exposed when highly motivated Al Qaeda fighters chose to retreat into the mountains and cave networks. There, airpower was not able to reach them, and land forces' unique "…ability to cope with targets who reduce their exposure to deep attack by dismounting, dispersing, covering, and concealing themselves…"[181] was revealed. Pape and Biddle's arguments countering Warden's theory that air power alone can win wars, however, do not discount the fact that Warden's targeting theory is an effective model for analysing systems and for then targeting them. As Arwood et.al. note, Warden's targeting model is a systematic method to accomplish that task.[182]

---

[178] Toby Dodge, 2005, "Iraqi Transitions: from regime change to state collapse," *Third World Quarterly* (Taylor and Francis, Ltd.) 26 (4-5), 719.

[179] *Ibid*.

[180] Stephen Biddle, "Afghanistan and the Future of Warfare: Implications for Army and Defense Policy", Monograph, Carlisle, PA: Strategic Studies Institute, 1.

[181] *Ibid*., 57.

[182] Sam Arwood, Robert Mills and Richard Raines, Operational art and Strategy in Cyberspace, *International Conference* (2010), 18.

SUMMARY

Why would one wish to select the targeting model of Colonel John Warden and apply it to cyber? The targeting model is flexible enough such that it can be applied to cyber warfare. While Warden himself is an airpower advocate, others have been able to apply his model to systems where airpower cannot generate an effect. This is due to the flexibility and versatility of Warden's model. While Clausewitz was critical of those who sought to map out models for conducting warfare,[183] the targeting model proposed by Colonel John A. Warden III has been employed in several conflicts since it was first employed during the Gulf War. In addition to being applied in traditional conflicts, it has also been applied against terrorist organizations, with success. Warden himself recognized that his model could be applied against any entity that could be analysed as a system.

Warden's idea that one did not have to wage wars of attrition or annihilation solely against the forces of an opponent actually correlate with the writings of many of the great military thinkers. Many military leaders and military thinkers alike disagreed with his view that airpower alone could win wars. Analysis of battles from the War in Afghanistan does confirm their conclusion, that airpower alone cannot win wars. This fact, however, does not take away from Warden's theory being an effective targeting model.

---

[183] The Clausewitz Homepage, "On War – Carl von Clausewitz," last accessed 6 August 2016, http://clausewitz.com/readings/OnWar1873/BK2ch02.html#a.

CHAPTER 2 – WHY CYBER?

NOMENCLATURE FRAMEWORK FOR CYBER

Having accepted that Warden's targeting theory is a flexible and effective model to apply to systems in general, the next focus of the discussion is on cyber. First off, what is cyber, and what does it consist of? The lexicon for describing cyber is still nebulous. There are many terms, many definitions, and many variations of definitions as well. The terms cyber domain, cyber environment and cyberspace are used by different authors. According to the NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), the definitions of twenty-nine separate nations are listed on their website when defining the term cyberspace (or cyber space).[184] For one American definition, cyberspace is described as being the "…notional environment in which communication over computer networks occurs…"[185] In their framework manual on cybersecurity, NATO CCDOE quotes the definition for *Cyber Environment* provided by the International Telecommunication Union (ITU). This definition declares that the cyber environment "…includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks."[186]The NATO CCDOE framework manual also quotes the definition from the International Organization for Standardization (ISO). Their definition included the human element, and described the cyber environment as "…the complex environment resulting from the

---

[184] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, n.d. "Cyber Definitions," NATO Cooperative Cyber Defence Centre of Excellence, accessed August 11, 2016, https://ccdcoe.org/cyber-definitions.html.

[185] *Ibid*.

[186] International Telecommunication Union, n.d, "ITU Terms and Definitions," International Telecommunication Union, accessed August 11, 2016, http://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&rlink={3E2AC1A2-9D18-4235-80B6-7946B3266788}.

interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form."[187]The NATO CCDOE cites a Finnish definition when describing the term cyber domain, which it defined as being "…an electronic information (data) processing domain comprising of one or several information technology infrastructures."[188] What is the difference between *cyber* environment and *cyber* domain? When comparing/contrasting definitions for the terms environments and domains, AJP-3 defines environments as being "…unlimited…"[189], as opposed to domains, which "…have borders."[190]

A discussion of the nomenclature pertaining to cyber is important because, as Major-General Brett Williams, Director of Operations, J3, U.S. Cyber Command noted in 2014, the "…misuse of the word "cyber" is one reason we do not have a common framework for discussing cyberspace."[191]As noted above, there are a number of established definitions used by many countries and by many players. Attempting to standardize nomenclature is necessary if military operations are to be conducted within cyberspace. Acknowledging Major-General Williams' comment that a nomenclature framework for discussing cyber is lacking,[192] and acknowledging that the NATO Cooperative Cyber Defence Centre of Excellence (CCDOE) website alone publishes 29

---

[187] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 2012, *National Cyber Security Framework Manual*, edited by Alexander Klimburg, Tallinn: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 8.

[188] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, n.d. "Cyber Definitions," NATO Cooperative Cyber Defence Centre of Excellence, accessed August 11, 2016, https://ccdcoe.org/cyber-definitions.html.

[189] North Atlantic Treaty Organization, AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, (NATO Joint Doctrine Branch, 2011), 4-3.

[190] *Ibid*.

[191] Brett Williams, 2014, Cyberspace: What is it, where is it and who cares? March 13, accessed September 25, 2016, http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.

[192] *Ibid*.

separate national definitions alone for the term cyberspace;[193] the American definitions will be used in this paper. Thus, as per Major-General Williams' definition, cyberspace will be analogous to the term "cyber domain", with the "…key difference between cyberspace and the physical domains is that cyberspace is man-made and constantly changing."[194]Cyberspace, or cyber domain, is constrained by borders,[195] whereas when one uses the term cyber environment there is no constraint by borders.[196]

While one could correctly argue that cyber in general is not constrained by geographical borders; when one considers Bryant's description for achieving cyber superiority, that it would be "…local and transient…;"[197]the delineation between the two definitions begin to make sense. For example, in August 2008, Russia initiated a series of cyber attacks against Georgia in conjunction with its overall military campaign.[198]This attack was "local,"[199] as per Bryant's definition, with the result that the attack resulted in a "…significant informational and psychological impact on Georgia: it effectively isolated the Caucasus state from the outside world."[200]Russia did not control the entirety

---

[193] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, n.d. "Cyber Definitions," NATO Cooperative Cyber Defence Centre of Excellence, accessed August 11, 2016, https://ccdcoe.org/cyber-definitions.html.

[194] Brett Williams, 2014, Cyberspace: What is it, where is it and who cares? March 13, accessed September 25, 2016. http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.

[195] North Atlantic Treaty Organization, AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, (NATO Joint Doctrine Branch, 2011), 4-3.

[196] *Ibid*.

[197] William D. Bryant, 2013 Cyberspace superiority: a conceptual model, Maxwell AFB: Air University, 39.

[198] Paulo Shakarian, 2011, "The 2008 Russian cyber campaign against Georgia," *Military Review* 91 (6), 63.

[199] William D. Bryant, 2013 Cyberspace superiority: a conceptual model, Maxwell AFB: Air University, 39.

[200] Paulo Shakarian, 2011, "The 2008 Russian cyber campaign against Georgia," *Military Review* 91 (6), 63.

of the cyber environment, all around the world. They did have "local"[201] cyber superiority within the cyberspace/cyber domain in and around Georgia, along with air and land superiority for their respective domains in support of their military campaign. The definitions, when applied in this manner, do correlate with what actually occurred during the 2008 Russian war in Georgia, and other recent world events.

WHY CONDUCT TARGETING IN CYBERSPACE?

If military forces can operate in either the cyber environment or cyberspace, can a targeting model be applied? Warden's concentric ring theory was originally based on using air power to achieve strategic paralysis. Warden himself extrapolated his theory to other systems, some of which could not be influenced by airpower. Various authors have begun applying Warden's theory to different systems, significantly, systems which could be influenced by capabilities other than airpower. For example, in 2002, Chappel applied Warden's targeting model to a terrorist organization.[202] Notably, he recognized that Warden's model was not airpower exclusive, and that the system vulnerabilities that are exposed when applying Warden's model provides "…insight on how these vulnerabilities can be subjected to various forms of national power, including lethal and non-lethal

---

[201] William D. Bryant, 2013 Cyberspace superiority: a conceptual model, Maxwell AFB: Air University, 39.

[202] George G. Chappel, Jr., 2002, A Terrorist Organization as a System: Unleashing Warden's Five Ring Model, Final Report, Joint Military Operations Department, Naval War College, Newport, R.I.: Naval War College, 9.

means."[203] In 2006, Hazdra applied Warden's model specifically to Al Qaeda.[204] Arwood et.al. applied Warden's theory to cyberspace in 2010.[205] These authors have begun to seize upon the true value in Warden's theory – its utility. The next question to be asked is why would a commander need to focus on cyber? What, for example was so important about cyber that the Russians would incorporate cyber attacks into their military campaign against Georgia (amongst other examples)?[206]

Cyber is an ever-expanding realm of human activity. The NATO Review Magazine notes that in 1993, 1% of the world's information was exchanged through the internet.[207] In the year 2000, that percentage had jumped to 51%, and in 2007, 97% of the world's information was relayed through the internet.[208] Increasingly, cyber capabilities and the internet are becoming essential tools in human society. Malicious actions within cyberspace were first observed in 1988 with the Morris worm.[209]This worm was an experiment by a computer programmer to see how large the internet had grown, and exploited a weakness in UNIX systems. It spread throughout the United States, and resulted in computers slowing down until they were no longer capable of

---

[203] George G. Chappel, Jr., 2002, A Terrorist Organization as a System: Unleashing Warden's Five Ring Model, Final Report, Joint Military Operations Department, Naval War College, Newport, R.I.: Naval War College, 2.

[204] Lieutenant-Colonel Richard J. Hazdra, 2006, Al Qaeda as a System, Research Project, Carlisle Barracks, Carlisle, PA: U.S. Army War College, 1.

[205] Sam Arwood, Robert Mills, and Richard Raines, 2010, "Operational art and Strategy in Cyberspace." *International Conference on Information Warfare and Security* (Academic Conferences International Limited), 18.

[206] Paulo Shakarian, 2011, "The 2008 Russian cyber campaign against Georgia," *Military Review* 91 (6), 63.

[207] NATO Review Magazine, n.d., Cyber conflicts in pictures, accessed August 14, 2016, http://www.nato.int/docu/review/2013/cyber/photostory-cyber/EN/index.htm.

[208] *Ibid*.

[209] NATO Review Magazine, n.d., Cyber Timeline, accessed August 14, 2016, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

being used.[210]Over the next two decades, however, malicious cyber activity expanded with the growth of cyber itself, and by 2007, it became apparent that cyber tactics were being incorporated into larger, grander state strategies. This was first evident with cyber attacks waged by Russia against Estonia that year.[211] In April of 2016, the United States military adopted an overt posture, and stated that in order to exploit and disrupt the Islamic State's heavy reliance on both the internet and social media, United States Cyber Command would "…now aim operations at ISIS with the hope of disrupting "the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions"."[212] Friend and foe alike are connected via the internet, their systems are linked through the internet, and are dependent upon cyber systems. Attacking these capabilities is a natural extension of warfare.

THE DOMAIN DEBATE

While there is debate about what exactly cyberspace is, it is being recognized as being a necessary area that commanders and military planners must start taking into account. AJP-3, Allied Joint Doctrine for the Conduct of Operations describes cyber as being part of the overall operational environment. This doctrinal publication defines the operational environment encompassing "…the sea, land, air and space the adversary,

---

[210] NATO Review Magazine, n.d., Cyber Timeline, accessed August 14, 2016, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

[211] *Ibid*.

[212] Dan Turkel, 2016, The US military has a new plan to fight ISIS — and it starts with making the group 'extremely paranoid', April 26, accessed August 14, 2016, http://www.businessinsider.com/new-us-cyber-war-against-isis-2016-4.

neutral and friendly actors, facilities, weather, terrain, electromagnetic spectrum (EMS), and the information environment, ***which includes cyberspace***, within the JOA and areas of interest."[213] Hence, NATO considers cyber to be part of the operating environment. Specifically, AJP-3 notes that the operational environment is not exclusively air, land and sea components anymore, and that "…space, computer networks and the EMS (electromagnetic spectrum), particularly in terms of the acquisition and control of information, are important constituents of joint operations."[214]

McGuffin challenged the notion that cyberspace constituted being its own domain. While noting that military activities do take place in cyberspace, he assessed that some of the traditional military functions of Command, Sense, Shield, Act and Sustain (which could be conducted in Air, Land, Maritime and Space) could not be conducted in cyber.[215] Notably, McGuffin concluded that the Sustain function did not occur in cyberspace,[216]and that the conclusions drawn by some that actions which demonstrated activity in the Act domain were up for debate.[217] In addition, McGuffin noted that there was a dimensional aspect to the Air, Land, Maritime and Space domains, along with a sovereignty aspect,[218] which did not present themselves in cyber. Later, McGuffin and Mitchell argued that cyber "…falls short of the full war-fighting spectrum that can occur

---

[213] North Atlantic Treaty Organization, AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, (NATO Joint Doctrine Branch, 2011), 4-3.
[214] *Ibid*.
[215] Lieutenant-Colonel W. C. McGuffin, "Soldiers of Fortran: Militarization of the 5th Dimension," (Masters of Defence Studies Thesis, Canadian Forces College, Toronto, 2013), 32-33.
[216] *Ibid*., 46.
[217] *Ibid*., 43-44.
[218] *Ibid*., 26-27.

in land, sea, air and space conflicts."[219]Further, they argue that "…opportunities for decisive control in cyberspace differ significantly from those that exist in established domains of operation."[220]Space, sea, land and air domains can have force projected into them resulting in desired military effects being achieved. In order to achieve this, military forces must have specialists trained "…in the tactics and operations of those domains."[221] In contrast, McGuffin and Mitchell note that this "…is not the case with cyberspace."[222] As a result, cyber did not "…warrant the status of a domain,"[223]however would play more of a "…supporting role to enable war fighting on land, on sea, in air, and in space."[224]

Applegate argued that "…cyberspace is considered a warfighting domain…",[225]while noting that it is a "…contested domain characterized by constant conflict between various competitor states, non-state actors and private entities".[226]Applegate applied maneuver theory to cyberspace, proposing that cyber had the maneuver attributes of "…capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage…"[227] Later, he expanded this thinking further, describing both offensive and defensive cyber maneuver:[228]

a. "Offensive cyber maneuver:

---

[219] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014), 397.
[220] *Ibid*.
[221] *Ibid*., 404.
[222] *Ibid*.
[223] *Ibid*., *411*.
[224] *Ibid*.
[225] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012), IEEE Commun. Soc., 2.
[226] *Ibid*.
[227] *Ibid*., 4.
[228] *Ibid*., 7-11.

i. Exploitive Maneuver;

ii. Positional Maneuver; (and)

iii. Influencing Maneuver;"[229]

b. "Defensive cyber maneuver:

i. Perimeter Defense and Defense in Depth;

ii. Moving Target Defense;

iii. Deceptive Defense; (and)

iv. Counter Attack."[230]

Kuehl similarly considers cyberspace to be a domain. His model for defining a domain was based upon two criteria:

a. Physical attributes sufficiently distinct from the other domains; and

b. The need by humans to utilize some form of technology to exploit them.[231]

Kuehl notes that humans needed technology such as the wheel and chariot to move about the land; ships to move about the water; aircraft to move about the air, and spacecraft and satellites to operate in space.[232]The distinct nature of their attributes, combined with the human need of some technology to operate on or within these

---

[229] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012), IEEE Commun. Soc., 7 - 9.

[230] *Ibid*., 9 - 11.

[231] Daniel T. Kuehl, "From cyberspace to cyberpower: Defining the problem." *Cyberpower and national security*, 2009, accessed via http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf, 1.

[232] *Ibid*.

domains, is what makes each of them a distinct domain.[233]These same attributes, he argues, give rise to cyber being a domain in its own right as the fifth domain.[234]Kuehl acknowledges that in some ways, cyber is different from the other four domains (Land, Sea, Air, Space), given that it is a "…manmade environment…"[235] Kuehl assesses that the only difference between cyber and the four traditional domains is that "…we can more easily see and sense those domains."[236] What is similar between each of the domains, however, is that humans require "…manmade technologies to enter and exploit the other domains…"[237] as well. That is significant, because if humans require technologies to operate within the cyber domain, *these technologies can be targeted*. Some would argue that cyber does not have one of the key attributes specified by McGuffin in his criteria for domain recognition – that being a third dimension.[238] Kuehl differs on cyber not having a dimensional aspect, arguing that cyberspace exists in the layered "…three dimensions of the information environment…"[239]While acknowledging that describing cyber in terms of "dimensions" is more of a metaphor, in 2013 the United States Joint Publication 3-12, Cyberspace Operations also described cyberspace as having three distinct layers, consisting of a "Physical Network Layer, Logical Network Layer, (and a) Cyber-Persona Layer."[240]

---

[233] Daniel T. Kuehl, "From cyberspace to cyberpower: Defining the problem." *Cyberpower and national security*, 2009, accessed via http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf, 1.

[234] *Ibid*.

[235] *Ibid*., 4.

[236] *Ibid*.

[237] *Ibid*.

[238] Lieutenant-Colonel W. C. McGuffin, "Soldiers of Fortran: Militarization of the 5th Dimension," (Masters of Defence Studies Thesis, Canadian Forces College, Toronto, 2013), 26.

[239] Daniel T. Kuehl, "From cyberspace to cyberpower: Defining the problem." *Cyberpower and national security*, 2009, accessed via http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf, 7.

[240] Director, Joint Staff, 2013, *Joint Publication 3-12 (R) Cyberspace Operations*, Washington: Joint Chiefs of Staff, I-3.

Whether one agrees with McGuffin and Mitchell that cyber is less of a domain and more of a supporting element,[241] or with Kuehl, that cyber is a domain,[242]the past decade has shown an increase in the use of cyber in warfare. If, as Kuehl notes, one needs technologies to operate within the cyber domain,[243]perhaps these technologies and structures can be mapped out systemically, and perhaps they can be targeted using Warden's model. If one accepts only part of Kuehl's argument that one requires technologies to operate within cyberspace,[244] this gives rise to systems, structures and vulnerabilities that could be mapped out and attacked. Hence there is potential to take a theory originally used in air warfare and apply it to cyber.

Similarly, McGuffin notes that "… cyber capability could contribute to future military operations and national security objectives."[245] The capabilities used to achieve this can also be analysed and described as a system, and Warden's theory can be applied to it. Hence, regardless of whether you agree that cyber is a domain or not, it can be analysed as a system using the concentric ring theory. Warden's approach has generated notable success, and could result in dividends if applied to cyber.

---

[241] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors), Vol. 69 (3) (2014), 411.

[242] Daniel T. Kuehl, "From cyberspace to cyberpower: Defining the problem," *Cyberpower and national security*, 2009, accessed via http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf, 1.

[243] *Ibid*., 4.

[244] *Ibid.*

[245] Lieutenant-Colonel W. C. McGuffin, "Soldiers of Fortran: Militarization of the 5th Dimension," (Masters of Defence Studies Thesis, Canadian Forces College, Toronto, 2013), 78.

SUMMARY

What are the characteristics of cyber that make it so important to a society? Why would a military commander wish to conduct cyber operations as part of a larger military campaign? While there are differences as to whether cyber constitutes being a domain akin to air, land, sea and space, its importance to individuals, states and societies warrant it being subject to targeting in a conflict. Cyber is interwoven into our lives, our militaries and into society, and is an ever-expanding realm of human activity. Attacking cyber capabilities is a natural extension of warfare.

A strong debate exists as to whether cyber is a domain. There are those who argue that cyber does not constitute being a domain, as one would consider the other, more established domains. McGuffin and Mitchell argue that cyber does not possess the characteristics of the other environmental domains.[246] Most importantly, they note that cyber does not have trained operators capable of conducting warfighting as the Army, Navy and Air Force currently have.[247]

Applegate argued that cyber is a domain.[248] Further, he applied maneuver theory to cyberspace, arguing that cyber had many of the attributes attributable to maneuver.[249] Later, he expanded this thinking further, describing both offensive and defensive cyber maneuver.[250] For offensive cyber maneuver, he described three possible strategies –

---

[246] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors), Vol. 69 (3) (2014), 397.

[247] *Ibid*., 404.

[248] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 2.

[249] *Ibid*., 4.

[250] *Ibid*., 7-11.

exploitive, positional and influencing maneuver.[251] Applegate's maneuver strategies will be analysed in more detail in the next chapter.

Regardless if one accepts that cyber is a domain or it is not, cyber is still essential for individuals, militaries and states to conduct their day to day business. It is due its being so essential that cyber warrants being targeted in a conflict.

---

[251] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012), IEEE Commun. Soc., 7 - 9.

CHAPTER 3 – WARDEN APPLIED TO CYBER

EARLY CYBER WARFARE

One of the first examples of cyber being considered as part of a larger military plan was an idea presented to General Norman Schwarzkopf during the First Gulf War (1990 – 1991), just prior to Warden's targeting plan being implemented. Clarke and Knake refer to an occasion where Special Operations Command presented a plan that would see a team of special forces soldiers attacking an Iraqi radar installation just prior to the commencement of hostilities. They would be accompanied by computer experts, who would upload software into the radar network, causing "…computers on the network all over the country to crash and be unable to reboot."[252]General Schwarzkopf did not have confidence in either the plan nor the personnel proposing it, and as a result he rejected it.[253]At the time, he felt that should "…you want to make sure their air defense radars and missiles don't work, blow them up first. That way they stay dead."[254]

By 2003, before the commencement of hostilities for the Second Gulf War, the American military's perception of cyber as a weapon had evolved. Clarke and Knake refer to the United States military hacking into the secure military computer network used by the Iraqi military.[255] The Americans were overt in their activities this time, however.

---

[252] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 9.

[253] *Ibid*.

[254] *Ibid*.

[255] *Ibid*.

They sent emails to Iraqi officers on Iraq's "closed loop" network,[256] just prior to the start of the war. United States Central Command told the officers that the American's quarrel was with Saddam Hussein and his sons, and that they had no quarrel with any Iraqi soldier who parked his tanks and vehicles and abandoned them.[257] This plan was successful. When the Americans moved into Iraq, "… many units had neatly parked their tanks in rows outside their bases, thus allowing U.S. aircraft to neatly blow them up. Some Iraqi army commanders sent their troops on leave in the hours before the war."[258]

RUSSIA VERSUS ESTONIA

In April 2007, the Government of Estonia arranged to move a statue called the "Bronze Soldier"[259]This action sparked a riot by the minority Russian community within Estonia.[260] Of greater significance, however was that between 27 April to 18 May 2007, powerful cyber attacks were launched - specifically distributed denial-of-service (DDoS) attacks - "…targeting the country's infrastructure (that) shut down the websites of all government ministries, two major banks, and several political parties. At one point, hackers even disabled the parliamentary email server."[261]The attacks were allegedly wrought by pro-Russian hackers, however Clarke and Knake note that this was not some amateur hacker attack. This was a well-organized, elaborate attack, which involved

---

[256] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 9.

[257] *Ibid*., 10.

[258] *Ibid*.

[259] Stephen Herzog, 2011 "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 50.

[260] *Ibid*.

[261] *Ibid*., 51.

"….targeting Internet addresses most people would not know, not those of public webpages, but the addresses of servers running parts of the telephone network, the credit-card verification system, and the Internet directory."[262]While Herzog acknowledges that "…we may never know the true extent of Kremlin involvement in the cyber attacks on Estonia, it is clear that Russian officials encouraged the hackers…"[263]Further, he assesses that the Russians "…tolerated and encouraged the cyber attacks, and the Kremlin may have even colluded with the hackers responsible for the strikes."[264]

ISRAEL VERSUS SYRIA

Later that year, on September 6, 2007, at a "…North Korean – designed nuclear weapons plant…"[265] under construction in Syria, an Israeli strike package of F-15 Eagles and F-16 Falcons launched an attack that completely destroyed the facility.[266]What is significant about this attack is that despite being equipped with a modern Russian air defence system, the Syrians were unaware of the incoming attack. In particular, what "…appeared on the radar screens was what the Israeli Air Force had put there, an image of nothing."[267]The Syrians immediately went to the Russians to ask what happened.[268]The Russians were distressed, not only because they were not exactly sure

---

[262] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 15.

[263] Stephen Herzog, 2011 "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 53.

[264] *Ibid*., 55.

[265] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 3.

[266] *Ibid*., 2.

[267] *Ibid*., 5.

[268] *Ibid*.

what was compromised in their system, but also because they were about to sell a similar system to Iran.[269] Exactly how Israel defeated the Syrian/Russian radar system is something known to only a select group. The consensus is that Israel launched a cyber attack to defeat the Syrian/Russian radar system, somehow transmitting "…1' s and 0' s to control what the Syrian air defense radars saw."[270] Applegate described the attack as being "…a combination of both electronic and cyber-attacks which caused all of Syria's air defense radar systems to go offline for the duration of the raid."[271]By launching a cyber attack instead of a kinetic strike against Syrian air defence radars, the Israeli's kept the element of surprise until the last minute, and "…in the age of cyber war, the Israelis ensured that the enemy could not even raise its defenses."[272] Applegate notes that Israeli confidence in launching this form of attack implies that they "…had already gained the necessary level of access into these systems and had pre-positioned themselves to carry out this attack."[273]

Clarke and Knake propose three possibilities as to how the Israelis managed to launch their cyber attack against the Syrian/Russian radar system. The first would involve a stealth drone, that would transmit data packets down to the radar system, telling it to

---

[269] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 6.

[270] *Ibid*.

[271] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8-9.

[272] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 6.

[273] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

display a blank screen, while simultaneously not reporting any defect to an operator.[274] Clarke and Knake note that the American military "… has a similar cyber-attack system, code-named Senior Suter."[275]The second would involve Israel or an ally somehow inserting a digital back door or "Trojan Horse,"[276] that would respond to pre-arranged codes or signals to display a blank screen.[277]The third would be if an Israeli operative somehow accessed the fibre-optic cable connecting the air defence system, and triggered the Trojan that way.[278]

RUSSIA VERSUS GEORGIA

The next example of cyber attacks being employed and coordinated as part of a larger campaign occurred during the August, 2008 Russian invasion of Georgia.[279] DDoS style attacks were launched against "…Georgian news and government websites."[280]Shakarian noted that these attacks occurred the day prior to the ground invasion, and concluded that "…the hackers knew about the date of the invasion beforehand."[281]Clarke and Knake noted the "…intensity and sophistication…"[282] of the

---

[274] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 6-7.

[275] Ibid., 7.

[276] *Ibid*.

[277] *Ibid*., 8.

[278] *Ibid*.

[279] Paulo Shakarian, 2011, "The 2008 Russian cyber campaign against Georgia," *Military Review* 91 (6), 63.

[280] *Ibid*.

[281] *Ibid*.

[282] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 19.

attack, which (as noted also by Shakarian),[283] was initiated "…just as the ground fighting broke out."[284]As a result of this significant cyber attack, hackers took control of the .ge web domain,[285] Georgia was cut-off from the global banking network (including credit card transactions),[286] and the government had to transfer the Georgian President's webpage to a site in the United States.[287] Chayes states that this war represented the first time where there was a coordinated cyber "…attack synchronized with major combat actions in the other warfighting domains."[288]

STUXNET VIRUS

In 2008, Israel suspected that Iran was planning on developing nuclear weapons using material from its Natanz nuclear facility, and requested specialized American bunker busting bombs and American authority to route an air attack through Iraqi airspace in order to destroy the facility.[289] Talbot notes that the Israeli attack plan was quite advanced, and included 100 fighter aircraft involved in "...a contingency exercise flown over the Mediterranean in 2008…"[290] Sanger reported that President Bush did not agree to this request, instead, he "…told the Israelis that he had authorized new covert

---

[283] Paulo Shakarian, 2011, "The 2008 Russian cyber campaign against Georgia," *Military Review* 91 (6), 63.

[284] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 19.

[285] *Ibid*.

[286] *Ibid*., 20.

[287] *Ibid*., 19.

[288] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 477.

[289] David E. Sanger, 2009, U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site, January 10, Accessed November 20, 2016, http://www.nytimes.com/2009/01/11/washington/11iran.html.

[290] Brent J. Talbot, 2011, "Stuxnet and After," *Journal of International Security Affairs*, Fall/Winter - Number 21, 74.

action intended to sabotage Iran's suspected effort to develop nuclear weapons…"[291] This covert action appears to have been using the Stuxnet virus to attack hardware within the Natanz facility.

The Stuxnet virus was first detected in June 2010,[292] however Chen notes that evidence has been reported by Microsoft that would date the code to as early as January 2009.[293] Lindsay states that the Stuxnet virus was a "…US-Israeli…"[294] initiative; just one element of a "…broader US cyber campaign against Iran code-named "Olympic Games"."[295]What is significant about the Stuxnet virus is that it "…is the first instance of a computer network attack known to cause physical damage across international boundaries."[296]How significant this attack was is up for debate. McGuffin and Mitchell note that the damages resulting from Stuxnet "…were not described as an armed attack by the targeted state."[297]The targeted state was Iran,[298] and the targeted systems were the uranium enrichment centrifuges at Iran's Natanz facility.[299] Chen states that the virus attacked the software (specifically the supervisory control and data acquisition software, or SCADA) that ran the programmable logic controllers (PLCs) which allowed users to enter information and control the centrifuges in question.[300]By interfering with this

---

[291] David E. Sanger, 2009, U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site, January 10, Accessed November 20, 2016, http://www.nytimes.com/2009/01/11/washington/11iran.html.

[292] Jon R. Lindsay, 2013, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22 (3), 365.

[293] Thomas M. Chen, 2010, "Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]," *IEEE Network* 24 (6), 2.

[294] Jon R. Lindsay, 2013, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22 (3), 366.

[295] *Ibid*.

[296] *Ibid*., 365.

[297] Chris McGuffin and Paul Mitchell, 2014, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3), 411.

[298] Jon R. Lindsay, 2013, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22 (3), 366.

[299] *Ibid*.

[300] Thomas M. Chen, 2010, "Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]," *IEEE Network* 24 (6), 3.

software, Shakarian notes that Stuxnet would then set a rotational frequency speed close to the maximum potential speed of the centrifuges in question, eventually damaging them.[301] The true impact of this attack is known only to the Iranians, and damage estimates vary in the literature. Chen noted a mysterious decrease of "…15 percent in production in 2009, around when Stuxnet is believed to have been spreading."[302]Shakarian notes that between 2009 and 2010, Iran "…decommissioned and replaced about 1,000 IR-1 centrifuges at the Natanz FEP (6 cascades of 164 centrifuges each)."[303]

In addition to setting back Iran's nuclear program, the Stuxnet attack also prevented a potential Middle East conflict from breaking out. Sanger reported that the Bush Administration was worried at the time that an "…airstrike could ignite a broad Middle East war in which America's 140,000 troops in Iraq would inevitably become involved."[304] This war did not occur, however, due to the damaging cyber attack that was launched.

UNITED STATES VERSUS ISLAMIC STATE

The Russian campaigns in Estonia and Georgia were examples where Russia sought to achieve cyber superiority over the countries in question, and then deny them

---

[301] Paolo Shakarian, 2011, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal* (United States Military Academy), smallwarsjournal.com, 4.

[302] Thomas M. Chen, 2010, "Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]," *IEEE Network* 24 (6), 3.

[303] Shakarian, Paulo, 2011, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal* (United States Military Academy) 1 – 10, smallwarsjournal.com, 5.

[304] David E. Sanger, 2009. U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site, January 10. Accessed November 20, 2016, http://www.nytimes.com/2009/01/11/washington/11iran.html.

access to the internet. The American efforts to defeat the Islamic State, referred to also as ISIS, ISIL or Daesh, are markedly different. Members of the Islamic State have been very active on social media. In addition to broadcasting prisoner videos, members of the Islamic state would post everything from selfies to trophy photos to threats against other countries. Lesaca estimates that as of 2015, Russia alone was threatened 25 times via the internet, and France was threatened 20 times.[305] Many people were understandably outraged at what was being posted by the Islamic State on social media. An unnamed source from one of the major social media sites acknowledged this very fact in an article in the Guardian, stating "…there are lots of people who want us to take these accounts down or block them."[306]The main reason they do not, however, is because "…the government intelligence and military want us to keep them up, because that's how they track them."[307] One specific example was provided by the Commander Air Combat Command, General Herbert "Hawk" Carlisle, who provided an example where USAF members "…recognized a comment on social media and turned that into an airstrike that resulted in three Joint Direct Attack Munition (JDAM) bombs destroying an Islamic State in Iraq and Syria (ISIS) headquarters building."[308]

In April of 2016, however, the United States openly acknowledged a new front in its cyber campaign. Instead of simply gathering intelligence from social media, the United

---

[305] Javier Lesaca, 2015, "Fight against ISIS reveals power of social media," The Brookings Institution, November 19, accessed October 5, 2016, https://www.brookings.edu/blog/techtank/2015/11/19/fight-against-isis-reveals-power-of-social-media/.

[306] Charles Arthur, 2014, "Taking down ISIS material from Twitter or YouTube not as clear cut as it seems," The Guardian, June 23, accessed October 5, 2016, https://www.theguardian.com/world/2014/jun/23/taking-down-isis-youtube-twitter-google-video.

[307] *Ibid*.

[308] Michael Hoffman,2015, "US Air Force Targets and Destroys ISIS HQ Building Using Social Media," DEFENSETECH, June 3, accessed October 5, 2016, http://www.defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/.

States overtly announced that it was engaging in cyber operations designed to "…disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters."[309] Pomerleau quotes Defense Secretary Ashton Carter, who stated the objectives to be "…interrupt ISIL command and control, interrupt its ability to move money around, interrupt its ability to tyrannize and control population, interrupt its ability to recruit externally – all of that it does in a cyber-enabled way…"[310] In addition to disrupting the Islamic State in general, Sanger notes that this strategy also has the benefit of rattling "…the Islamic State's commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data."[311]One tactic, which both rattles commanders and delivers kinetic effects against fighters on the ground is a process whereby American cyber operatives first study Islamic State commanders, and learn their "…online habits."[312] The Americans then "…imitate them or to (sic) alter their messages, with the aim of redirecting militants to areas more vulnerable to attack by American drones or local ground forces."[313] In another example, the Americans would target finances, by "…using cyberattacks to interrupt electronic transfers and misdirect payments."[314]

---

[309] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[310] Mark Pomerleau, 2016, "Cyber operations come out of the shadows," DEFENSE SYSTEMS. May 5, accessed October 5, 2016, https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.

[311] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[312] *Ibid*.

[313] *Ibid*.

[314] *Ibid*.

RUSSIA AND THE 2016 AMERICAN ELECTION

On October 7th, 2016, the Department of Homeland Security issued a press release, stating that the United States "…is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations."[315]Specifically, they concluded that the mass leaks of hacked information and emails by Guccifer 2.0, WikiLeaks and DC Leaks were "…consistent with the methods and motivations of Russian-directed efforts…",[316] with the intent of interfering "…with the US election process."[317]Noting that Russia has employed these same tactics across both Eurasia and Europe, with the intent of influencing public opinion;[318]Homeland Security officials conclude that "…only Russia's senior-most officials could have authorized these activities."[319]Meyer notes that the "…hack has especially targeted individuals around Democratic nominee Clinton…,"[320] was ordered by the Russian government leadership, and "…is an attempt to influence the presidential election and advance the broader strategic objectives of the Putin regime."[321]

These are all impressive examples of cyber warfare in action, each with varied intent and purpose. The question must now be asked, however, are any patterns emerging? Can any models or systems be applied or derived from these examples? Are

---

[315] Department of Homeland Security Press Office, 2016, Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security, October 7, Accessed October 8, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[316] *Ibid*.

[317] *Ibid*.

[318] *Ibid*.

[319] *Ibid*.

[320] Meyer, Josh. 2016, Russia Hack of U.S. Politics Bigger Than Disclosed, Includes GOP, October 8, accessed October 10, 2016, http://www.nbcnews.com/news/us-news/russia-hack-u-s-politics-bigger-disclosed-includes-gop-n661866.

[321] *Ibid*.

these just random actions, striking at diverse targets, or can some form of framework be applied to what has occurred (whether intended by the aggressors or not)?

APPLEGATE'S CYBER MANEUVER THEORY

Applegate applied maneuver theory to cyberspace.[322] He noted that the overall goal of cyber maneuver was the same as kinetic forms of maneuver, namely to "…secure positional advantages in respect to an enemy or competitor state…"[323] While doing so, he noted (as did McGuffin and Mitchell)[324] that cyber maneuver is *different* from kinetic forms of maneuver, with Applegate noting that the manner in which cyber maneuver is executed is "…conducted at machine speeds inside a virtual construct."[325] Cyber effects are somehow different as well, however, in that following known cyber attacks such as Stuxnet, the targeted state did not view the outcome as having been an "…armed attack…"[326] While McGuffin and Mitchell argued that this fact contributed to cyber not warranting domain status,[327] Applegate observed that this was a unique feature of cyber warfare – the duality that anonymity and difficulties with attributing the attack result in no retaliations, in comparison with real world actions that would have resulted in open

---

[322] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012), IEEE Commun. Soc., 7.

[323] *Ibid*.

[324] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014), 410.

[325] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012), IEEE Commun. Soc., 7.

[326] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014), 411.

[327] *Ibid*.

conflict.[328] Above all else, however, the effect that cyber maneuver generates is to "…influence human and machine behaviour."[329]

The idea of using maneuver to avoid battle (or conduct warfare by different means) also correlates with Delbrück's thinking. He agreed with Turenne,[330] preferring a "…maneuver strategy that is clever and active but avoids combat….,"[331] with the result that "…one could turn completely away from the decision by battle…,"[332] and that a nation could achieve its aims in a different way.[333]Applegate's maneuver theory corresponds to that proposed by Delbrück, and agrees with Warden as well.

Applegate's theory outlines different operational forms of maneuver. They could be employed separately, or together, in a phased approached. In particular, he described the elements of offensive cyber maneuver:[334]

a. Exploitive Maneuver – securing information for advantage at the tactical, operational or strategic level;[335]

b. Positional Maneuver – compromising or outright seizing of key nodes in the cyber environment, and then utilizing these nodes for your benefit;[336] and

---

[328] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012), IEEE Commun. Soc., 14.

[329] *Ibid*., 4.

[330] Hans Delbrück, 1975, English language edition published 1985, *History of the Art of War Within the Framework of Political History*, Translated by Walter J. Renfroe, Jr., Vol IV, Westport: Greenwood Press, 335.

[331] *Ibid*.

[332] *Ibid*., 387.

[333] *Ibid*.

[334] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 7.

[335] *Ibid*., 7 - 8.

[336] *Ibid*., 8 - 9.

c. Influencing Maneuver – Applegate describes an influencing maneuver as "…the process of using cyber operations to get inside an enemy's decision cycle or even to force that decision cycle though direct or indirect actions." For example, somehow compromising an enemy's C2 system, injecting or changing data, and influencing a commander such that he begins to doubt his systems and/or slow down his decision loop."[337]

Has Applegate defined different strategies that can be conducted when waging cyber warfare? Does his model make sense? Looking back at the examples provided earlier in this chapter, it appears that in some cases, the attacker wanted to deny and disrupt the internet use of the country under attack. This was demonstrated in 2007 with Russian aggression against Estonia,[338] and in 2008 during the Russian invasion of Georgia.[339]These strategies correspond most closely with Applegate's definition of Influencing Maneuver, where cyber operations are conducted "…to gain and maintain information superiority and dominance and to maintain freedom of maneuver in cyberspace."[340]

The United States is not following this strategy, however, in its war against the Islamic State. In this case, the strategy adopted by the Americans it to *not* deny access or use of the internet to its opponent. Both the Islamic State and individual fighters are being

---

[337] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

[338] Stephen Herzog, 2011, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 51.

[339]Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 19.

[340] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

allowed access to the internet, via their computer systems and personal cell phones. Access to social media sites has been allowed as well (despite pressure otherwise), with the United States taking full advantage of targeting opportunities that arise due to poor operational security on the part of Islamic State fighters.[341]This example most closely correlates with Applegate's definition of Exploitive Maneuver, whereby an attacker captures "…information resources in order to gain a strategic, operational or tactical competitive advantage."[342] Applegate notes that how the information gained from this form of maneuver is applied "…makes it a valid and dangerous form of cyber maneuver."[343]

In the final type of example, cyber was used in a manner similar to that noted by McGuffin and Mitchell, that being as a supporting capability to a larger military operation.[344] Applegate referred to this as being Positional Maneuver, whereby "…key physical or logical nodes in the information environment…"[345] are captured or compromised. The example that Applegate himself gives for this type of maneuver is the 2007 Israeli attack on a Syrian reactor, which was preceded by an apparent electronic and cyber attack.[346]In keeping with McGuffin and Mitchell's thinking that cyber would be supporting a larger operation,[347] Applegate notes that using "…positional maneuver prior

---

[341] Michael Hoffman, 2015, "US Air Force Targets and Destroys ISIS HQ Building Using Social Media," DEFENSETECH, June 3, accessed October 5, 2016, http://www.defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/.

[342] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 7.

[343] *Ibid*.

[344] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014), 411.

[345] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8.

[346] *Ibid*.

to the initiation of actual kinetic combat operations set them up for success and illustrates the potential decisive nature of this form of cyber maneuver,"[348]

Whether intended or not, each of the examples given at the beginning of this chapter seem to fit one of Applegate's three maneuver models. In some cases, an attacker seeks to obtain cyber superiority, and then deny internet access to its opponent.[349] In other cases, an attacker intentionally allows a defender to continue to access the internet, while reaping the treasure trove of intelligence leaked by an unsuspecting foe.[350] Or, an attacker may use cyber to support a larger operation.[351]To date, Applegate's maneuver strategy seems to quite accurately describe the different cyber strategies that have been conducted during recent campaigns.

WARDEN AND CYBER

Can one apply Warden's targeting theory to each one of Applegate's maneuver strategies? Warden found most complex systems could be broken down into sub-elements. The first step in applying Warden's model to any potential system is systems understanding. As discussed earlier, for most systems, be they biological, industrial or natural, Warden found that each could be broken down into five separate components:

a. "leadership or direction;

---

[347] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014), 411.

[348] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

[349] *Ibid*.

[350] *Ibid*., 7.

[351] *Ibid*., 8.

b. organic essentials;

c. infrastructure;

d. population; (and)

e. a fifth component that protects the system from outside attack or general degradation."[352]

Can this model be applied to cyber? Arwood et.al. noted that the systems and targeting model developed by Warden were "…developed to provide insight into how a complex system (nation-state, drug cartel, terrorist group) would be attacked via its centers of gravity, with emphasis on defeating the organization."[353]In comparing cyber power to air power, Arwood et.al. note that the core of "…strategic air power theory was the idea that wars could be won by striking at the heart of the enemy rather than having to grind through a protracted terrain conflict."[354] They note that a unique feature of air power was the compressed "…time and distance…"[355] on the battlefield, and that similar features are shared by cyber; notably that attacks may be launched "…from anywhere in the world…"[356]

When noting the similarities between air power and cyber power, one must also consider the issue of domain superiority. A key tenet in Warden's theory using airpower was that both strategic and operational air superiority were crucial to the success of the

---

[352] John A. Warden, 1995, "The Enemy as a System," *Airpower Journal* 9 (1), accessed September 11, 2016, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

[353] Sam Arwood, Robert F. Mills, and Richard A. Raines, 2010, "Operational Art and Targeting Strategy for Cyberspace Operations," *IOSphere* (Spring), 34.

[354] *Ibid*., 32.

[355] *Ibid*.

[356] *Ibid*.

overall plan.[357] How would one define cyber superiority? In building his definition for cyber superiority, Bryant used the air domain as a template.[358] He argued that cyber superiority "…will be local and transient."[359] Further, Bryant cited Joint Publication 3-12, Cyberspace Operations, which states cyberspace superiority is the "…degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary."[360]

When trying to apply Warden's theory to Applegate's maneuver strategies, a logical counter argument would be that perhaps the attackers were not thinking of Warden's model when they conceived of their attack. This issue was addressed by Distelzweig in his analysis of Operations Unified Protector and Odyssey Dawn in Libya. There, he concluded that the "…planning and execution of Operations Odyssey Dawn and Unified Protector followed Colonel John A. Warden's theory of warfare, based on the importance of air superiority and attacking the enemy as a system, **even if this was not the intended methodology**."[361]

---

[357] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 118.

[358] William D. Bryant, 2013, Cyberspace superiority: a conceptual model, Maxwell AFB, Air University, 26.

[359] *Ibid*., 39

[360] Director, Joint Staff, 2013, *Joint Publication 3-12 (R) Cyberspace Operations*, Washington: Joint Chiefs of Staff, GL-4.

[361] Kurt Distelzweig, "Operations Odyssey Dawn and Unified Protector: Another Win for Warden's Theory" (School of Advanced Military Studies Monograph, School of Advanced Military Studies. 2014), 2.

If one accepts that argument, can Warden's concentric ring theory be applied to Applegate's cyber-maneuver model; namely the three distinct offensive strategies which appear to be emerging?

WARDEN AND APPLEGATE'S EXPLOITIVE MANEUVER STRATEGY[362]

This targeting model would be similar to the cyber strategy adopted by the Americans against ISIS. The enemy would not be denied access to the internet nor cyber capabilities, allowing the attacker to exploit the enemy through the internet. Applying Warden's template, the model[363] would look like this:

a. Fielded military – The United States overtly announced that it was engaging in cyber operations designed to "…disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters."[364] This strategy directly affects the fielded fighting forces of the Islamic State; by impacting recruiting efforts, and by affecting the confidence that Islamic State fighters have in their State, in particular if an outside power can disrupt their pay system.[365] One tactic which would have a significant impact on morale would be spoofing orders given by their own commanders (whom the Americans

---

[362] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 7.

[363] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter, (Air University Press No. 3, 1995), 108.

[364] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[365] *Ibid*.

have studied and learned their "…online habits…"[366]). While directly affecting the inner leadership ring, this tactic would also affect the troops on the ground as well. Once Islamic State fighters became aware that the Americans were capable of spoofing their commanders online, they would never know if orders being passed were those of their commanders ordering them to battle, or if they were spoofed orders from the Americans, ordering them to a location where death from lethal coalition airpower would be waiting for them. The overall American strategy against the Islamic State's fighting forces was to permit them to stay online, while reaping the benefits of the intelligence that could be gained while concurrently disrupting operations and causing a loss of confidence with respect to their leadership and the orders they were being given.

b. Population – The American cyber strategy with respect to the population appears focused on disrupting "…the ability of the Islamic State to spread its message…"[367] Pomerleau notes that part of their strategy is to "…interrupt its ability to tyrannize and control (the) population…"[368] By interfering with the Islamic State's ability to communicate, influence and terrorize the population, the Americans are influencing the population itself.

---

[366] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[367] *Ibid*.

[368] Mark Pomerleau, 2016, "Cyber operations come out of the shadows," DEFENSE SYSTEMS. May 5, accessed October 5, 2016, https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.

c. Infrastructure – According to American Treasury Secretary Jacob Lew, "…Isis needs access to the international financial system for oil equipment, weapons, communications equipment and other imported items which requires them to move funds and that provides opportunities for attack."[369] Along with other tactics, the Americans would target finances, by "…using cyberattacks to interrupt electronic transfers and misdirect payments."[370] Pomerleau notes that the Americans would use cyber against the Islamic State to "…interrupt its ability to move money around…"[371]By attacking financial infrastructure, the Americans concurrently disrupted two important system essentials – oil (sold for money), and money itself. With respect to other possible infrastructure cyber targets, Agence France-Presse cited a 2015 briefing to a Senate panel by the director of the National Security Agency, Admiral Michael Rogers. Specific mention was made of, "…critical infrastructure networks -- power grids, transportation, water and air traffic control, for example -- where a computer outage could be devastating."[372]

d. System Essentials – American Treasury Secretary Jacob Lew assessed oil and oil revenues to be an Islamic State strength, noting that "…Isis has reaped an

---

[369] Associated Press at the United Nations, 2015, United Nations adopts plan to attack Islamic State's funding, December 17, accessed October 9, 2016. https://www.theguardian.com/world/2015/dec/17/united-nations-plan-islamic-state-funding-terrorist-group-al-qaida.

[370] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[371] Mark Pomerleau, 2016, "Cyber operations come out of the shadows," DEFENSE SYSTEMS. May 5. Accessed October 5, 2016, https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.

[372] Agence France-Presse, 2015, Cyber Attackers Leaving Warning 'Messages': NSA Chief, March 19, accessed November 20, 2016, http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief.

estimated $500m from black market oil and millions more from the people it brutalises (sic) and extorts."[373] This financial strength, however, is also something that could be targeted. In another example, the Americans would target finances, by "…using cyberattacks to interrupt electronic transfers and misdirect payments."[374] The United States would also attack the Islamic State's financiers, oil and money directly. In 2015, American Special Forces conducted a raid that killed senior Islamic State financier Abu Sayyaf, obtaining "…reams of data on how ISIS operates, communicates and earns its money," the official told CNN, referring to some of the communications elements, such as computers, seized in the raid."[375] Exploiting the intelligence gleaned from the computers taken during the Sayyaf raid, along with "…a combination of satellite imagery, electronic intercepts and informers' tips, analysts have tracked Islamic State operatives storing huge amounts of cash in bank vaults, private residences and other hiding places."[376] The result, as of May 2016, has been "…21 strikes on cash storage and distribution sites since October, destroying what the Central Command said was hundreds of millions

---

[373] Associated Press at the United Nations, 2015, United Nations adopts plan to attack Islamic State's funding, December 17, accessed October 9, 2016. https://www.theguardian.com/world/2015/dec/17/united-nations-plan-islamic-state-funding-terrorist-group-al-qaida.

[374] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[375] Barbara Starr and Laura Smith-Spark, 2015, Abu Sayyaf, key ISIS figure in Syria, killed in U.S. raid, May 17, accessed October 9, 2016, http://www.cnn.com/2015/05/16/middleeast/syria-isis-us-raid/.

[376] Schmitt, Eric, 2016, U.S. Says Its Strikes Are Hitting More Significant ISIS Targets, May 25, Accessed October 10, 2016, http://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?_r=0.

of dollars."[377] The American cyber strategy with respect to system essentials appears to be to use it in conjunction with other kinetic means to disrupt and destroy essential resources such as oil and money.

e. Leadership – The example cited earlier, of American hacking directly into the secure military computer network used by the Iraqi military,[378]is a good example of targeting the center leadership ring in an exploitive cyber maneuver strategy. By sending personal emails directly to Iraqi officers,[379] prior to the commencement of hostilities, the Americans influenced these leaders to park the fighting vehicles under their command and send personnel on leave.[380] The Americans did not have to fight these armoured vehicles nor those troops on the ground."[381] By employing a similar exploitive strategy against the Islamic State, the United States is influencing the leadership a different way. The Americans are disrupting the ability of the State to "…circulate orders from commanders and carry out day-to-day functions...."[382] The Americans are being overt in their actions, however, with the effect of rattling "…the Islamic State's commanders, who have begun to

---

[377] Schmitt, Eric, 2016, U.S. Says Its Strikes Are Hitting More Significant ISIS Targets, May 25, accessed October 10, 2016, http://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?_r=0.

[378] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 9.

[379] *Ibid*.

[380] *Ibid*., 10.

[381] *Ibid*.

[382] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

realize that sophisticated hacking efforts are manipulating their data."[383] Finally, by studying Islamic State commanders, and learning their online habits, the Americans intermittently spoof them by sending false orders to their troops.[384] The American cyber strategy with respect to leadership appears to be disrupting the ability of the Islamic State commanders to command effectively, and to affect the confidence they have with respect to the information they are receiving, and the orders they are giving.

WARDEN AND APPLEGATE'S INFLUENCING MANEUVER STRATEGY[385]

This targeting model would be similar to the cyber strategy adopted by the Russians against Estonia in 2007 and Georgia in 2008. The attacking state would seek to achieve cyber superiority, and then would attempt to deny access to the internet for the country under attack. Applying Warden's template, the model[386] would look like this:

a. Fielded military – Hollis notes that the first cyber target attacked by Russia in their 2008 campaign against Georgia was a hacking forum.[387] While not military targets per se, in cyber warfare this group does constitute "fielded military". Hollis states that by attacking the Georgian hacking community

---

[383] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[384] *Ibid*.

[385] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 9.

[386] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 108.

[387] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, no. 11 (January 6, 2011), 3.

first, "…Russian-supported hacker militia pre-emptively (sic) tried to forestall or mitigate a counter-attack (or returning fire) from Georgian hackers."[388] This attack contributed to Russian cyber superiority. Chayes notes that the deluge of DDoS cyber attacks against Estonia in 2007 left their military "…unable to communicate."[389]One year later, during the 2008 war between Russia and Georgia, the Russians again launched DDoS attacks against Georgian military networks;[390] again impacting the military's ability to communicate. The overall Russian cyber strategy against the military appeared to be to shut down its communications, impacting it ability to operate.

b. Population – The cyber attacks by Russia against Estonia had a significant impact upon the Estonian population. Chayes notes that "Estonia was a highly-wired society…,"[391] however the conveniences of having such a wired society also served as a vulnerability. Herzog notes that "…97 percent of bank transactions occur online; and in 2007, 60 percent of the country's population used the Internet on a daily basis."[392] The ability of the population to properly function as a society "…was nearly brought to a halt in less than a month…"[393] due to the Russian cyber attacks. When the Russians conducted similar attacks against Georgia in 2008, the result was that the Russians

---

[388] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, no. 11 (January 6, 2011), 3.

[389] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 476.

[390] *Ibid*., *477*.

[391] *Ibid*., 476.

[392] Stephen Herzog, 2011, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 51.

[393] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 476.

"…sowed panic and confusion among the Georgian civilian population because it was unable to communicate with its government."[394] The Russian cyber strategy against the population appeared to be to disrupt, blind and create fear and confusion.

c. Infrastructure – Clarke and Knake noted the complexity and sophistication of the cyber attacks being waged against Estonian infrastructure in 2007. The specificity of targets made them surmise that this was not some amateur hacker attack. The attack was well organized and elaborate, targeting obscure yet specific webpages such as "….the addresses of servers running parts of the telephone network, the credit-card verification system, and the Internet directory."[395] Herzog notes that "…Estonia relies on the Internet for its critical infrastructure; electronic networks are integral to the functioning of government operations, electric power grids, banking services, and even Tallinn's water supply."[396] Further, the Estonian government has adopted a model known as "…paperless government…,"[397] and is dependent on access to the internet. By attacking the websites that they did, the Russian cyber strategy effectively shut down "…the websites of all government ministries, two major banks, and several political parties. At one point, hackers even

---

[394] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 477.

[395] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 15.

[396] Stephen Herzog, 2011, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 51.

[397] *Ibid*.

disabled the parliamentary email server."[398] The Russian cyber strategy against vital infrastructure appears to have been to shut down key infrastructure needed for the government to govern, and the society to function effectively.

d. System Essentials – by launching cyber attacks against financial websites, Russia directly affected a system essential – money - in a society where "…97 percent of bank transactions occur online…"[399] Herzog notes that the attacks "…prevented credit card and automatic teller machine transactions from occurring for several days."[400] The Russian cyber strategy against system essentials seems to be to target digital transfers of money, in a highly wired and connected country.

e. Leadership – During the 2007 cyber attacks against Estonia, repeated attacks "…crashed Estonia's Internet system, leaving the government—including the president, parliament, police, and military—unable to communicate."[401] This had a direct impact on the ability of Estonian leadership, at all levels, to lead or govern. By conducting similar attacks against Georgia one year later, with similar effect, the Russians again shut down government and military networks and websites.[402] Chayes notes that in addition to this impacting the Georgian leadership's ability to lead and govern, "…the attackers sowed panic

---

[398] Stephen Herzog, 2011, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 51.

[399] *Ibid*.

[400] *Ibid*., 52.

[401] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 476.

[402] *Ibid*., 477.

and confusion among the Georgian civilian population because it was unable to communicate with its government."[403] As a result of this significant cyber attack, Russian hackers took control of the (Georgian) .ge web domain,[404] Georgia was cut-off from the global banking network (including credit card transactions),[405] and had to transfer the Georgian President's webpage to a site in the United States.[406] The cyber strategy adopted by the Russians against the Georgian leadership appears to be to deny them access to the internet, and separate the leadership from the people in order to stoke fear and uncertainty.

WARDEN AND APPLEGATE'S POSITIONAL MANEUVER STRATEGY[407]

This targeting model would be similar to the cyber strategy adopted by the Israelis against Syria. The attacker would infiltrate the defender's cyber systems, and would compromise them in order to support a kinetic attack. In this case, Warden's template[408] would still be used, however it would be against "…key physical or logical nodes in the information environment which can then be leveraged during follow-on operations."[409] Warden's theory would then be applied against these nodes, which could "…be viewed as

---

[403] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 477.

[404] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 19.

[405] *Ibid*., 20.

[406] *Ibid*., 19.

[407] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8.

[408] Colonel John A. Warden III, "Air theory for the twenty-first century," in *Battlefield of the Future: 21st Century Warfare Issues*, ed. Barry R. Schneider and Lawrence E Grinter. (Air University Press No. 3, 1995), 108.

[409] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8.

centers of gravity in the information environment and gaining logical control of these nodes will give the attacker key advantages and leverage during the escalation of conflict…"[410] As a result, when employing positional maneuver strategy, an attacker would direct efforts against specific nodes and specific vulnerabilities within a defender's cyber systems.

SUMMARY

Has Applegate accurately defined different offensive cyber maneuver strategies, and can Warden's targeting theory be applied to these different strategies? Is there merit in incorporating cyber into a military campaign? Although a cyber attack was dismissed by General Schwarzkopf as being a reliable means of attacking Iraq's air defence network during the first Gulf War,[411] by the time the Second Gulf War erupted just over a decade later; cyber warfare capabilities, and military leaders' confidence in them, had improved considerably.[412] The first decade of the twenty-first century saw cyber warfare being used increasingly as part of overall campaign strategies. Demonstrating the flexibility of cyber warfare, it was used to effect quite different outcomes in each of the manners in which it was employed. With the STUXNET example, it was used to prevent an escalation to a larger scale kinetic conflict. With the Israeli attack against a Syrian nuclear reactor, cyber warfare was employed in a singular contained military operation. Finally, the examples of

---

[410] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8.

[411] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 9.

[412] *Ibid*.

Russian employment in Estonia and Georgia, along with the American example against the Islamic State, demonstrated how cyber warfare was being employed in major conflicts.

Three distinct maneuver strategies emerged, which closely matched Applegate's model of offensive maneuver; these were exploitive, positional and influencing maneuver. The Russian strategies against Estonia and Georgia most closely matched Applegate's definition of influencing maneuver. The American strategy against the Islamic State most closely matched Applegate's definition of exploitive maneuver. Finally, cyber warfare could be employed in a supporting role to a military operation, in a manner similar to that proposed by McGuffin and Mitchell, which Applegate himself called positional maneuver.

Warden's concentric ring theory was then applied to influencing and exploitive maneuver. Analysis of open source information pertaining to the wars against Estonia, Georgia and the Islamic State demonstrated that Warden's targeting model could be applied to offensive cyber maneuver strategies. A generic targeting model, based on Applegate's offensive cyber maneuver strategies and Warden's targeting theory will be discussed next.

CHAPTER 4 – GENERIC CYBER STRATEGY

In the last decade, Russia and the United States have conducted two completely different cyber strategies as part of larger military campaigns. Both appear to have been effective. While these strategies were described anecdotally in the previous chapter, can a generic model be extracted for each strategy? Secondly, how would cyber be employed as part of a larger military campaign? These questions will be studied in this chapter.

WARDEN APPLIED TO APPLEGATE'S EXPLOITIVE CYBER MANEUVER

For exploitive cyber maneuver, an attacker would allow an opponent to have access to the internet, and the attacker would be overt with its cyber strategy. The effect desired would be to subvert the confidence of fielded fighting forces and the population. While the exact methods are closely held, the means most likely employed to accomplish this would-be software and password hacking. With respect to Warden's theory, the generic model would be described as follows:

a. Fielded military. With this model, an attacker would conduct cyber warfare against command and control, logistics and administrative networks. The aim would be to disrupt fuel, supply, administration and pay systems in order to affect troop confidence and morale.[413] Using enemy leadership electronic accounts and addresses, an attacker would transmit spoofed orders to enemy fighters to direct

[413] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

them where an attacker would want them to go.[414] The attacker would be overt in its actions, with the result that even legitimate orders from enemy commanders would be suspect. Once the fielded fighting forces became aware that an attacker possessed this capability, they would never know if messages from their superiors were proper commands, or spoofed orders directing them to a location where enemy aircraft were waiting to attack;

b. Population. Here, an attacker would aim to disrupt the ability of enemy leadership to deliver its messages to the population. The effect desired would be to prevent enemy leadership from exerting influence over the population;[415]

c. Infrastructure. In this situation, the objective would be to attack infrastructure by conducting cyber warfare against the enemy's financial and banking networks.[416] In addition, electrical systems, water systems, internet, pipelines, transportation systems and air traffic control systems could all be attacked.[417]The effect desired would be to disrupt or shut down infrastructure, and thus paralyze the state under attack;

d. System essentials – A system essential in any state is money. The means of conducting banking and commerce are also quite easy to attack. Here, one would attack the financial and banking systems via the internet;[418] and

---

[414] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[415] *Ibid*.

[416] Mark Pomerleau, 2016, "Cyber operations come out of the shadows," DEFENSE SYSTEMS. May 5, accessed October 5, 2016, https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.

[417] Agence France-Presse, 2015, Cyber Attackers Leaving Warning 'Messages': NSA Chief, March 19, accessed November 20, 2016, http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief.

e. Leadership. In this situation, an attacker could communicate directly with mid-level leadership,[419] subverting the higher ruling authority. While spoofing leader online identities, email accounts and promulgating false orders was referred to earlier as creating an effect within the fielded fighting force, this tactic would also affect enemy leadership by subverting their authority.[420] By allowing a defender unrestricted use of the internet, an attacker could exploit poor operational security. By doing so, an attacker would determine locations of key leaders, headquarters and fighting units, and then target them with kinetic strikes.[421]

WARDEN APPLIED TO APPLEGATE'S INFLUENCING CYBER MANEUVER

For influencing cyber maneuver, an attacker would deny or disrupt an opponent on the internet. At least initially, an attacker's posture would be covert. The effect desired would be to prevent an opponent's ability to access the internet. The means most often employed to accomplish this to date has been distributed denial of service (DDOS) attacks, which involve large numbers of random computers around the world sending information to a website all at the same time. The result is that the website becomes

---

[418] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[419] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 9.

[420] David E. Sanger, 2016, "U.S. Cyberattacks Target ISIS in a New Line of Combat," The New York Times, April 24, accessed October 5, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[421] Michael Hoffman,2015, "US Air Force Targets and Destroys ISIS HQ Building Using Social Media," DEFENSETECH, June 3, accessed October 5, 2016, http://www.defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/.

overwhelmed and cannot respond to legitimate requests. With respect to Warden's theory, the generic model would be described as follows:

a. Fielded military. With this model, an attacker would disrupt or deny military command, control and communications systems, hindering the ability of leadership and fielded fighting forces to communicate with each other.[422] An attacker could also disrupt sensitive yet critical military warning and offensive technologies (such as air defence),[423] along with weapons systems, logistics and administrative systems in order to paralyze an opponent's military forces;

b. Population. Here, an attacker would conduct cyber attacks against government[424] and banking websites.[425] By shutting down these websites, the effects desired would be to disrupt and blind both the government and population, and to create fear and confusion;

c. Infrastructure. In this situation, an attacker would attack servers running the telephone network, internet and credit card verification systems.[426] Electrical systems, water systems, internet, pipelines, transportation systems and air traffic control systems could all be attacked.[427] The intent would be to shut down these systems, paralyzing the state;

---

[422] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 476.

[423] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 6.

[424] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 477.

[425] Stephen Herzog, 2011, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 51.

[426] Richard A. Clarke and Robert Knake, 2010, *Cyber War: The Next Threat to National Security and What to Do About It?*, Toronto: HarperCollins, Kindle Edition, 19-20.

d. System essentials. As with exploitive cyber maneuver, a system essential in any state is money. Here, an attacker would attack the banking and financial systems, depriving the state and society of being able to access and transfer money online;[428] and

e. Leadership. Here, an attacker would conduct cyber attacks against government websites, preventing leadership from being able to communicate with the population, government services and the military.[429]As with the model for population above, by shutting down these websites, the effects desired would be to disrupt and blind both government and the population, and to create fear and confusion. The government would simply not be able to communicate its messages to the population.

WARDEN APPLIED TO APPLEGATE'S POSITIONAL CYBER MANEUVER

For positional cyber maneuver, an attacker would allow an opponent to access the internet. An attacker's posture would be covert, in order to not alert an opponent as to what they are doing. When employing positional maneuver strategy, an attacker would direct efforts against specific nodes and specific vulnerabilities within a defender's cyber systems.[430] The effect desired would be to access command and control systems, weapons

---

[427] Agence France-Presse, 2015, Cyber Attackers Leaving Warning 'Messages': NSA Chief. March 19, accessed November 20, 2016, http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief.

[428] Stephen Herzog, 2011, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4 (2), 52.

[429] Antonia Chayes, 2015, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6, http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf, 476.

[430] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations." *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 8.

systems, and critical sensors, and allow an attacker to have the equipment perform in a manner desired by the attacker. The means most often employed to accomplish this would be via cyber hacking.

COMPARISON WITH OTHER MODELS

The generic models developed to describe Warden's theory applied to Applegate's offensive cyber maneuver strategies will now be compared and contrasted to other applications of Warden's theory to different systems. These comparisons can be found in Table 4.1.

Table 4.1 – Comparison With Other Models

WARDEN'S RINGS	WARDEN		HAZDRA	OFFENSIVE CYBER MANEUVER	
	Warden's Model Applied to a State[431]	**Warden's Model Applied to a Drug Cartel**[432]	**Hazdra's Application of Warden to Al Qaeda**[433]	**Warden's Model Applied to Exploitive Cyber Maneuver**	**Warden's Model Applied to Influencing Maneuver**
Leadership	"Government: **Communication** Security	"**Leader**: **Communication** Security	**Leadership:** **bin Laden** **Al-Zawahiri** **Communication** Alliances	Impersonate leadership online **Communicate false messages** **Communicate with mid-level leaders and influence** **Exploit poor OPSEC, target leadership kinetically**	**Communication** **Government websites**
System Essentials	Energy: Electricity Oil Food **Money**	Coca source plus conversion	"**Money** Weapons False Documents Sanctuaries"	**Money** via banking system	**Money** **Banking** **Money transfer**
Infrastructure	**Roads** **Airfields** Factories	**Roads** **Airways** Sea Lanes	"**Transportation infrastructure** of host states" "Al Qaeda Companies and Businesses" "Al Qaeda Terrorist Training Camps"	Banking Finance Electricity Water Internet **Transportation** **Air Traffic** Control	Electrical Water Internet Pipelines **Transportation** **Air Traffic Control** Telephone Internet Credit Card
Civilian Population	**People**	Growers Distributors Processors	**Muslim World**	**Government communications with population**	**Government communications with population**
Fielded Military	**Military** Police Firemen"	**Street Soldiers**"	" **recruits and Al Qaeda's networked terrorist cells**"	**Fielded Military**: Command, control networks Logistics networks Administrative networks Spoof leadership orders	Communication Sensors Weapons systems

[431] Warden III, John A. 1995, "Air theory for the twenty-first century," edited by Barry R. Schneider and Lawrence E Grinter, *Battlefield of the Future: 21st Century Warfare Issues* (Air University Press) No. 3, 107.

[432] *Ibid*.

[433] Lieutenant-Colonel Richard J. Hazdra, 2006, Al Qaeda as a System, Research Project, Carlisle Barracks, Carlisle, PA: U.S. Army War College, 1 - 24.

Sources: Colonel John A. Warden III, "Air theory for the twenty-first century", 107; Lieutenant-Colonel Richard J. Hazdra, "Al Qaeda as System", 16; David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat;" Mark Pomerleau, "Cyber operations come out of the shadows;" Agence France-Presse, Cyber Attackers Leaving Warning 'Messages': NSA Chief.; Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It?; Michael Hoffman, 2015, "US Air Force Targets and Destroys ISIS HQ Building Using Social Media; " Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks;" Stephen Herzog, 2011 "Revisiting the Estonian cyber attacks: Digital threats and multinational responses;" Scott D. Applegate, "The Principle of Maneuver in Cyber Operations."

Similarities between systems have been highlighted in bold in table 4.1. Based on these highlighted similarities, it is assessed that there are numerous commonalities between the proposed application of Warden to Applegate's Offensive Cyber Maneuver Strategies, two models proposed by Warden against a state and a drug cartel, and a model proposed by Hazdra against the Al Qaeda terrorist network.

CYBER WARFARE AS PART OF A LARGER MILITARY CAMPAIGN

When building the operational design for a campaign, Bonner outlined where cyber would fit into the overall plan. Since World War I, achieving air superiority at the

beginning of a campaign quickly became a necessity.[434] Achieving air superiority at the beginning provided attacking forces with "…the ability to exploit airpower for reconnaissance, mobility, and attack without prohibitive enemy interference."[435] Once air superiority was achieved, it would then support the ground war through air interdiction, which "…destroys or interrupts those elements of an enemy's system of supply or communication for a sufficient time that the degradation will immediately or in due course prove fatal to his continuance of effective operations."[436]Because of this, achievement of air superiority has always been towards the beginning of a campaign's operational design.

Shakarian notes that Russia preceded its military campaign against Georgia by launching a cyber attack.[437] This attack "…targeted Georgian news and government websites…,"[438] with the result that the population was blinded and confused and the government lost its ability to communicate with the people. Similarly, Bonner states that when developing the operational design for a campaign, planners "…should have as their priority the attainment and maintenance of cyber superiority…"[439] Once achieved, cyber would then play a supporting role similar to what airpower plays once air superiority is achieved (in this case, supporting the ground war). Bonner states that once cyber superiority is achieved, it would then support "…kinetic operations with a

---

[434] E. Lincoln Bonner, 2014, "Cyber Power in 21st Century Joint Warfare," *Joint Force Quarterly* 74 (3rd Quarter), 103.

[435] *Ibid*.

[436] *Ibid*.

[437] Paolo Shakarian, 2011, "The 2008 Russian cyber campaign against Georgia," *Military Review* 91 (6), 63.

[438] *Ibid*.

[439] E. Lincoln Bonner, 2014, "Cyber Power in 21st Century Joint Warfare," *Joint Force Quarterly* 74 (3rd Quarter), 109.

focus on supporting the air campaign."[440]

SUMMARY

Applegate has accurately described three different strategies that can be employed when waging offensive cyber warfare. Warden's targeting model can be applied to each of these, and generic targeting models for cyber warfare can be developed. A generic exploitive cyber maneuver strategy would allow an opponent to continue to access the internet, and an attacker would be overt with their intentions. The effect desired would be to subvert the confidence of the fielded fighting forces and population in their government. While the means to accomplish this are clandestine, malicious software and password hacking would be the most likely means of conducting this form of cyber warfare. The fielded fighting forces and population would be affected by disrupting command, control and logistics networks. With respect to infrastructure and system essentials, the attacker would disrupt financial and banking networks (with money being a system essential). In addition, with respect to infrastructure, electrical, water, internet, pipeline, transport and air traffic control systems could all be targeted, with the intent of paralyzing the state.

For influencing cyber maneuver, the attacker would deny or disrupt an opponent's access to the internet. The attacker's posture would be covert (at least initially), with the effect desired being to prevent an opponent from accessing the internet. Up to this point in time, the means most often employed to accomplish this has been a distributed denial

---

[440] E. Lincoln Bonner, 2014, "Cyber Power in 21st Century Joint Warfare," Joint Force Quarterly 74 (3rd Quarter), 109.

of service attack, which overwhelms a site under attack. For fielded military and the population, an attacker would focus on government and military communications sites, along with banking websites. For infrastructure, the targets would be very similar to exploitive cyber maneuver, and would involve financial and banking networks (with money being a system essential), along with electrical, water, internet, pipeline, transport and air traffic control systems. The intent would be to paralyze the state. For system essentials, the target again is money, with financial and banking websites being targeted. Finally, for leadership, government websites would be attacked, preventing the leadership from being able to lead the people.

For positional cyber maneuver, an attacker would direct efforts against software vulnerabilities within the computer systems of an opponent's command, control, weapons or sensor systems, with the intent of the attacker being able to have these systems do or display what the attacker wants. These devices would then be working for the attacker, not the defender who paid for this equipment.

When comparing Applegate's exploitive and influencing maneuver against how Warden applied his model to a state and a drug cartel; and against how Hazdra applied Warden's model to Al Qaeda, numerous similarities quickly became apparent across all five applications. One can conclude that the application of Warden's theory to each of the cyber maneuver models is consistent with other applications of his model.

Finally, a paradigm shift was noted in campaign operational design. While the achievement of air superiority is still very important, it is now apparent that cyber superiority must be achieved first, and then cyber is used to aid in the achievement of air superiority. This new maxim has been seen in recent military campaigns.

CONCLUSION

Applegate has accurately described three different strategies that can be employed when waging offensive cyber warfare; exploitive, positional and influencing maneuver. The targeting model developed by Colonel John Warden can be used to analyse and attack an opponent's cyber capabilities for each of these offensive cyber maneuver strategies. An analysis of several recent military campaigns and operations demonstrate that countries have already started basing their attacks against their opponent's cyber capabilities using these models, along with incorporating cyber into the operational designs of their overall military campaigns.

Warden's targeting model is flexible and versatile enough such that it can be applied to cyber. While Clausewitz was critical of those who sought to map out models for conducting warfare,[441] the targeting model proposed by Colonel John A. Warden III has been employed in several conflicts since it was first employed during the Gulf War. In addition to being applied in traditional conflicts, it has also been applied against terrorist organizations, with success, and now offensive cyber maneuver strategies as well.

While there are differences as to whether cyber constitutes being a domain akin to air, land, sea and space, its importance to individuals, states and societies warrant it being subject to targeting in a conflict. There are those who argue that cyber does not constitute being a domain, as one would consider the other, more established domains. McGuffin and Mitchell argue that cyber does not possess the characteristics of the other

---

[441] The Clausewitz Homepage, "On War – Carl von Clausewitz," last accessed 6 August 2016, http://clausewitz.com/readings/OnWar1873/BK2ch02.html#a

environmental domains.[442] Most importantly, they note that cyber does not have trained operators capable of conducting warfighting as the Army, Navy and Air Force currently have.[443]

Applegate argued that cyber was a domain.[444] Further, he applied maneuver theory to cyberspace, arguing that cyber had many of the attributes attributable to maneuver.[445] Later, he expanded this thinking further, describing both offensive and defensive cyber maneuver:[446] For offensive cyber maneuver, he described three possible strategies – exploitive, positional and influencing maneuver.[447]

Regardless if one accepts that cyber is a domain or it is not, cyber is still essential for individuals, militaries and states to conduct their day to day activities. Cyber is interwoven into our lives, our militaries and into society, and is an ever-expanding realm of human activity. These essential, interwoven characteristics of cyber are what warrant it being targeted by militaries in a conflict. Attacking cyber capabilities is a natural extension of warfare. Recent examples in Georgia and Estonia have demonstrated that when cyber has been incorporated into the operational design of a larger military campaign, the result is paralysis within the country being attacked.

Although a cyber attack was dismissed by General Schwarzkopf as being a means of attacking Iraq's air defence network during the first Gulf War, [448] by the time the

---

[442] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the practice of warfare," *International Journal* (The Authors) Vol. 69 (3) (2014), 397.

[443] *Ibid*., 404.

[444] Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," *2012 4th International Conference on Cyber Conflict (CYCON)* (Tallinn, Estonia, 2012): IEEE Commun. Soc., 2.

[445] *Ibid*., 4.

[446] *Ibid*., 7-11.

[447] *Ibid*., 7 - 9.

Second Gulf War erupted just over a decade later; cyber warfare capabilities, and military leaders' confidence in them, had improved considerably.[449] The first decade of the twenty-first century saw cyber warfare being used increasingly as part of overall campaign strategies. Demonstrating the flexibility of cyber warfare, it was used to effect quite different outcomes in each of the manners in which it was employed. With the STUXNET example, a clandestine computer code attack against equipment in an Iranian nuclear facility prevented an escalation to a larger scale kinetic conflict. When Israel attacked a Syrian nuclear reactor, cyber warfare was employed in a supporting role in a singular, contained military operation. Finally, the examples of Russian employment in Estonia and Georgia, along with the American example against the Islamic State, demonstrated how cyber warfare was being employed in major conflicts, when incorporated into the operational design of a much larger military campaign.

Three distinct maneuver strategies emerged, which closely matched Applegate's model of offensive maneuver; these were exploitive, positional and influencing maneuver. The Russian strategies against Estonia and Georgia most closely matched Applegate's definition of influencing maneuver. The American strategy against the Islamic State most closely matched Applegate's definition of exploitive maneuver. Finally, cyber warfare could be employed in a supporting role to a military operation, in a manner similar to that proposed by McGuffin and Mitchell, which Applegate himself called positional maneuver.

---

[448] Richard A. Clarke and Robert Knake, 2010, Cyber War: The Next Threat to National Security and What to Do About It?, Toronto: HarperCollins, Kindle Edition, 9.

[449] *Ibid*.

Warden's concentric ring theory was then applied to influencing, positional and exploitive maneuver. Analysis of open source information pertaining to the wars against Estonia, Georgia and the Islamic State demonstrated that Warden's targeting model could be applied to cyber warfare.

A generic exploitive cyber maneuver strategy would allow an opponent to continue to access the internet, and an attacker would be overt with its intentions. The effect desired would be to subvert the confidence of the fielded fighting forces and population in their government and military leadership. While the means to accomplish this are clandestine, malicious software and password hacking would be the most likely means of conducting this form of cyber warfare. The fielded fighting forces and population would be affected by disrupting command, control and logistics networks. With respect to infrastructure and system essentials, the attacker would disrupt financial and banking networks (with money being a system essential). In addition, with respect to infrastructure, electrical, water, internet, pipeline, transport and air traffic control systems, these could all be targeted, with the intent of paralyzing the state.

For influencing cyber maneuver, the attacker would deny or disrupt an opponent's access to the internet. The attacker's posture would be covert (at least initially), with the effect desired being to prevent an opponent from accessing the internet. Up to this point in time, the means most often employed to accomplish this has been a distributed denial of service attack, which overwhelms a website. For fielded military and the population, an attacker would focus on government and military communications sites, along with banking websites. For infrastructure, the targets would be very similar to exploitive cyber maneuver, and would involve financial and banking networks (with money being a

system essential), along with electrical, water, internet, pipeline, transport and air traffic control systems. The intent would be to paralyze the state. For system essentials, the target again is money, with financial and banking websites being targeted. Finally, for leadership, government websites would be attacked, preventing the leadership from being able to lead the people.

For positional cyber maneuver, an attacker would direct efforts against software vulnerabilities within the computer systems of an opponent's command, control, weapons or sensor systems, with the intent of the attacker being able to have these systems act or display in a manner desired by the attacker. These devices would then be working for the attacker, not the defender who is relying on this equipment.

When analysing exploitive and influencing maneuver against how Warden applied his model to a state and a drug cartel; and against how Hazdra applied Warden's model to Al Qaeda, numerous similarities quickly became apparent across all five applications. One can conclude that the applications of Warden's theory to each of the cyber maneuver models are consistent with other applications of his model.

Finally, a paradigm shift was noted in campaign operational design. While the achievement of air superiority is still very important, it is now apparent that cyber superiority must be achieved first, and then cyber is used to aid in the achievement of air superiority. This new maxim has been seen in recent military campaigns.

Thus, Applegate has accurately described three different strategies that can be employed when waging offensive cyber warfare, and that the targeting model developed

by Colonel John Warden can be used to analyse and attack an opponent's cyber capabilities.

BIBLIOGRAPHY

Agence France-Presse. 2015. *Cyber Attackers Leaving Warning 'Messages': NSA Chief.* 19 March. Accessed November 20, 2016. http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief.

Applegate, Scott D. 2012. "The Principle of Maneuver in Cyber Operations." *2012 4th International Conference on Cyber Conflict (CYCON).* Tallinn, Estonia: IEEE Commun. Soc. 1 - 13.

Arthur, Charles. 2014. "Taking down ISIS material from Twitter or YouTube not as clear cut as it seems." *The Guardian.* 23 June. Accessed October 5, 2016. https://www.theguardian.com/world/2014/jun/23/taking-down-isis-youtube-twitter-google-video.

Arwood, Sam, Robert F. Mills, and Richard A. Raines. 2010. "Operational Art and Targeting Strategy for Cyberspace Operations." *IOSphere* (Spring): 30-36.

Arwood, Sam, Robert Mills, and Richard Raines. 2010. "Operational art and Strategy in Cyberspace." *International Conference on Information Warfare and Security* (Academic Conferences International Limited) 16 - 22.

Associated Press at the United Nations. 2015. *United Nations adopts plan to attack Islamic State's funding.* 17 December. Accessed October 9, 2016. https://www.theguardian.com/world/2015/dec/17/united-nations-plan-islamic-state-funding-terrorist-group-al-qaida.

Bartholomees Jr., J. Boone. 2010. "The issue of attrition." *Parameters* 40 (1): 5 - 19.

Biddle, Stephen. 2002. *Afghanistan and the Future of Warfare: Implications for Army and Defense Policy.* Monograph, Carlisle, PA: Strategic Studies Institute.

Biddle, Tami Davis. 2012. The Airplane and Warfare: Theory and History. In *U.S. Army War College Guide to National Security Issues*, *Volume I: Theory of War and Strategy*, edited by J. Boone Bartholomees, Jr., 273 - 294. Carlisle Barracks, PA: Strategic Studies Institute.

Bonner, E. Lincoln. 2014. "Cyber Power in 21st Century Joint Warfare." *Joint Force Quarterly* 74 (3rd Quarter): 102 - 109.

Boyd, John R. 13 March 2006. "Boyd's OODA Loop." *Slideshare.net.* Accessed August 6, 2016. http://www.slideshare.net/Mewthom/boyds-ooda-loop.

—. December 1986. "Patterns of Conflict." *Air Power Australia.* Accessed August 6, 2016. http://ausairpower.net/APA-Boyd-Papers.html.

Bryant, William D. 2013. *Cyberspace superiority: a conceptual model.* Maxwell AFB: Air University.

Canada. Department of National Defence. 2008. *B-GL-300-001/FP-001 Land Operations (English).* Edited by Director of Army Doctrine. Ottawa: Chief of Land Staff.

Chappel, Jr., George G. . 2002. *A Terrorist Organization as a System: Unleashing Warden's Five Ring Model.* Final Report, Joint Military Operations Department, Naval War College, Newport, R.I.: Naval War College, 1 - 26.

Chayes, Antonia. 2015. "Rethinking Warfare: The Ambiguity of Cyber Attacks ." *Harvard National Security Journal* 6: 474 - 519. http://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf.

Chen, Thomas M. 2010. "Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]." *IEEE Network* 24 (6): 2-3.

Clarke, Richard A., and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It?* Toronto: HarperCollins. Kindle Edition.

Clausewitz, Carl von. 1832. *On War.* Translated by Howard/Paret. Berlin. http://clausewitz.com/readings/OnWar1873/TOC.htm#TOC.

De Jomini, Baron Antoine Henri. 1862. *The Art of War.* 1910. Edited by Andrew McNab. Translated by Captain G.H. Mendell and Lieutenant W.P. Craighill. Apostrophe Books Ltd, Kindle Edition.

Delbrück, Hans. 1975, English language edition published 1985. *History of the Art of War Within the Framework of Political History.* Translated by Walter J. Renfroe, Jr. Vol. IV. Westport: Greenwood Press.

Department of Homeland Security Press Office. 2016. *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security.* 7 October. Accessed October 8, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Director, Joint Staff. 2013. *Joint Publication 3-12 (R) Cyberspace Operations.* Washington: Joint Chiefs of Staff.

Distelzweig, Kurt. 2014. *Operations Odyssey Dawn and Unified Protector: Another Win for Warden's Theory.* Monograph, School of Advanced Military Studies, Army Command and General Staff College, Fort Leavenworth, Kansas: Army Command and General Staff College.

Dodge, Toby. 2005. "Iraqi Transitions: from regime change to state collapse." *Third World Quarterly* (Taylor and Francis, Ltd.) 26 (4-5): 705-721.

Echevarria II, Antulio J. 2007. *Clausewitz and Contemporary War.* Kindle Edition. Oxford University Press.

Fadok, David S. 1995. *Air Power's Quest for Strategic Paralysis.* Thesis, Faculty of the School of Advanced Air Power Studies , Maxwell Air Force Base, Alabama: Air University Press, 1 - 59.

Gat, Azar. 1989. *The Origins of Military Thought From the Enlightenment to Clausewitz.* New York: Oxford University Press.

Gordon, Michael R., and General Bernard E. Trainor. 1995. *The generals' war: the inside story of the conflict in the Gulf.* Toronto: Little, Brown and Company.

Grant, Rebecca. 1999. "Airpower Made it Work." *Air Force Magazine* 30 - 37. http://www.airforcemag.com/MagazineArchive/Documents/1999/November%201999/1199airpower.pdf.

Hanson, Victor Davis. 2004. "The western way of war." *Australian Army Journal* 2 (no. 1): 157 - 164.

Hazdra, Lieutenant-Colonel Richard J. 2006. *Al Qaeda as a System.* Research Project, Carlisle Barracks, Carlisle, PA: U.S. Army War College, 1 - 24.

Herzog, Stephen. 2011. "Revisiting the Estonian cyber attacks: Digital threats and multinational responses." *Journal of Strategic Security* 4 (2): 49-60.

Hoffman, Michael. 2015. "US Air Force Targets and Destroys ISIS HQ Building Using Social Media." *DEFENSETECH.* 3 June. Accessed October 5, 2016. http://www.defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/.

International Telecommunication Union. n.d. "ITU Terms and Definitions." *International Telecommunication Union.* Accessed August 11, 2016. http://www.itu.int/net/ITU-R/asp/terminology-definition.asp?lang=en&rlink={3E2AC1A2-9D18-4235-80B6-7946B3266788}.

Johnston, Patrick B. 5 March 2016. *The Islamic State's Money Problems.* The Rand Blog, The Rand Corporation. Accessed August 4, 2016. http://www.rand.org/blog/2016/03/the-islamic-states-money-problems.html?utm_source=t.co&utm_medium=rand_social.

Keaney, Thomas A., and Eliot A. Cohen. 1993. *Gulf War Air Power Survey Summary Report.* Summary Report, Washington, D.C.: US Government Printing Office, 1 - 276.

Kober, Avi. 2007. “Targeted killing during the second intifada: The quest for effectiveness.” *Journal of Conflict Studies* 27 (no. 1). https://journals.lib.unb.ca/index.php/JCS/article/viewArticle/8292/9353.

Kuehl, Daniel T. 2009. “From cyberspace to cyberpower: Defining the problem.” *Cyberpower and national security* 1 - 17. http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf.

Lambeth, Benjamin S. 2001. *NATO's Air War for Kosovo: A Strategic and Operational Assessment.* Arlington, VA: Rand Corporation.

Lesaca, Javier. 2015. “Fight against ISIS reveals power of social media.” *The Brookings Institution.* 19 November. Accessed October 5, 2016. https://www.brookings.edu/blog/techtank/2015/11/19/fight-against-isis-reveals-power-of-social-media/.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22 (3): 365-404.

McGuffin, Chris, and Paul Mitchell. 2014. “On Domains: Cyber and the practice of warfare.” *International Journal* (The Authors) Vol. 69 (3): 394-412.

McGuffin, Lieutenant-Colonel W. C. 2013. “Soldiers of Fortran: Militarization of the 5th Dimension.” Masters of Defence Studies Thesis, Canadian Forces College, Toronto, 1 - 93.

Meyer, Josh. 2016. *Russia Hack of U.S. Politics Bigger Than Disclosed, Includes GOP.* 8 October. Accessed October 10, 2016. http://www.nbcnews.com/news/us-news/russia-hack-u-s-politics-bigger-disclosed-includes-gop-n661866.

National Public Radio Staff. 29 June 2016. *U.S. Envoy: "We're Taking Out" About 1 ISIS Leader Every 3 Days.* National Public Radio. Accessed August 4, 2016. http://www.npr.org/2016/06/29/484058317/u-s-envoy-were-taking-out-about-1-isis-leader-every-3-days.

NATO Review Magazine. n.d. *Cyber conflicts in pictures.* Accessed August 14, 2016. http://www.nato.int/docu/review/2013/cyber/photostory-cyber/EN/index.htm.

—. n.d. *Cyber Timeline.* Accessed August 14, 2016. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

North Atlantic Treaty Organization. 2011. *AJP-3 - Allied Joint Doctrine for the Conduct of Operations.* Joint Doctrine Branch.

North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. n.d. “Cyber Definitions.” *NATO Cooperative Cyber Defence Centre of Excellence.* Accessed August 11, 2016. https://ccdcoe.org/cyber-definitions.html.

—. 2012. *National Cyber Security Framework Manual.* Edited by Alexander Klimburg. Tallinn: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence.

Pape, Robert A. Winter 1997/98. "The Limits of Precision-Guided Air Power." *Security Studies* 7 (no. 2): 93-114.

Pomerleau, Mark. 2016. "Cyber operations come out of the shadows." *DEFENSE SYSTEMS.* 5 May. Accessed October 5, 2016. https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.

Sanger, David E. 2016. "U.S. Cyberattacks Target ISIS in a New Line of Combat." *The New York Times.* 24 April. Accessed October 5, 2016. http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

—. 2009. *U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site.* 10 January. Accessed November 20, 2016. http://www.nytimes.com/2009/01/11/washington/11iran.html.

Schmitt, Eric. 2016. *U.S. Says Its Strikes Are Hitting More Significant ISIS Targets.* 25 May. Accessed October 10, 2016. http://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?_r=0.

Schwartzkopf, H. Norman. 1993. *It Doesn't Take a Hero: The Autobiography of General H. Norman Schwartzkopf.* New York: Bantam Books.

Shakarian, Paulo. 2011. "Stuxnet: Cyberwar Revolution in Military Affairs." *Small Wars Journal* (United States Military Academy) 1 - 10. smallwarsjournal.com.

Shakarian, Paulo. 2011. "The 2008 Russian cyber campaign against Georgia." *Military Review* 91 (6): 63 - 68.

Starr, Barbara, and Laura Smith-Spark. 2015. *Abu Sayyaf, key ISIS figure in Syria, killed in U.S. raid.* 17 May. Accessed October 9, 2016. http://www.cnn.com/2015/05/16/middleeast/syria-isis-us-raid/.

Strategic Studies Institute. 2012. *John Warden's Five Ring Model and the Indirect Approach to War.* Vol. I: Theory of War and Strategy, in *U.S. Army War College Guide to National Security Issues*, edited by J. Boone Bartholomees, Jr., 295 - 307. Carlisle, PA: Strategic Studies Institute.

Talbot, Brent J. 2011. "Stuxnet and After." *Journal of International Security Affairs* Fall/Winter - Number 21: 69-78.

Turkel, Dan. 2016. *The US military has a new plan to fight ISIS — and it starts with making the group 'extremely paranoid'.* 26 April. Accessed August 14, 2016. http://www.businessinsider.com/new-us-cyber-war-against-isis-2016-4.

Tzu, Sun. 2015. *The Art of War, The Original Authoritative Edition.* Kindle Edition. Edited by Lionel Giles. Translated by Lionel Giles. Sweden: Chiron Academic Press.

United States. Center of Military History, United States Army. 2010. *War in the Persian Gulf - Operations Desert Shield and Desert Storm August 1990 - March 1991.* Washington, D.C.: Center of Military History Publication.

Warden III, John A. 1995. "Air theory for the twenty-first century." Edited by Barry R. Schneider and Lawrence E Grinter. *Battlefield of the Future: 21st Century Warfare Issues* (Air University Press) No. 3: 103 - 124.

Warden III, John A. 1992. "Employing Air Power in the Twenty-first Century." Edited by Richard H. Shultz and Robert L. Pfaltzgraff, Jr. *The Future of Air Power in the Aftermath of the Gulf War* (Air University Press) 57 - 82.

Warden, III, John A. Winter 1997/98. "Success in Modern War - A Response to Robert Pape's Bombing to Win." *Security Studies* 7 (no. 2): 172-190.

Warden, John A. 1995. "The Enemy as a System." *Airpower Journal* 9 (1). Accessed September 11, 2016. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.

Williams, Brett. 2014. *Cyberspace: What is it, where is it and who cares?* 13 March. Accessed September 25, 2016. http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/.

Wolf, John D. 1983. *The Military and Moral Implications of the Peloponnesian War.* Newport, R.I.: Naval War College.