National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SOLDIERS OF FORTRAN: MILITARIZATION OF THE 5TH DIMENSION

Lieutenant-Colonel W.C. McGuffin

JCSP 39

Master of Defence Studies

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.

PCEMI 39

Maîtrise en études de la défense

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 39 – PCEMI 39
2012 – 2013

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

SOLDIERS OF FORTRAN: MILITARIZATION OF THE 5TH DIMENSION

By Lieutenant-Colonel W.C. McGuffin
Par le lieutenant-colonel W.C. McGuffin

This paper was written by a student attending the Canadian Armed Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence

Word Count : 16 500

La présente étude a été rédigée par un stagiaire du Collège des Forces armées canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.

Compte de mots : 16 500

ABSTRACT

Cyberspace is a new and evolving realm of human interaction. What started as a remote computer access system for defense research expanded to support education, social correspondence, entertainment, commerce and crime. The focus has returned to security and defense concerns. Threats to commercial and government interests are being identified and cyberspace has been accepted as a domain of military of operations by many nations. While investments are being made to develop military cyber capabilities, there are few examples of military cyber operations from which doctrine can be distilled. In order to bridge the gap between speculation and experience, the principles related to land, sea and air forces can provide a useful reference for the cyber domain. In particular, the operational functions should apply to all domains. While the functions of Command, Sense and Shield apply to cyberspace the Sustain function does not. Critically, the applicability of the Act function is speculative and possibly comparable to a special forces capability. Cyberspace can certainly contribute to the projection of force but it does not satisfy the Clausewitzian conditions necessary for categorization as warfare. The adoption of cyberspace as a domain has more to do with marketing than doctrinal consistency with physical domains. Until some future military cyber operations are categorized as armed attacks there is insufficient cause to categorize cyberspace as a distinct domain.

CONTENTS

INTRODUCTION

Every fortnight the senior civilian and military leaders of the Department of National Defense meet as a Programme Management Board to decide the fate of key projects and initiatives. These leaders, representing the Army, Navy, Air Force and each of the other Departmental Level 1 organizations, have a keen interest in the allocation of resources. Decisions regarding the staffing of new positions are particularly contentious at a time when the Canadian Armed Forces (CAF) strength is being reduced due to budgetary limitations. [1] Nonetheless, when the PMB Chairperson, the Vice Chief of Defence Staff, raised the subject of staffing for the CAF Cyber Task Force, the board members approved the immediate allocation of 20 persons to undertake the new assignments.[2] These people and the additional 20 planned to join them in 2013 will have to be exceptionally motivated, technically proficient and well-supported to deliver the advice, education and doctrine required for the CAF.

A similar decision was made one hundred years ago when Canada's Minister of Militia and Defence ordered the creation of the Canadian Aviation Corps.[3] As early as 1907, in a work of science fiction, H.G. Wells described the German rise of air power and

[1] Budgetary reductions in Fiscal Year 2012 imposed a cap of 68,000 Regular Force members and a reduction in Reserve Force contracts. New capabilities like the C-17, Chinook Helicopters and Cyber Task Force create additional demand for personnel without offering trade-offs. See http://www.forces.gc.ca/site/pri/first-premier/defstra/rebuild-rebatir-eng.asp, http://news.nationalpost.com/2011/10/24/canada-to-freeze-size-of-regular-forces-shut-down-facilities/, and http://www.vcds-vcemd.forces.gc.ca/cres-cdts/fc-cc/index-eng.asp, all accessed on 25 January 2013.

[2] A.B. Donaldson, “Memorandum to PMB – Immediate Surge Requirements in Support of CF Cyber Force,” 1150-110/P15 (Cyber TF), February 2012.

[3] Canadian Wings, “The History of Canada’s Air Force,” accessed on 13 January 2013, http://www.canadianwings.com/history/beginning.php.

that they “may seize the air—as once the British seized the seas.”[4] Two years later, Giulio Douhet, an Italian staff officer predicted that “the sky would become another battlefield no less important than the battlefields on land and sea.”[5] At the start of World War 1 and only five years after the first controlled powered flight in Canada, the initial attempt to create a national air force experienced numerous challenges.[6] Nonetheless, Canada eventually contributed flight training, pilots and two squadrons of aircraft to the allied war effort. It was not until World War 2 that the employment of military aviation would reach a sufficient level of maturity for commanders to capitalize on the capabilities delivered by air power. Douhet, who would rise to command Italy’s Air Force at the end of the World War 1, published “The Command of the Air” in 1921. This early treatise on air power presented the case for a separate and distinct military service. Douhet’s writing was a welcomed foundation to air power theory but it also contained some exaggerations. As he noted: “Nothing man can do on the surface of the earth can interfere with a plane in flight, moving freely in the third dimension.”[7] The influence of ground based air defence systems and stinger missiles on aircraft are reminders that it is unwise to be so definite when making predictions about new technology. [8] The statements made by military

[4] Herbert George Wells, *The War in the Air*, Project Gutenberg EBook #780, August 10, 2008, Chap 4.

[5] Dan McCaffery, *Battlefields in the Air: Canadians in the Allied Bomber Command* (Toronto: Lorimer, 1995), 3. Also note that H.G. Wells published *The War in the Air* in 1908 which prophesized the use of aircraft in war fighting.

[6] Royal Canadian Air Force, “Air Force History,” accessed on 13 January 2013, http://www.rcaf-arc.forces.gc.ca/v2/hst/page-eng.asp?id=526.

[7] Giulio Douhet translated by Dino Ferrari, *The Command of the Air* (Washington: Air Force History and Museums Program, 1998), 10.

[8] P. W. Singer, *Wired for War* (New York: The Penguin Press, 2009), 9.

theorists addressing new capabilities may be influenced by partisan perspectives or the fear that overestimations are required in order to be acknowledged.[9]

The Internet has matured considerably since the first packet-switching networks of the 1960s.[10] Standardization of the TCP/IP network interconnection protocol and the affordability of personal computers in the 1980s initiated a growth that would expand rapidly with the distribution of commercial internet service providers in the late 1980s. In 2000 5% of the World population and 31% of North Americans made use of the internet. By 2012 there was 34% of the World and 79% of North Americans using the Internet.[11] Today, a sufficiently representational portion of our cultural exchanges occur over this electronic medium that we think of it as the artificial environment described in 1980s cyberpunk writing by William Gibson.[12] In *Neuromancer* Gibson wrote "The matrix has its roots in primitive arcade games…Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation…"[13]

Of course, there are many forms of social exchange, licit and illicit. It is therefore not surprising that early technophiles wanted to do more than the messaging and file exchanges permitted by Bulletin Board Services in the 1980s. By the 1990s, marketing, commerce, sex services and crime began to thrive. Robert O'Connell suggests a pattern for the evolution of human social interaction in *Tide of the Second Horseman: The Birth*

[9] Nate Silver, *The Signal and the Noise: Why So Many Predictions Fail-but Some Don't,* Penguin Press e-pub, 2012, Intro, 24/32.

[10] Barry M. Liner *et al*., "Brief History of the Internet," accessed on 13 January 2013, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

[11] Internet World Stats, "World Internet Usage and Population Statistics," June 30, 2012 accessed on 25 January 2013, http://www.internetworldstats.com/stats.htm.

[12] William Gibson first described cyberspace in Burning Chrome (1982). Fiction author Jack Womack suggested that these writings shaped the development of the Internet. See the afterword in the 2000 re-issue of *Neuromancer*.

[13] William Gibson Neuromancer Ace Books, Jan 2010, 91/720.

and Death of War. As people accumulated in early Sumerian times, O'Connell describes an environment rich in social interaction that naturally led to culture, politics and conflict.[14] This same evolution can be observed in the Internet's history. Today, there appear to be more opportunities for military activity in this artificial environment than originally envisioned by its creators within the Advanced Research Projects Agency of the United States Department of Defense.[15]

The wired nations of the western World are just beginning to rationalize the scope and nature of the powers that threaten their sovereignty in the virtual World. On 7 April 2007, Estonia suffered a distributed denial of service (DDoS) attack that paralyzed many of its public and national internet based services for two weeks.[16] This example, popularly referred to as "Web War 1"[17] was followed by attacks on Georgia in 2008, Iran in 2009 and Burma in 2010.[18] The North Atlantic Treaty Organization (NATO) established the NATO Cooperative Cyber Defence Centre of Excellence in May 2008 to enhance cyber defence capabilities within the Organization.[19] Individual NATO members also began establishing their own expertise to develop national capabilities. Notably, the US Cyber Command declared initial operational capability in

[14] Robert O'Connell, *Tide of the Second Horseman: The Birth and Death of War* (Oxford: Oxford University Press, 1995), 93.

[15] Barry M. Liner et al., "Brief History of the Internet…

[16] Mark Lander and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," New York Times, Last Accessed on 19 December 2012, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0.

[17] Matt Murphy, "War in the fifth domain," The Economist, Last Accessed on 19 December 2012, http://www.economist.com/node/16478792.

[18] Jim Giles, "Are States Unleashing the Dogs of War," NewScientist, 16 December 2010, accessed on 13 January 2013, http://www.newscientist.com/article/mg20827915.100-are-states-unleashing-the-dogs-of-cyber-war.html.

[19] NATO, Cooperative Cyber Defence Centre of Excellence, "The Tallinn Manual." Last accessed on 19 December 2012, http://www.ccdcoe.org/249.html.

May 2010[20] and the existence of a Cyber Centre in the People's Liberation Army of China was reported in July 2010.[21]

The Canadian response to cyber threats is articulated in general terms in the 2010 Canada Cyber Security Strategy. Direction to the Department of National Defence is to collaborate with other federal entities and partner with allies.[22] In actuality the CAF have been operating in cyberspace for as long as that nomenclature has existed. The Defence Wide Area Network (DWAN), classified and environmental networks, even the issued Blackberry devices constantly give us access to what people think of as cyberspace. Given that these established systems are already maintained and defended by network administrators, what changes are called for to address the militarization of cyberspace?

The ubiquity of cyberspace and the reach it has in the conduct of our personal and professional activities demands that we give careful consideration to the methods used to assure its availability for Canadian use. An important portion of the Canadian Gross Domestic Product depends on or is attributable to Internet access and e-commerce was called a "priority policy area for the Government of Canada" by David Sweet, Chair of the Standing Committee on Industry, Science and Technology.[23] The warnings being articulated by Richard Clarke and Robert Knake in their book *Cyber War: The Next*

[20] United States Strategic Command, "U.S. Cyber Command," accessed on 13 January 2013, http://www.stratcom.mil/factsheets/Cyber_Command/.

[21] Times of India, "PLA sets up cyber base, assures it's not for war," 23 July 2010 accessed on 13 January 2013, http://articles.timesofindia.indiatimes.com/2010-07-23/china/28321900_1_cyber-war-cyber-security-base.

[22] Government of Canada *Canada's Cyber Security Strategy* (Ottawa: Her Magesty the Queen in Right of Canada, 2010), 10.

[23] David Sweet, "E-Commerce in Canada: Pursuing the Promice," Report of the Standing Committee on Industry, Science and Technology, 41st Parliament, 1st Session, May 2012, 1.

Threat to National Security and what to do about it[24] are fueling fears similar to those that surrounded nuclear weapons during the Cold War. The results of cyber espionage may be intangible for most people. However, every Canadian with a Social Insurance Number is at some risk of identity theft.[25] Unlike the Cold War where the threat was from a bipolar clash with nuclear warheads, the new threat is from thousands of cyber criminals deploying imaginative ways to steal our financial worth. The Honourable Vic Towes, Minister of Public Safety, has compared cyber viruses and malware to antibiotic resistant bacteria and advised Canadians to update their anti-virus software.[26] While the advice is warranted it may prove as futile as the fall-out shelters that Americans were encouraged to build in their basements in the 1960s.[27]

The United Nations (UN) proposed updates to the 1988 Telecommunications treaty in December 2012.[28] This was an attempt to reach consensus regarding updates to a treaty established before the internet age. Not surprisingly there were disagreements between Western nations, emphasizing the concepts of democracy, liberalism and net neutrality and the perspective of more authoritarian regimes interested in greater government control. Canada's Minister of Industry, Christian Paradis, stated that "Our government will continue to support an open and accessible internet that facilitates

[24] Richard A. Clarke and Robert Knake *Cyber War: The Next Threat to National Security and what to do about it* (Harper Collins e-books, 2010), 273/571.

[25] Service Canada, "Your Social Insurance Number: A Shared Responsibility! Protect it! Safeguard it!" accessed on 18 April 2013, http://www.servicecanada.gc.ca/eng/sin/info/yoursin.shtml.

[26] Government of Canada *Canada's Cyber Security Strategy*…, 6.

[27] While fallout shelters may have provided some comfort to the families that had access to them, they contributed nothing to the elimination of the threat. Martin Mann, "Plain Facts about Fallout Shelters," Popular Science, December 1961, 56- 60.

[28] Associated Press, "U.S., Canada decline to sign UN telecoms treaty," accessed on 13 January 2013 http://www.cbc.ca/news/world/story/2012/12/13/un-us-internet.html.

economic development and prosperity."[29] At the far end of the open internet spectrum is the hacker group known as Anonymous calling for international recognition of Distributed Denial of Service (DDoS) Attacks as a legitimate form of protest.[30] While the Canadian position "defends the right to communicate as a basic human right"[31] the government has already established limits. For example, legislation has been announced that will make it a crime to use a computer system to sexually exploit a child.[32] While this specific censorship policy is an easy one to defend it also makes it difficult to prevent Canadian companies from selling internet censorship technology to countries that might use it to prosecute political objectors.[33] The clash of cultures is unlikely to be resolved soon.

This paper will argue that cyberspace does not possess the characteristics necessary to be categorized as a separate domain. While this new realm introduces new and distinct methods with which to apply force it falls short of the full war-fighting spectrum that can occur in land, sea, air and space conflicts. Several authors have taken to describing cyberspace as the 5th domain of operations.[34] While this writer agrees that

[29] Associated Press, "U.S., Canada decline to sign UN telecoms treaty…

[30] Jeff Goldman, "Anonymous Hackers Seek Recognition of DDoS Attacks as Legitimate Form of Protest," accessed on 13 January 2013, http://www.esecurityplanet.com/hackers/anonymous-hackers-seek-recognition-of-ddos-attacks-as-legitimate-form-of-protest.html.

[31] Brian Murphy, "Canada Joins Western Nations in Rejecting UN Internet Treaty," 14 Dec 2012, accessed on 13 January 2013, http://www.ctvnews.ca/sci-tech/canada-joins-western-nations-in-rejecting-un-internet-treaty-1.1079239.

[32] Government of Canada *Canada's Cyber Security Strategy*…, 13.

[33] Amy Dempsey, "Guelph tech firm accused of making tools to censor Internet abroad now embroiled in controversy with Australian telecom." June 28, 2012, accessed on 13 January 2013, http://www.thestar.com/news/canada/article/1218965--guelph-tech-firm-accused-of-making-tools-to-censor-internet-abroad-now-embroiled-in-controversy-with-australian-telecom.

[34] See: Matt Murphy,"War in the fifth domain," The Economist, 1 July 2010, http://www.economist.com/node/16478792 and William Lynn, "Defending a New Domain," Foreign Affairs, Last Accessed on 18 April 2013, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

cyber threats must be recognized, studied and countered, the offensive possibilities are not comparable to those that exist in established domains of operation. In Chapter 1 the nature of the domains of operation will be examined using the operational functions of Command, Sense, Act, Shield and Sustain. These operational functions provide a frame of reference or inter-service nomenclature to permit the comparison of military activities between elements. Since they apply to each of the established domains they should also apply to any new contenders. Military activity that supports the operational functions from the land, sea and air domains will first be described. Following that a comparison will be made with the space domain to verify the applicability of the evaluation criteria. Chapter 2 will dissect cyberspace and draw parallels to the recognized domains of warfare. Operational functions like Sense and Shield are readily supported in cyberspace. The Act and Sustain functions are less applicable and limit the scope of military possibilities in the cyber environment. Terminology will be presented to help describe the offensive and defensive efforts in conventional ways. Ultimately this chapter concludes that cyber warriors are more likely to support a capability resembling special forces which does not warrant the status of a domain. Chapter 3 will examine the current threats resident to cyberspace and suggest future possibilities. These threats originate from the complexity of hardware and software in information technology (IT), the market driven design and manufacturing processes and the fallibility of human decision making. However unexpected these threats may be they still echo conventional threats like targeted killings, jamming and sabotage. Cyber threats are also subject to the influence of friendly, adversary and other parties who can all exert influence in cyberspace. Cyber weapons can therefore be untimely in delivering the desired effect or be rendered obsolete without warning. Finally the ephemeral nature of cyber activity can make attribution to a specific actor or nation particularly difficult. Cyberspace is a host for new forms of social interaction including military activity. However, it falls short of the full range of military activity required for it to be considered a domain with the status of land, sea, air and space.

> *…one must be alert to different times, different outlooks, different ideas, different problems, different mind-sets, different capabilities, different decision making structures, and different technologies.. Despite the contrasts between past and present one can perceive some broad, recurring characteristics, issues and problems that arise…. From these, one can outline a broad concept…*
>
> - John B. Hattendorf, "What is Strategy"

CHAPTER 1 – THE NATURE OF A DOMAIN

Historically there have been three sufficiently compelling motivations to urge societies to expend large portions of their collective wealth. First is paying tribute to a supreme being which may take the form of a god or royalty. The Egyptian pyramids are the most obvious example of this display.[35] While less sophisticated in their construction techniques, the Rapa Nui of Easter Island expended virtually all their resources to build their monolithic tributes to ancestors. The second motivation is the quest for wealth. It is economic competition that funded the explorations of Christopher Columbus from Spain and the Dutch West (and East) Indies Company. The third motivation for large investment is war. The Chinese built the Great Wall to defend against nomadic aggressors and the Romans financed legions to defend and expand their territory.[36] The Manhattan Project of WW 2 which led to the production of the World's first four nuclear weapons cost the equivalent of 30 billion $US adjusted for 2012.[37] For comparison, In

[35] Robert L. O'Connell, *Ride of the Second Horseman, The Birth and Death of War* (New York: Oxford University Press, 1995), 91.

[36] Neil deGrasse Tyson, "The Case for Space," *Foreign Affairs*, March/April 2012, 22.

[37] The Brookings Institution, "The Costs of the Manhattan Project," accessed on 22 January 2013, http://www.brookings.edu/about/projects/archive/nucweapons/manhattan.

2010/2011, while Canada was contributing to high intensity operations in Afghanistan, $22 billion was spent on defence, roughly 8% of the total federal budget.[38]

The tremendous cost of maintaining professional military forces should compel the parent nation to be deliberate and discriminating about the capabilities that will be resourced. Decisions to acquire costly equipment like the "Land Combat Vehicles", "Canadian Surface Combatant" ships, and "Next Generation Fighters"[39] are large targets for criticism by political opponents. In order to substantiate these costly investments procurement decisions are based on doctrinal employment concepts and government defence policy. Doctrinal employment concepts provide a sound and defendable foundation for procurement decisions because they are based on national and international historical precedents.

The North Atlantic Treaty Organization (NATO) defines military doctrine as the "Fundamental principles by which the military forces guide their actions in support of objectives."[40] Doctrine is developed for each of the services, whether armies, navies or air forces. These principles are an authoritative guide to how the group thinks about fighting in their corresponding environment. The various environments have become known as "domains" in military terminology. Within these domains,[41] military capabilities are applied to observe, move, defend and strike.

[38] Department of Finance Canada, "Your Tax Dollar: 2010-2011 Fiscal Year," accessed on 25 January 2013, http://www.fin.gc.ca/tax-impot/2011/html-eng.asp.

[39] National Defence, "Projects," accessed on 26 January 2013, http://www.forces.gc.ca/site/pri/2/index-eng.asp.

[40] NATO, *AAP-6(V) NATO Glossary of Terms and Definitions* (Brussels, 2008).

[41] Unfortunately, the use of the terms environment, domain and dimension are not consistent in Canadian doctrine publications. The United States JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 15 December 2012 uses domain in the context proposed in this paper.

This chapter will demonstrate that a domain of military operations can be described by key attributes and characteristics that align with and contribute to military activities. The attributes will be distilled from the doctrine pertaining to widely accepted domains of warfare: land, sea and air. The manner in which military objectives are pursued varies with the environment in which the activity takes place. Therefore, CAF doctrine has adopted the operational functions of Command, Sense, Act, Shield and Sustain to permit the categorization of environmental activities in a manner that promotes understanding between land, sea and air personnel. It is pertinent to acknowledge the important debate regarding the nature of war in the information age advanced by David Lonsdale in *The nature of war in the information age: Clausewitzian Future.*[42] This author agrees with Lonsdale's assessment that Clausewitzian principles remain valid in contemporary warfare. In his work *On War*, Carl von Clausewitz stressed the importance of the moral and physical aspects of war. To him, war required the energetic clash of force against counterforce. However, Clausewitz also acknowledged that many other means of projecting force and influence can exist in a conflict. [43] Consistent with that belief is the necessity for domains of military operation to support the full range of military activities which will be drawn from the nature of conflict as it has evolved over time in each of the established domains. The criteria distilled from land, sea and air will then be tested using the characteristics associated with space which the US Department of Defence established as a unified combatant command in 1985.

[42] David J. Lonsdale, *The nature of war in the information age: Clausewitzian Future*. Vol. 9. (Routledge, 2004).

[43] Michael I. Handel, *Masters of War: classical strategic thought* (London: Newbury House, 2001), 35.

Canadian doctrine describes military power as the potential military capabilities possessed by a nation; a combination of conceptual, moral and physical components.[44] While the conceptual and moral aspects of military power are equally important sources of influence they will only be referred to superficially. It is the physical component, the domains[45] of operation, which will be discussed here. The domains are where the activity takes place to create effects and ultimately compel an adversary to comply with the will of the victorious state.

THE CONTINENTAL PERSPECTIVE

The original domain of military operation must be on land where early people hunted, gathered and eventually formed communities. The recorded history of land based warfare extends back to Sumerian times where conflict was sufficiently prevalent to document early deterrence theory "The state weak in armaments – The enemy will not be driven from its gates."[46] Some early principles of land warfare are evident from the ruins of ancient cities and fortifications: perimeter walls to resist enemy attack; observation towers for early warning; and elevated positions from which to fight attackers. Other principles relied on technique and skill. Speed and agility combined with proficiency as archers made the horse riding nomads of the steppe successful raiders.[47]

Land power evolved as new tactics were introduced and new technology was applied to war fighting. Spears allowed a soldier to distance himself from the reach of a

[44] Department of National Defence, B-GJ-005-000-FP-001, *Canadian Military Doctrine* (Ottawa: DND Canada: 2011), 2-3.

[45] In CAF Joint doctrine domain refers to the physical, moral and informational realms.

[46] Robert L. O'Connell, *Ride of the Second Horseman…,* 98.

[47] Erik Hildinger, *Warriors of the Steppe: A Military History of Central Asia 500 BC to 1700 AD* (Cambridge, MA: Da Capo Press, 2001), 7.

sword. Arrows could be launched beyond the reach of spears. Cavalry was faster than infantry. Rifles were more accurate and faster to shoot than muskets. Tanks offered protection and the ability to manoeuvre heavier guns.

The fundamental principles of land operations are prescribed by the nature of terrain itself. Sun Tzu wrote “The natural formation of the country is the soldier's best ally.”[48] However the opposite is also true. Terrain can be a persistent opponent to land forces even when the enemy is not present. In *Military Strategy*, J.C. Wylie explains that terrain is “the point of departure for the soldier’s concept of warfare.”[49] The land domain is comprised of geography, weather, indigenous population, infrastructure and the enemy.[50] Even with the benefits of modern clothing and equipment available to wealthy nations soldiering remains a physically demanding activity. Soldiers must apply their skills in desert heat and frigid arctic weather. Heavy loads are still the norm for troops on patrol in dust, sun or rain. Local populations, urban infrastructure and participating non-military organizations and non-conventional enemy create complex problems for soldiers to negotiate. Canadian doctrine states that land combat is “characterized by friction, uncertainty, ceaseless change, and violence…it is a fundamentally human endeavour.”[51] The proximity of the soldier to his environment and the limits of range and endurance results in a perspective on the operational environment that is different from those operating in other domains. The natural boundaries created by shores, mountains and

[48] Sun Tzu and Lionel Giles, *The Art of War* (Internet Classics Archive: 1994), Chap X, para 21

[49] J.C. Wylie, *Military Strategy: A General Theory of Power and Control* (New York: Rutgers, 1967), 50.

[50] Department of National Defence, B-GJ-300-001/FP-001, *Land Operations* (Ottawa: DND Canada: 2008), 2-2.

[51] *Ibid*., 2-17.

deserts delineate soldier's view into theatres whereas the nature of sea and air compel a much larger view from sailors and aviators.[52]

In *The Future of Power*, Joseph Nye explains that classical realists believe that war stems from human greed and the desire to dominate. Modern realists assign greater importance to the need for security. [53] Land forces exist to control the threats that may jeopardize that security. The most obvious expression of control through the application of combat power but land forces are employed in a wide spectrum of activities. This spectrum can be described as a continuum of operations where peace is at the low end and war is at the high end.[54] The activities are categorized into three broad types. Offensive operations include the attack, raid, reconnaissance, pursuit, ambush, breakout and the demonstration. Defensive operations are "to defeat or deter an adversary's offensive actions, and to hold ground".[55] Manoeuvre operations are used to gain an advantageous position and include advancing to the enemy, envelopments, and obstacle crossings. Delay operations are used to gain time, usually to permit the completion of a defensive position. Stability operations are "to establish and maintain the conditions for normal civic activity and responsible government."[56]

The previous examples of land force activities are designed to attack an adversary's cohesion, or to affect the will of the adversary and other targets. Canadian doctrine states that these are executed through three core dynamic functions: Find, Fix,

[52] J.C. Wylie, *Military Strategy…, 49.*
[53] Joseph Nye, Jr, *The Future of Power* (New York: Public Affairs, 2011), 26-27.
[54] Department of National Defence, B-GJ-300-001/FP-001, *Land Operations…,* 305.
[55] *Ibid*., 749.
[56] *Ibid*., 793.

and Strike.[57] Each of these can be categorized within one, and occasionally more, operational function.[58] For example, an infantry platoon contributes to the Act function during an attack but they contribute to Shield and Sustain when they provide protection for a logistics convoy. These functions are the frame of reference with which land, sea and air forces can compare the activities that they engage in. Maritime and air forces attack the adversary in different manners than the army does but they can all cause physical destruction which is part of the Act function. Thus, we have a doctrinally based starting point.

Each of the operational functions can be supported in the land domain. Military commanders can Command by directing activity in person and passing orders over radio, network or paper documents. [59] Information and observations are key to planning operations, locating targets and responding to adversary actions. Sentries, remote cameras and sniper teams contribute greatly to the Sense function.[60] Whenever army forces strike a target or causes an adversary to react the Act function is alive. Attacks can be fleeting if the intent is to confuse or delay the adversary and they can be decisive engagements to destroy the adversary's ability to continue fighting.[61] The Shield function protects existing force capabilities. It includes the use of protective structures, minefields, camouflage, flack vests and prophylactic medication.[62] The Sustain function includes the

[57] Department of National Defence, *B-GJ-300-001/FP-001, Land Operations…,* 419.
[58] The operational functions are Command, Sense, Act, Shied and Sustain. *Ibid.*, 4-18.
[59] Department of National Defence, B-GJ-300-001/FP-001, *Land Operations…*, 413.
[60] *Ibid*., 414.
[61] *Ibid*., 415.
[62] *Ibid*., 416.

replenishment of consumables, medical care for the wounded and replacing troops when they become fatigued.[63]

THE MARITIME PERSPECTIVE

The second domain of military operation is the maritime one. The first water craft were used for harvesting food from, and for transportation on, lakes, rivers and seas. There are 8000 year old Chinese maritime artefacts illustrating the early history of people using watercraft.[64] The Khufu ship buried at the foot of the Great Pyramid of Giza is an impressive example of ship building skill from 4500 years ago.[65] The technology of naval warfare likely evolved from the vessels used for commerce. In 500 BC, the Greeks and Persians were using ships to transport troops and supplies over the Mediterranean Sea.[66] Navy crew began defending their ships and eventually adopting offensive weapons and procedures. The Vikings were successful raiders and reached North America by ship 200 years before the Portuguese and Spanish.[67] Ship propulsion technology progressed from oar to sail to steam to oil and today the atom powers the largest military vessels.

As maritime trade contributed larger measures of a nation's wealth there was greater interest in protecting trade routes.[68] Jacob Viner made a strong case for the relationship between Naval power and national economic prosperity in the seventeenth

[63] Department of National Defence, *B-GJ-300-001/FP-001, Land Operations…,* 417.

[64] Geoffrey Till, Seapower – A Guide for the Twenty-First Century (London: Frank Cass, 2004), 9.

[65] Danee Gilmartin, "Did Pharaohs Get Seasick?: Khufu Boat Museum: Giza, Egypt," 1 March 2010, accessed on 29 January 2013, http://museumchick.com/2010/03/khufu-boat-museum-giza-egypt-felucca.html.

[66] Colin Gray, *The Leverage of Sea Power*, (New York: The Free Press, 1992), 94.

[67] Geoffrey Till, Seapower – A Guide…, 9.

[68] *Ibid*., 10.

and eighteenth centuries.[69] Navies were expanded both to defend the sources of prosperity and because of it.[70] Canadian doctrine lists four roles for the navy: sea control, sea denial, fleet in being and maritime power projection.[71] Naval historian S.W Roskill wrote that maritime strategy is not "to establish complete control of all sea communications…as to develop the ability to establish zones of maritime control wherever and whenever they may be necessary…"[72] It is pertinent to note that these roles are not viewed in isolation and sea control can be limited in scope, geography or time and still achieve the desired freedom of movement.[73] Wiley adds that maritime theory is both the "control of the sea, and the exploitation of the control of the sea toward establishment of control on the land."[74]

Notwithstanding the relative autonomy of modern war ships, able to sail for months at a time (limited only by food supply in the case of nuclear vessels), there remains a strong joint element to naval forces.[75] In his examination of sea power, Colin Gray stated that "Navies fight at sea only for the strategic effect they can secure ashore, where people live."[76] The blockade may occur on the ocean but its purpose is to isolate land from a maritime line of communication. Sparta for example, was unable to defeat Athens in land warfare due to the resources Athens accessed through maritime

[69] Jacob Viner, "Power and Plenty as Objectives of Foreign Policy in the Seventeenth and Eighteenth Centuries," World Politics, Vol. 1, no. 1, October 1948.

[70] Only wealthy nations could fund a navy and the naval force protected the international trade routes that were the source of wealth.

[71] Department of National Defence, *Securing Canada's Ocean Frontiers – Charting the Course from Leadmark* (Ottawa: DND Canada, 2005), 18.

[72] S.W. Roskill, *History of the Second World War, The War at Sea 1939-1945, vol 1: The Defensive* (London: HMSO, 1954), 3.

[73] Colin Gray, The Leverage of Sea Power…, 9.

[74] J.C. Wylie, *Military Strategy…,* 39.

[75] Colin Gray, *The Leverage of Sea Power…,* 2.

[76] *Ibid*., 1.

commerce. Athens was only defeated after Persia supplied Sparta with the resources necessary to build a powerful naval fleet.[77] Joint requirements similarly drove modern operations when the re-conquest of Europe and the Pacific islands required the merging of ships, weapons, communications and doctrine to permit amphibious operations against a defending enemy.[78]

Maritime operations on open water are vastly different than those on land. While land forces seek to maintain contact with the enemy, opposing navies will search, pursue and evade until they have opportunity to engage the adversary in advantageous conditions. Historical victories at sea were the result of superior scouting and concealing one's intentions and naval power; essentially the basis for manoeuvre warfare.[79]

When operating in littoral waters there are some similarities with continental warfare in that naval vessels must negotiate the coast and bottom terrain features.[80] Icebergs and islands can be obstacles to movement and limit radar and visual observation. Weather will degrade the performance of a ship just as they degrade land operations. However, unlike land force personnel, the navy moves, lives and fights in an environment that can ultimately consume them. The Spanish Armada sailing against England in 1588 was decimated by an unusually strong North Atlantic storm off the west coast of

[77] *Ibid*., 7.

[78] J.C. Wylie, *Military Strategy…,* 41.

[79] Wayne Hughes, "Naval Manoeuvre Warfare," Naval War College Review, Vol L, No 3, Summer 1997, 25-49.

[80] Department of National Defence, *Securing Canada's Ocean Frontiers…,* 34.

Ireland.[81] The US Navy has lost over forty ships in its history and 22 of them in the last century.[82]

Canadian doctrine describes naval operation using the dynamic functions Float, Move, and Fight.[83] Ships and submarines have three core functions when conducting sea control operations: anti-air, anti-surface and anti-submarine warfare.[84] Returning to the operational functions, Command is exercised over maritime forces and the command structure is evident from the leaders present at all rank levels. Ships and submarines are equipped with radar, sonar and optical observation systems to Sense their environment. Ships can Act by movement and by firing guns and torpedoes. They can also influence their adversary by their very existence (the fleet in being) even, or perhaps especially, if their location is unknown as is the case with submarines. Ships can Shield themselves from attack with air-defence systems, stealthy shapes and radar absorbent coatings. Ships can resupply their fuel and food for crew at port and from resupply vessels. The Sustain function can also be exercised by aircraft that ferry crew and equipment to the ships.

THE AVIATOR'S PERSPECTIVE

The air domain was used for military purposes well before the first controlled heavier than air flight in 1903. The Chinese reportedly made use of small hot-air "sky

[81] Sources claim the loss of 24 Spanish ships out of 130 up to a claim of 50% of the armada. See http://britishbattles.com/spanish-war/spanish-armada.htm. Accessed on 18 April 2013.

[82] On 4 October 1945, a typhoon claimed 22 ships and smaller vessels near Okinawa. "U.S. Navy Ships Lost in Selected Storm/Weather Related Incidents." Accessed on 18 April 2013. http://www.history.navy.mil/faqs/faq102-2.htm.

[83] Department of National Defence, *Leadmark – The Navy's Strategy 2020* (Ottawa: DND Canada, 2001), 20.

[84] Department of National Defence, *Securing Canada's Ocean Frontiers...*, 33.

lanterns" as military signals in the third century.[85] The French Corp d'Aerostiers reportedly employed lighter than air balloons for aerial observation at the battles of Charleroi and Fleurus in 1794.[86] Hydrogen balloons were used for reconnaissance and artillery spotting by both sides in the American civil war in the 1860s.

Only 10 years after the Wright brother's first flight, military aviation in World War 1 military forces was initially limited to reconnaissance. Aircraft were still predominantly experimental at the time and it was common for aviators to acknowledge each other in flight.[87] It was not long however before pilots and spotters of opposing sides began shooting at each other with their pistols. The aerial arms race progressed to mounted machine guns, dedicated gunners, then specialized fighter and bomber aircraft. The tactics, techniques and technology of air power has matured significantly over the last century. Supersonic speeds, precision guided munitions, stealth technology and unpiloted aerial vehicles (UAVs) are employed by several contemporary nations.[88]

Despite the advances in aircraft technology, several of the principles proposed by Douhet before World War 1 have survived in contemporary air power doctrine. Concepts like the deep battle and destroying adversary air forces while they are on the ground remain sound. [89] Likewise, his definition: "command of the air means to be in a position

[85] History of Sky Lantern, accessed on 5 February 2013, http://www.chineseskylantern.com/.

[86] Civil War Trust, "Civil War Ballooning," accessed on 20 April 2013, http://www.civilwar.org/education/history/civil-war-ballooning/civil-war-ballooning.html

[87] Centruy of Flight, "Aces of World War One," accessed on 8 February 2013, http://www.century-of-flight.net/new%20site/frames/WW1%20aces_frame.htm.

[88] David Axe, Real U.S. Stealth-Tech Advantage: Its Assembly Lines, 6 July 2011, Accessed on 6 February 2013, http://www.wired.com/dangerroom/2011/07/stealth-advantage/.

[89] Giulio Douhet translated by Dino Ferrari, *The Command of the Air*, (University of Alabama Press, 2009), 19.

to prevent the enemy from flying while retaining the ability to fly oneself"[90] is readily applicable to modern air forces.

Aircraft provide a platform from which to deliver valuable military capabilities but they are also finicky. Flying operations are sensitive to weather and can be limited by crew fatigue and mechanical wear. The physical platforms are fragile and dependent on infrastructure for protection from damage and for the conduct of frequent maintenance. Aircraft are capable of delivering rapid effects such as the movement of troops, bombs on targets and imagery of specific sites with little concern for surface obstacles.[91]

Canadian doctrine reflects the maturity that air power theory has developed over the past century. Each of the operational functions can be generated through air operations. Command provides the vertical integration required to direct air power when and where required. Aircraft support the Sense function by contributing to the commander's situational awareness. Still and video imagery and radar tracking all provide valuable information with which to plan. The Act function for aviators is both movement and engagement. Missiles and bombs are clearly kinetic and comparable to land and maritime weapons. The mobility of aircraft can support force projection of land troops and airspace interdiction. Similarly to ships in the maritime environment, the availability of aircraft provides a credible deterrent threat which can limit the adversary's military options.[92] Aircraft contribute to the Shield function through early warning of threats and deterrence of aggression and evacuation of forces. The Sustain function is

[90] *Ibid*., 24.

[91] Department of National Defence, B-GA-400-000/FP-000, *Aerospace Doctrine* (Ottawa: DND Canada: 2010), 25.

[92] Department of National Defence, B-GA-400-000/FP-000, *Aerospace Doctrine…,* 32-33.

provided whenever materiel is airlifted and also when conducting air refueling to prolong the range of other aircraft.[93]

The versatility of aircraft create considerable demand for support to land and sea forces. Bombers can reach far beyond the range of artillery guns and aircraft can rapidly insert regular soldiers and paratroopers on the battlefield where they can be most effective. Aircraft greatly expand the range of ship sensors beyond the horizon, they can launch torpedoes at distant enemy vessels and they provide a lifeline to shore for high priority personnel and equipment movement. This versatility creates a demand that has traditionally exceeded available capacities. In order to address the need for prioritization the tenant of centralized control and decentralized execution of air power is employed by the CAF.[94]

COMMON DOMAIN ATTRIBUTES

Each of the three previous domains exercises Command and supports the Sense, Act, Shield and Sustain functions. Military forces are able to observe, move, strike targets, defend from threats and exist in each of the respective domains. Each of these abilities is affected to some degree by weather conditions. Military power can be projected from any of the previous domains to generate effects in the other domains. Air defence systems that deny access to aircraft are employed by land forces. [95] Aircraft can

[93] Canadian aerospace doctrine includes "Generate" as an operational function which the Army and Navy have dropped for consistency with NATO and US doctrine. See B-GA-400-000/FP-000…, 35.

[94] Department of National Defence, B-GA-400-000/FP-000, *Aerospace Doctrine*…, 28.

[95] In Canada the air defense role is assigned to the artillery branch while other countries like Germany have assigned the role to the air force. However, hand-held ground-to-air missiles known as Man Portable Air Defense Systems (MANPADS) like the US made Stinger and Russian SA series are available to land forces of over 100 countries. See DFAIT, "MANPADS Countering the Terrorist Threat,"

drop bombs on land targets or anti-submarine torpedoes in the water. Navy destroyers can reach land targets with their guns and some nuclear submarines carry inter-continental ballistic missiles (ICBM) like the Trident II with a range of 11000 kilometers.[96] The littorals and seaways are where ships are vulnerable to land based defenses.[97] Land forces have the ability to strike maritime targets using direct and indirect fire from guns and artillery as evidenced by the military forts that pepper the Great Lakes in North America. When considering the Act function, each of the domains can generate the physically destructive effects necessary to satisfy the Clausewitzian definition of war.

The Land, Sea and Air domains each possess a dimensional quality. The fundamental objective of the elemental forces is to control portions of those domains.[98] Army elements may measure progress in kilometers, defend a frontage of specific width and compare the effective ranges of their weapons. Maritime forces employ nautical miles per hour (or knots) and measures of depth below the ocean surface. Aviation forces are keenly aware of their range for a given weight and fuel supply. Each has an Area of Operations and Area of Responsibility.[99] Considerable effort is applied in joint operations to coordinating activity in the battle space to prevent fratricide and accidents like helicopters flying through active artillery corridors. The freedom of movement and freedom of action that come from the control of land, maritime and air traffic is what permits one force to dominate another.

Commonwealth of Australia, June 2008. Accessed on 19 April 2013, http://www.dfat.gov.au/security/MANPADS_countering_terrorist_threat.pdf.

[96] Andreas Parsch, “Lockheed Martin UGM-133 Trident II,” accessed on 6 February 2013, http://www.designation-systems.net/dusrm/m-133.html.

[97] Peter Dutton, Robert S. Ross, and Oystein Tunsjo, *Twenty-First Century Seapower* (New York: Routledge, 2012), 21.

[98] The control theme is repeated in service doctrine with the understanding that friendly forces are able to exercise their freedom of movement and action while the same is denied to the adversary forces.

[99] Department of National Defence, B-GA-400-000/FP-000, *Aerospace Doctrine…,* 63.

Sovereignty is closely related to the dimensional attributes of land, sea and air. The concept of a nation having absolute authority over their land, territorial waters and airspace is well established. This authority manifests itself through border security, customs agents, coast guards, and fly-over arrangements. Protecting national sovereignty is central to the concept of *Jus ad bellum* described in the United Nations Charter.[100]

COMPARING MATTER AND SPACE

The examination of space provides a yardstick with which to compare the criteria distilled from the first three domains. Much like the history of powered flight, success only came from an accumulation of technology and innovation. The first liquid fueled rocket, capable of escaping earth's gravity came approximately two thousand years after the rocket-like Hero engine was demonstrated in Alexandria.[101] When the Soviet Union launched the World's first artificial satellite into orbit in 1957, the race for achievements in space became a proxy for conflict during the Cold War. President Kennedy called upon the United States to accept the challenge in a 1961 speech to Congress which would later be described as "not simply a call for advancement and achievement; it was a battle cry against communism."[102]

Space is classified as a separate domain of military operation by the United States and has been supported by a distinct military command in the United States military since

[100] United Nations Charter, Chapter VII Article 51.

[101] NASA, "Brief History of Rockets," accessed on 8 February 2013, http://www.grc.nasa.gov/WWW/k-12/TRC/Rockets/history_of_rockets.html.

[102] Neil deGrasse Tyson, "The Case for Space…, 23.

1982.[103] Most countries have accepted the definition from the *Fédération Aéronautique Internationale* specifying that space begins 100 kilometers above the surface of the earth.[104] By this definition, only 530 people have ever been to space in five decades of space travel.[105] That exclusivity only partially explains why this environment is considered exotic and distinct from the Air domain.

There are several unique characteristics associated with space operations. Foremost are the particularities associated with orbital mechanics. Satellites travel at speeds and altitudes that are orders of magnitude beyond those of atmospheric craft. Global Positioning Satellites, for example, travel 11,000 kilometers per hour at an altitude of 20,000 kilometers.[106] Boeing's 737, the most common passenger airliner,[107]flies at a comparatively slow 800 kilometers per hour and ten to twelve kilometers in altitude. Satellites are not flown or controlled like airplanes. Orbits are fixed by the final trajectory of the launch delivery system and only minor changes can be made to correct altitude and rotation speed. The amount of fuel that powers the thrusters for attitude control is a critical factor in the service life of the satellite. When there is no means of correcting a satellite's attitude, it will degrade from the pull of lunar gravity. These positional changes ultimately affect communications controlling the satellite as

[103] Robert Kehler, "Shaping the Joint Fight in Air, Space and Cyberspace," *Joint Force Quarterly*, issue 49, 2nd Quarter 2008, 33.

[104] The United States defines space from an altitude of 50 km. See Fédération Aéronautique Internationale, "FAI Sporting Code Section 8 – Astronautics," 2009, para 2.18.2.

[105] Joshua J. Romero, "How Many People Have Been In Space?" Scienceline, accessed on 8 February 2013, http://scienceline.org/2007/03/ask-romero-people_in_space/.

[106] http://royal.pingdom.com/2010/03/23/everything-you-ever-wanted-to-know-about-gps/

[107] Max Kingsley-Jones, "6,000 and counting for Boeing's popular little twinjet," Flightglobal accessed on 9 February 2013, http://www.flightglobal.com/news/articles/pictures-6000-and-counting-for-boeings-popular-little-twinjet-325472/.

antennas cannot be oriented toward their ground stations.[108] The remoteness of objects in orbit makes them costly to refuel and they normally become space debris in the course of their lifecycle.

The argument favouring the integration of space operations into the domain of air power provides an alternate view of the space domain. Bruce DeBlois, a professor of Air and Space Technology at the School of Advanced Airpower Studies, summarized a pervasive theme from western nations at the Airpower Conference in the United Kingdom on 12-13 September 1996: “the next logical step from the exploitation of airpower and space capabilities was [sic] the merging of the two environments toward the exploitation of “aerospace” power.”[109] While their extreme elevation is beneficial for political and technical reasons, the capabilities delivered by satellites can be compared to those delivered by assets operating in earth’s atmosphere. The command and control, monitoring and management of these assets are similar to long range and high endurance unpiloted aerial vehicles like the Global Hawk which are occupying a greater role in some fixed wing fleets.[110] Canada has adopted a partially inclusive *Aerospace Doctrine* which addresses the employment and use of space assets.[111] However, this may speak to the modest ownership of space services more than possible ambitions of assuming a role similar to the Canadian Space Agency.

[108] *Encyclopædia Britannica Online*, s. v. "satellite communication," accessed on 9 February 2013, http://www.britannica.com/EBchecked/topic/524891/satellite-communication.

[109] Bruce M. DeBlois, “Beyond the Paths of Heaven - The Emergence of Space Power Thought,” School of Advanced Airpower Studies, September 1999, ix. Accessed on 19 April 2013. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA421934.

[110] Craig Caffrey, "US DoD Revises Long-Term Fixed-Wing Investment Plan, " accessed 2/9/2013, 2013, http://www.janes.com/products/janes/defence-security-report.aspx?ID=1065929717.

[111] Department of National Defence, B-GA-400-000/FP-000, *Aerospace Doctrine*…, ii.

The applicability of the operational functions to space is clear. A command structure applies to the prioritization of use for space based services. Similar to the case with air power, centralized command is necessary since the demand for services like communications bandwidth exceeds the available capacity. Imaging satellites contribute to the Sense function using visible light, radar and other spectrums to provide geographic and infrastructure information in addition to mobile objects. The Act function could be considered in several ways. GPS satellites provide the data required for some smart munitions, such as the Excalibur artillery projectile, to strike their targets.[112] It is possible to place a weapon in orbit which could remain there waiting for a signal to re-enter the atmosphere and strike a designated target. It is also possible to place a satellite in orbit with a laser or radio frequency antenna designed to disable or jam an enemy satellite. The Outer Space Treaty of 1967 forbids the placement of weapons of mass destruction in space but it is still technically possible to do so[113] and there was evidence in the 1980s that the soviets had developed anti-satellite satellites.[114] The Shield function includes preserving the capabilities and freedom of action of the force. From that perspective, the GPS preserves positional awareness capability for troops, vehicles, ships and aircraft when other means would be less effective. Accurate positional awareness is a critical requirement to avoiding fratricide in the conduct of kinetic operations.[115] The repair

[112] Raytheon, “Excalibur Precision Guided Extended Range Artillery Projectile,” accessed on 9 February 2013, http://www.raytheon.com/capabilities/products/excalibur/index.html.

[113] Outer Space Treaty, 27 January 1967, Article IV.

[114] James Canan, War in Space (New York: Harper & Row, 1982), 175.

[115] US Army, “ADRP 3-37 Protection,” Dept of the Army, Washington: 28 February 2013, 4-1.

service provided by astronauts to the Hubble telescope is one example of the Sustain function in the space domain.[116]

The dimensional and atmospheric qualities also apply to space with some notable differences. National sovereignty does not extend to space the same way it applies to land, water and air. Above 100 kilometers, the lowest altitude that can accommodate an earth satellite, international treaties do not recognize national ownership.[117] All geostationary satellites occupy a nearly continuous position and other types of orbits necessarily pass over different territories. The 1967 Space Treaty makes clear that assets in space are owned by the nation of origin but space and celestial bodies cannot be claimed by states. The weak signals used to communicate between satellites and their ground stations are subject to atmospheric attenuation which is further degraded by rain, snow and dust. Atmospheric attenuation only applies to objects in low earth orbit but all satellites can be affected by solar wind and flairs.[118]

The dimensional aspects of objects in orbit also change the notion of control in space. James Lee, in *Counterspace Operations for Information Dominance* suggests that it is unnecessary to control space through the use of physical (read anti-satellite) means. The growing number of nations who have established space assets and the lasting impact of space debris make physical destruction of adversary satellites an impractical option.[119]

[116] The Hubble telescope was designed with service missions in mind so that critical parts and fuel could be replaced in orbit. See http://hubblesite.org/the_telescope/team_hubble/servicing_missions.php.

[117] Several equatorial countries claimed the space above their borders in 1976 through the Bogota Declaration but their claim has not been acknowledged. Thomas Gangale authored an explanation of why terrestrial land claims principles should not apply to orbital mechanics. Accessed on 9 February 2013 http://pweb.jps.net/~gangale/opsa/ir/WhoOwnsGeostationaryOrbit.htm.

[118] Peter J. Brown, “Solar Weather Effects on Satellites,” Intelsat accessed on 9 February 2013. http://www.intelsat.com/resources/tech-talk/solar-weather.asp.

[119] Melissa Gray, “Chinese space debris hits Russian satellite, scientists say,” CNN accessed on 19 April 2013, http://www.cnn.com/2013/03/09/tech/satellite-hit.

Lee suggests that the focus should be on the role of satellites as sources of information. Conventional jamming, destruction or interference with satellite ground stations can deny an adversary the benefit of satellite imagery and communications that are valued by the military. By targeting the information flow to and from satellites, space control can be achieved albeit indirectly.[120]

SUMMARY

Canadian, NATO and United States doctrine provide a sound basis from which to draw key attributes for defining a domain. Of particular importance is that a domain be capable of addressing the five operational functions of Command, Sense, Act, Shield and Sustain. By comparing the land, sea, air and space domains we can also conclude that domains possess a dimensional quality that can define an area of operation but is not necessarily bound by the historical concept of sovereign territory. From each of the domains examined is possible to project influence into the other domains. There is also a measure of environmental influence whereby adverse conditions (weather or terrain can degrade the effectiveness of activity in each of the four domains.

The ability to direct activity, observe, move, strike, defend and preserve those abilities; the essence of the operational functions; are key to the projection of military force and influence which result in control. All of these functions can be supported in each of the domains considered with the acknowledgement that physical control of space would be impractical and information control serves as a proxy. Therefore, the conclusion is that the operational functions provide a screen through which new domains

[120] James G. Lee, “Counterspace Operations for Information Dominance,” Paper for master’s degree, School of Advanced Airpower Studies, Air University, Maxwell AFB, Ala., 1996.

should be able to pass. The next chapter will apply this process to cyberspace to demonstrate that it falls short of meeting the requirements to be considered a domain of military operations.

Unfortunately, no one can be told what the Matrix is. You have to see it for yourself.

- Morpheus, The Matrix, 1999

CHAPTER 2 – THE NATURE OF CYBERSPACE

This chapter will demonstrate that cyberspace possesses many of the characteristics necessary to qualify as a domain of military operations. However, it also lacks permanence and habitability. Cyberspace is not easily defined by operational boundaries and multiple actors can have influence at the same time. This creates a high potential for interference. Those characteristics imply the need for centralized control and centralized execution of cyber operations. This chapter will argue that the aforementioned deficiencies make it inappropriate to compare cyberspace with the four established domains. Cyberspace has more in common with special operations than an environmental domain.

Land, sea and air power theory is derived from our occupation of the corresponding environment and how its characteristics influence the way we project force. The army, navy and air force all train specialists in the tactics and operations of those domains. Notwithstanding the years of study required to develop that domain centric proficiency, aviators, sailors and soldiers can draw parallels and understand the other's domain using joint language.[121] Even space, defined by vacuum, gravity and

[121] Refer to Canadian Forces Joint Publication A1: Department of National Defence, A-AE-025-000/FP-000, *Joint Doctrine Development Manual* (Ottawa: DND, May 2008), Forward; and Geoffrey Till, Seapower – A Guide…, 33.

orbits can be described in plain terms to a non-specialist. The reality of the International Space Station and civilian space activity[122] are evidence that our science fiction, depicting regular travel into space and between planets, has factual potential.[123] Space can become as accessible to military operations as the atmosphere is today. This is not the case with cyberspace.

Contemporary military doctrine is struggling with the form and function of cyberspace. Vincent Manzo, a Research Analyst at the National Defense University, agrees that it is misleading to treat cyberspace as an independent domain when its effects are better categorized as a cross-domain enabler.[124] This struggle is consistent with previous attempts to qualify non-physical force projection in common terms. Despite the ubiquity of cyberspace through private, corporate and government activity non-specialists fail to understand it. Michael Hayden, former director of the US National Security Agency stated "rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon."[125] Hayden's words echo those of Morpheus at the top of this chapter. This new realm has expanded and continues to grow faster than our ability to grasp the military implications. Nonetheless, many Western nations have embraced the concept of cyber war and effectively swallowed the same red pill that Neo did in *The Matrix*.[126]

[122] Virgin Galactic and Boeing each have civilian space ambitions and SpaceX is currently providing transportation service for NASA to the ISS. Accessed on 6 April 2013, http://www.nasa.gov/mission_pages/station/structure/launch/index.html.

[123] This statement is not a prediction of faster than light travel; just an expectation that travel beyond earth's atmosphere will eventually become commonplace.

[124] Vincent Manzo, "Deterrence and Escalation in Cross-domain Operations Where Do Space and Cyberspace Fit?," JFQ, issue 66, 3rd Quarter 2012, 9.

[125] Thomas Rid, "Cyber War will Not Take Place," Journal of Strategic Studies, 35:1, 9.

[126] In the story, Neo is offered a blue pill which will send him back to his regular life, or a red pill which will initiate the release from, and revelation of, the matrix.

This chapter will examine cyberspace from three perspectives. First, the environment will be defined to establish its boundaries. From container to content, the elements that comprise cyberspace will be delaminated with a brief look at the Open Systems Interconnection (OSI) model. The origins of the hardware, firmware and software will be mapped and their flaws revealed. Then, using the elements distilled from chapter 1, cyberspace will be subjected to the litmus test of military operations. Some activities like the attack and defence have obvious parallels to the physical domains. The reconnaissance and withdrawal are also fairly obvious. Other terms commonly applied to physical domains are less obvious such as vital ground, superiority, and being “in-contact” with the adversary. Finally, the key differences will be considered. Fundamentally it is the malleability of cyberspace and our inability to occupy it that set it apart from the established domains. Cyberspace can be exploited for military purposes and may prove to be decisive in future conflicts. However, that possibility does not provide the seed from which to grow a cyberspace force akin to the Royal Canadian Air Force. While land, sea and air can be called doctrinal siblings and space is (for now) a cousin, cyberspace is not in the same family. The new domain is more closely related to information operations and the electromagnetic spectrum which have never warranted the status of a domain.

WHAT IS CYBERSPACE?

Cyberspace first needs to be defined in order to describe its possibilities and limitations from an operational military perspective. Cyberspace is comprised of all existing computer networks and all the devices connected to those networks.[127] This scope is much larger than the Internet. The Internet is described as a vast network of commercial, educational, government and private computer networks all linked and able to exchange data using a common set of communication protocols.[128] Connectivity is a criterion for inclusion for the Internet so a regular mobile telephone, an MP3 player and GPS receiver are excluded. Cyberspace would include the three previous devices just as it includes all network enclaves and isolated devices so long as they contain a data processing element.

There are different models used to describe the spectrum of hardware, programming and data required for information technology (IT) to operate. The OSI model separates the spectrum into seven layers: Physical, Data Link, Network, Transport, Session, Presentation and Application. A widely used model that applies to the Internet is the Transmission Control Protocol and Internet Protocol (TCP/IP) model which describes four layers: Link, Internet, Transport and Application. The key to understanding activity in cyberspace is to recognize that, whatever model is used, each layer offers opportunities for access into the environment. Some access was intentionally provided by the engineers, programmers, administrators and users. Some access is unintentional but just as functional for those who understand the technology and programming.[129]

The terrain of cyberspace is defined by each of the layers that comprise an IT system. The hardware can be compared to continental geography. The hardware is

[127] Richard Clarke, William Barnes and Robert Knake, *Cyber War: The Next Threat to National Security and what to do about it* (Harper Collins e-books, 2010), 148/571.

[128] Dictionary.com “The Internet” accessed on 6 April 2013, http://dictionary.reference.com/browse/internet.

[129] Bradley Mitchell, “OSI Model - Open Systems Interconnection model,” accessed on 7 April 2013, http://compnetworking.about.com/cs/designosimodel/g/bldef_osi.htm.

permanent and immobile; shaped into mountains, swamps, rivers and highways at the time it was manufactured. The firmware provides the first layer of programming and data for the hardware. The firmware may remain unaltered for the life of the device if it is recorded on permanent memory. If the firmware is recorded on Electronically Programmable Read Only Memory (EPROM) or flash memory it can be upgraded or altered.[130] Modified firmware known as a hack can be used to circumvent limits imposed by a manufacturer such as the "Nikon Hacker"[131] which removes video recording time limits and makes native image files accessible to the user. When used on *Apple* devices, firmware hacking is referred to as "jailbreaking."[132] This malleability extends up through the presentation and application layers. The quality of non-permanence is the first characteristic that truly separates cyberspace from the other domains and will be explored later in this chapter.

Since hardware and firmware recorded onto permanent memory are the two unalterable elements of IT it is important to recognize a few realities related to their origin. First is the pressure for IT companies to deliver products with a vast array of features to remain competitive in a field that values innovation.[133] Many of these features are made possible by the computational speed of central processing units and special

[130] Webster's New World Telecom Dictionary, "Firmware,". Indianapolis: Wiley Publishing, Inc 2010.

[131] AluKd, "First Nikon Firmware Hack Out: Limitless (kinda) Video," DP Review.com, accessed on 7 April 2013, http://forums.dpreview.com/forums/post/41094074.

[132] Apple iPhone School, "What is Jailbreaking?," Appleiphoneschool.com, accessed on 7 April 2013, http://www.appleiphoneschool.com/what-is-jailbreaking/.

[133] Keshav Murgesh, "Innovation to drive growth in IT," accessed on 6 April 2013, http://www.business-standard.com/article/companies/innovation-to-drive-growth-in-it-113021500085_1.html.

purpose integrated circuits.[134] Boy Luthje from the University of Frankfurt has studied the IT manufacturing chain and highlights “a new type of relationship between brand-name firms (OEM) and their contractors in manufacturing, resulting from vertical specialization in the most advanced sectors of the computer and telecommunications industry.”[135] Luthje describes the manufacturing migration from Silicone Valley to Chinese companies beginning in the early 1990s. Name brand American and European companies like Dell, Compaq, Ericsson and IBM outsourced their manufacturing to lower cost plants in Asia. This vertical specialization also accelerates the cycle between product design, engineering, manufacturing and delivery to market. This product delivery model creates an opportunity for the manufacturer to add features to the integrated circuits or the firmware that would be known only to them and, possibly, the authority that requested the additions. Even if the engineering and design specifications are produced, and then tested, by the named company, the complexity of the assemblies is such that new features are likely to remain undetected. The result is that any level of outsourcing creates opportunities for an adversary to add cyber terrain features. These could constitute the continental equivalent of “high ground” or “key terrain” that is unknown until they are exploited by that adversary. The US House of Representatives' intelligence committee has stated publicly that products from Huawei and ZTE, large Chinese technology firms, are cyber security threats to national telecommunications

[134] Cyber Media, “From the Labs: Information Technology,” accessed on 2 April 2013, http://www.technologyreview.in/computing/38506/.

[135] Boy Lüthje, “IT and the Changing Social Division of Labor: The Case of Electronics Contract Manufacturing,” Draft paper for Conference on Transforming Enterprise, Washington, D.C., January 27-28, 2003, 5.

infrastructure.[136] Other Chinese companies that assemble computers and load software have been accused of adding malware and counterfeit operating systems with security vulnerabilities.[137]

The subsequent layers of the IT systems are as malleable as they are porous to intrusion and those entry points come from many sources. Operating systems, software applications and the user interface can all contain thousands of lines of programming code. Frequently, they are created to achieve the objectives of the program before there are any thoughts of security.[138] Even when security is a deliberate consideration at the designing and programming stages of application development, vulnerabilities are common.[139] When first revealed these weaknesses are called zero day exploits, a reference to the time the manufacturer has had to correct the vulnerability.[140] There was also a cultural shift in programming from the 1980s to the 1990s. As the cost of computer memory dropped there was less pressure on programmers to be efficient and elegant with their code. The popularity of Object Oriented Programming in the 1990s established large libraries of modular code that programmers could draw from to accomplish common tasks.[141] Programmers from that time and still today can integrate modules for

[136] Charles Arthur, "China's Huawei and ZTE pose national security threat, says US committee," accessed on 7 April 2013, http://www.guardian.co.uk/technology/2012/oct/08/china-huawei-zte-security-threat.

[137] Associated Press, "Malware infecting PCs on production line, Microsoft says," http://www.cbc.ca/news/technology/story/2012/09/13/tech-ap-malware-microsoft.html.

[138] Larry Dignan, "Why is security usually an afterthought?" accessed on 7 April 2013, http://www.zdnet.com/blog/security/why-is-security-usually-an-afterthought/865.

[139] Susan Kennedy, "Common Web Application Vulnerabilities," accessed on 2 April 2013, http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Pages/Common-Web-Application-Vulnerabilities1.aspx.

[140] Definition of "zero-day exploit" accessed on 2 April 2013, http://searchsecurity.techtarget.com/definition/zero-day-exploit.

[141] Oregon State University, "Thinking Object Oriented," accessed on 2 April 2013, http://web.engr.oregonstate.edu/~budd/Books/oopintro2e/info/chap01.pdf.

interpreting mouse movements, manipulating data or creating graphics without ever seeing the way those lines were coded.[142] The now common practice of introducing new versions of popular software that remain compatible with previous versions also invites the retention of vulnerabilities that an adversary can exploit such as the case with Java.[143]

Programming practices are not the only source of porosity. Vulnerabilities can either stem from the way the system was designed or the way it is employed by the end user or administrator. The analogy of automobile security provides a useful reference. Many current vehicle manufacturers install locks and electronic theft deterrents to enhance security. However, if the vehicle operator leaves the doors unlocked or in a poorly monitored area a thief can enter the car and steal the items inside. In 2008, Joshua Fruhlinger, a technology writer for Engadget, described how 68% of the electronic gadgets returned by customers were due to customer frustration and dissatisfaction. Only 5% of the $13.8 billion in returned gadgets were due to device failure.[144] These figures create tremendous pressure for manufacturers to simplify the ease of operation for customers. The resulting *Plug and Play* devices rely on default settings amounting to unlocked doors for adversaries to exploit.[145]

[142] Luca Cardelli, “Bad Engineering Properties of Object-Oriented Languages,” Digital Equipment Corporation, Systems Research Center, accessed on 2 April 2013, http://lucacardelli.name/Papers/BadPropertiesOfOO.html.

[143] Jeong Wook (Matt) Oh, “Recent Java exploitation trends and malware,” Black Hat USA 2012 Las Vegas, accessed on 2 April 2013, https://media.blackhat.com/bh-us-12/Briefings/Oh/BH_US_12_Oh_Recent_Java_Exploitation_Trends_and_Malware_WP.pdf.

[144] Joshua Fruhlinger, “95 percent of all returned gadgets still work, Americans don't read manuals,” Engadget accessed on 2 April 2013, http://www.engadget.com/2008/06/03/95-percent-of-all-returned-gadgets-still-work-americans-dont-r/.

[145] HD Moore, “Whitepaper: Security Flaws in Universal Plug and Play: Unplug, Don't Play,” Security Street, accessed on 2 April 2013, https://community.rapid7.com/docs/DOC-2150.

COMPARING CYBERSPACE AND REAL SPACE

There are many rational explanations for the current popular acceptance of cyberspace as a domain. The growth of our artificial environment over the past 15 years has delivered new ways of communicating, conducting business and projecting influence. Remote communities that were unlikely to receive services taken for granted in 1st World nations like land line telephones and cable television have been linked to a global community through mobile smart phones and internet cafes. People can interact and experience alternate lives in cyberspace through the avatars in *Second Life, Onverse* and over 20 other virtual environments.[146] The social exchange possibilities previously limited to speculative science fiction are becoming commonplace. Clearly, an environment that permits the exchange of services, currency and ideas can be compared to the physical World. Cyberspace can, in some circumstances, be used to compel behaviour and create tangible physical effects.[147] Supporters of the cyber domain will argue that an environment that supports criminal activity and police work can also be used for military purposes.[148]

Indeed, there are many military activities that can be executed in cyberspace. The operational functions described in chapter 1 are a helpful way to categorize these undertakings. The Sense function includes reconnaissance, surveillance and information gathering. Much information can be gathered from network accessible storage once a

[146] Ariane B, “3D Virtual Worlds”, accessed on 3 April 2013, http://arianeb.com/more3Dworlds.htm.

[147] Lt Col Russell F. Mathers, “Cyberspace Coercion in Phase 0/1: How to Deter Armed Conflict,” US Naval War College, 2007, accessed on 3 April 2013, http://www.dtic.mil/dtic/tr/fulltext/u2/a476693.pdf.

[148] David S. Wall, “Policing Cybercrimes,” accessed on 3 April 2013, http://www.cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf.

computer network has been penetrated. Access can be obtained through a variety of techniques including the Trojans and key logging malware commonly used by identity thieves.[149] The documents and correspondence accessed through cyberspace could significantly contribute to intelligence gathering and understanding of an adversary's physical battle space. However, it is also pertinent to recognize that misinformation is an ancient technique recognized by Sun Tzu[150] and repeatedly used during the Cold War.[151] Clausewitz cautioned that misleading information was a risk to operational planning[152] and it would be easier to create an "Operation MINCEMEAT"[153] in cyberspace than it was in real space. Cyberspace offers a new medium for both sides of a conflict to employ and the intelligence principle of verifying the credibility of information from multiple sources remains valid.

Few people would deny that the Act function can be exercised through cyberspace. Richard Clarke and Robert Knake describe many cyber threats that have the potential to deliver physical effects in their book *Cyber War*.[154] Experiments have demonstrated that the electrical grid, power generators and the control systems for

[149] Deepac Saini, "How Keyloggers are Used to Hack Any Type of Online Account," accessed on 3 April 2013, http://hackerspirit.blogspot.ca/2012/07/how-keyloggers-are-used-to-hack-any.html.

[150] Sun Tzu and Lionel Giles, The Art of War (Internet Classics Archive: 1994), 2.

[151] The Farewell Dossier describes several CIA deception operations from the 1980s. Jeffrey Carr, "The Myth of the CIA and the Trans-Siberian Pipeline Explosion," accessed on 5 April 2013, http://www.infosecisland.com/blogview/21566-The-Myth-of-the-CIA-and-the-Trans-Siberian-Pipeline-Explosion.html.

[152] Carl von Clausewitz, Charles Keller, and David Widger, On War (Gutenberg EBook, 2006), Book 4, Chap XIV.

[153] Operation Mincemeat was an elaborate and successful deception used in 1943 to convince the Germans that Allied forces would attack Greece instead of Sicily. Accessed on 3 April 2013, http://www.bbc.co.uk/history/topics/operation_mincemeat.

[154] Richard Clarke, William Barnes and Robert Knake, *Cyber War: The Next Threat to National Security and what to do about it* (Harper Collins e-books, 2010), Chap Three, 59 of 61.

hydroelectric dams can, under certain conditions, be compromised by malware.[155] Several newer threat possibilities will be explored in chapter 3. However, it is pertinent to highlight that the only publicly acknowledged example of a cyber-attack resulting in physical damage is the *Stuxnet* virus. A NATO research team has suggested that *Stuxnet* does constitute an “act of force” but it is not an “armed attack”.[156] While that decision may be biased in favour of the originator of *Stuxnet*, the US perspectives also conceded that a cyber-attack resulting in damage of sufficient extent, intensity or duration could be considered an armed attack and justify a military response.[157] It is pertinent to note that Iran, the victim of *Stuxnet*, has not claimed it to be an armed attack. The gap between kinetic cyber-attacks and the attacks from bombs and missiles is likely to remain until an example can be studied by the World nations. Until then the political and military perspectives on cyberspace are as ephemeral as the information warfare doctrine of the 1990s; an insufficient foundation upon which to build a domain.

The Shield function has been exercised from the early days of military networks. When the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense created the ARPANET[158] the design included a high degree of redundancy to promote availability of the service. Initially, access to ARPANET was limited to insiders and physical access to the computers was a sufficient level of network security. As the

[155] Richard Clarke, William Barnes and Robert Knake, *Cyber War: The Next Threat to National Security and what to do about it* (Harper Collins e-books, 2010), Chap Three, 59 of 61.

[156] Global Research, “US-Israeli Stuxnet Cyber-attacks against Iran: “Act of War”,” accessed on 5 April 2013, http://www.globalresearch.ca/us-israeli-stuxnet-cyber-attacks-against-iran-act-of-war/5328514.

[157] Siobhan Gorman and Julian E. Barnes, “Cyber Combat: Act of War,” accessed on 7 April 2013, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

[158] The ARPANET is the computer network that evolved into the Internet. Accessed on 7 April 2013, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

network community expanded to other government sites and universities there was a greater need for network tools that provided authentication of credentials, confidentiality and data integrity.[159]

The protection of data, network integrity and availability remains a full time effort for network administrators and information technology security staff. Ed Bott, a technology writer, described a complex ecosystem of viruses and malware circulating in cyberspace.[160] Most of the threats are variants of a few hundred distinct viruses, none of which were originally launched for military purposes. Once a piece of code has been released into the wild it can be recycled and repurposed by other actors. Malware can be "weaponized" for military use as demonstrated by *Stuxnet* which exploited a vulnerability originally targeted by the Conflicker worm.[161] Other threats include intrusion attempts by hackers, disgruntled employees, and unauthorized releases of data.

As described in Chapter 1, command is exercised between people. That exchange is independent of the domain they are operating in. Command can be enabled by cyberspace just as it is enabled by the electromagnetic spectrum that radios depend on. Command can also be crippled by a cyber-attack that disables radars, networks or databases but the effect can be directed to the land, sea, air, and space domains just as much as the cyber domain. For this reason, this author does not view the Command function to be a helpful discriminator.

[159] *The Froehlich/Kent Encyclopedia of Telecommunications* vol. 15. (Marcel Dekker, New York, 1997), 231-255. Accessed on 5 April 2013, http://www.cert.org/encyc_article/.

[160] Ed Bott, "The malware numbers game: how many viruses are out there?," ZNet accessed on 5 April 2013, http://www.zdnet.com/blog/bott/the-malware-numbers-game-how-many-viruses-are-out-there/4783.

[161] Aleksandr Matrosov, et al, *Stuxnet Under the Microscope Rev 1.31*, eset, 2011, 34.

The Sustain function highlights a more obvious dissimilarity between our virtual and physical environments. This function includes personnel and material availability to permit the military activity being conducted in each of the domains. Senior commanders frequently refer to logistics as the crux of military success. Sun Tzu cautioned that “the line between disorder and order lies in logistics.”[162] General Patton stated that “the officer who doesn't know his communications and supply as well as his tactics is totally useless.” Notwithstanding the importance of this function it does not occur in cyberspace. The provision of information technology equipment, the links between them and the specialists to install, repair and operate the systems all occur in real space. The air force conducts air-to-air refueling and the navy conducts replenishment at sea. It is also possible to replenish the consumable fuel used by satellites.[163] There is no comparable example for sustainment in cyberspace.

KEY DIFFERENCES

The key differences between cyberspace and the other domains are technical, procedural and physical. The fundamental technical difference is that cyberspace is a human creation that can be altered. As previously explained the physical infrastructure, programming and graphical user interfaces are volatile. There is no comparable in the physical World where armies can occupy high ground, aircraft have maximum speeds and ships are influenced by weather. In cyberspace this volatility presents opportunities

[162] International Military Quotes, accessed on 7 April 2013, http://www.military-quotes.com/forum/logistics-quotes-t511.html.

[163] NASA, “NASA'S Refueling Demonstration Proves Viability Of Satellite-Servicing Technologies,” Release: 13-046, 8 Feb, 2013, accessed on 5 April 2013, http://www.nasa.gov/home/hqnews/2013/feb/HQ_13-046_RRM.html.

for the sides with the technical ability to identify vulnerabilities and reprogram the environment they wish to operate in. Libicki suggests that cyber warriors could alter their networks to eliminate vulnerabilities when they are detected while they exploit the weaknesses in adversary networks.[164] An advancing army with this power could flatten hills, create open lanes, turn night into day and neutralize enemy weapons. Although it is possible to alter the physical environments in the conduct of war, laying minefields, destroying bridges and establishing air defence barriers take time and are frequently limited by geography and weather.

Procedural differences result from the technical differences between cyberspace and the physical domains. The volatility of cyberspace suggests that security vulnerabilities will be corrected as soon as they are detected. This places a premium value on the zero day vulnerabilities that are identified. Since an exploit is unlikely to compromise an adversary network the same way twice,[165] the malware produced with that aim may be controlled at very high levels in a military hierarchy. However, a large portion of cyberspace is governed by civilian infrastructure and software. Richard Bejtlich, an IT security specialist, reminds us that core internet services like BGP, DNS and SSL have held known vulnerabilities for several years.[166] System administrators can alter network security settings to considerable effect but short of removing commercial software some vulnerabilities will remain until they are addressed by the software manufacturer. The influence of civilian and adversary changes to cyberspace also means that a vulnerability can be eliminated at any time rendering a cyber-weapon useless. This

[164] Martin C. Libicki, *Cyberdeterrence and cyberwar* (Rand Corporation, 2009), 144.

[165] *Ibid*., 20.

[166] Richard Bejtlich, “Review of Cyberdeterence and Cyberwar,” accessed on 6 April 2013, http://www.amazon.com/review/R927SD2CZ7NTB.

unknown best-before, and bad-after expiry date may result in a greater inclination for commanders to launch the malware. If there is concern that subordinate commanders will launch cyber-weapons prematurely control over them will be retained at the highest levels.

The potential for conflicting cyber activities also suggests a high level of control will be necessary. If a subordinate commander's cyber soldiers were conducting an operation to benefit their mission the act could alert the adversary that their network has been compromised. This might derail higher priority cyber operations planned to occur at a later time. As previously discussed, cyberspace is not measured in the distances that apply to a division or carrier group area of operations. Therefore, coordination of and authority for cyber operations are likely to remain at a very high level.

Furthermore, it may be impossible to establish control over cyberspace the way physical space permits. The only physical control that can be exercised over cyberspace is to create enclaves by severing the links to external networks. *Stuxnet* demonstrated that isolated networks remain vulnerable and any control established by a future *Stuxnet* can be expected to be fleeting.[167] Counter arguments to this will highlight that information control was offered as a proxy for space control in chapter 1. However impractical it may be, physical means of control can still be exercised over space assets.

The inclination for centralized control and centralized execution of cyber operations constitutes an important difference with operations in physical domains.[168] One could argue that space operations are highly centralized in control and execution but

[167] Aleksandr Matrosov, et al, *Stuxnet Under the Microscope*…, 43.

[168] System administrators are decentralized but they respond to IT security policies established by a central authority. This author suggests that offensive cyber operations like *Stuxnet* should be directed by a central authority and executed by a core team.

that is likely to be the result of the high value and low number of space resources. Conceivably, activity in the space domain could expand to the point where it was structured like the air force with decentralized execution.[169] Even if cyber operations became more frequent, there is no cyber equivalent to an air traffic controller. The governance and dimensional peculiarities of cyberspace do not call for doctrinal parity with the physical domains.

Finally, the obvious physical difference is that people cannot enter or occupy cyberspace. In his examination of maritime and air power Wylie, explains that naval guns and aerial bombs, while formidable are incapable of winning a war in isolation.[170] Douhet's theory that air power was the ultimate means for military victory was proven wrong in World War 2 when the massively destructive bombing campaigns failed to subdue either Axis or Allied nations. In order to achieve victory military force must be in contact with the adversary and their population. This is done by soldiers on the ground. The cyber warrior may be a highly skilled technician, programmer or engineer but they will fight from a keyboard physically removed from the battle space. Cyber operations will certainly be a key enabler to each of the domains but cyberspace does not need the status of a domain to achieve that effect.

IS THERE A THERE THERE?

Michael Faraday first described a link between electromagnetic radiation and electromagnetism in 1845. Forty years later, Heinrich Hertz built a device that generated

[169] Royal Canadian Air Force, *Canadian Armed Forces Aerospace Doctrine* B-GA-400-000/FP-000 28 (Winnipeg: CFAWC), November 2010, 28.

[170] J.C. Wylie, *Military Strategy: A General Theory of Power and Control* (New York: Rutgers), 1967, 41.

and detected the electromagnetic energy that we now call radio but believed they had "no practical application."[171] He was wrong of course but his response speaks to the challenge many people have in understanding the intangible. The wireless telegraph grew out of the work of many physicists and innovators and by 1898 the Royal Navy was convinced of the utility of the communications device demonstrated by Marconi. The same year Nikola Tesla patented and demonstrated a remote control boat in Madison Square Garden.[172] Military forces were quick to embrace the wireless. Radio communications were used by all three services and the German Navy employed remote control boats to attack enemy vessels in World War 1.[173] It is noteworthy that air power doctrine developed from the application of technology and equipment in World War 1 and World War 2. During the same period the military employed radio, radar and television yet there is little consideration to raise the electromagnetic spectrum to the status of a domain of operation.[174]

In a series of attempts to grip the evolving nature of conflict western militaries adopted a series of new terms beginning in the 1990s. Terms like Information Warfare, Command and Control Warfare and Network Centric Warfare were used without a clear understanding of what they were[175] or how they addressed what Martin Libicki referred

[171] Heinrich Hertz is credited with this statement from an interview with a reporter soon after he published his experimental confirmation of Maxwell's Equations in 1886. Accessed on 5 April 2013, http://www.searchquotes.com/quotes/author/Heinrich_Rudolf_Hertz/.

[172] P.W. Singer, *Wired for War* (New York: The Penguin Press), 2009, 46.

[173] Jonas Klink, "Remote Controls – a Historical Background," CSE510 Washington University, accessed on 5 April 2013, http://www.cs.washington.edu/education/courses/cse510/05sp/lab1/Lab%201%20Jonas%20Klink.pdf.

[174] Some papers proposing acceptance of an EM Domain have been written by members of the Association of Old Crows, see Walter Wolf, "21st Centruy EM Domain Capabilities," The Journal of Electronic Defense, October 2011.

[175] Martin C. Libicki, "What Is Information Warfare?" National Defense University, October 1995.

to as “non-obvious warfare.” Libicki explains that “some forms of warfare are non-obvious because the relationship between the attacker and a state is unclear.”[176] While it is possible in some circumstances to confirm identity and origin of acts in cyberspace the attribution can be elusive in others. The *Stuxnet* worm has been attributed to the US and Israel[177] but there was no proof of that from a detailed examination of the malware.[178] This problem of attribution may suggest that military activities in Cyberspace should be categorized under the Special Operations heading rather than a separate domain.

Libicki has argued that the adoption of cyberspace as a war fighting domain has more to do with marketing and resourcing than the conduct of military activities. The senior officers are accustomed to operational activities from their experiences in the four physical domains. Therefore, they have a natural tendency to describe cyberspace in similar terms when creating policy and lobbying for resources to generate the desired capabilities.[179] In 1995 Libicki compared discussions of cyber warfare to a Victorian era discussion of air to air combat.[180] Doctrinal maturity of cyber warfare may not be realized until the cyber equivalent of two great wars has passed.

DO PHYSICAL DOMAIN ANALOGYS APPLY?

While the operational functions described earlier in this chapter can be helpful in categorizing cyber activities, other terms have no meaning in cyberspace. Tactical terms

[176] Martin C. Libicki, “The Specter of Non-Obvious Warfare,” Strategic Studies Quarterly, Fall 2012, 90.

[177] Nate Anderson, “Confirmed: US and Israel created Stuxnet, lost control of it,” accessed on 6 April 2013, http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

[178] Aleksandr Matrosov, et al, Stuxnet…, 10.

[179] Martin C. Libicki, “Cyberspace is not a Warfighting Domain,” 25 January 2012, 18-19.

[180] Martin C. Libicki, “What Is Information Warfare?..., 75.

used in continental warfare such as *vital ground* and *in-contact* are not consistent with an environment where bits and bytes are proxies for warriors. Unless designed to erase itself, malware cannot be recalled by the nation that launches it so a *withdrawal* is just as impossible as an *occupation* is meaningless. *Air superiority* does not translate to an environment where friendly and adversary activities can occur simultaneously and without attribution.[181] The *blockade*, a key form of sea control cannot occur without a network being isolated and, as previously mentioned, *Stuxnet* demonstrated that such networks remain vulnerable. Libicki argues that such comparisons are counterproductive. They lead to confusion, misunderstandings and delay the appropriate categorization of military activities conducted in cyberspace.[182]

Military doctrine is not alone in the struggle to define a relationship with intangible operating environments. In the age of cyberspace politicians have been forced to reconsider how they campaign. Businesses that embraced e-commerce have flourished while others, like Blockbusters, have been rendered obsolete.[183] The music industry continues to adjust its business model with subscription services and “pay what you want downloads.”[184] Traditional understandings of property rights and territorial law are being tested in the courts.[185]

[181] Some authors have ranked certain nations based on their perceived cyber capability. However, cyber war is not like an aerial dogfight. There is no evidence that a superior “cyber war strength” will translate into superiority in conflict. See Richard Clarke, William Barnes and Robert Knake, *Cyber War: The Next Threat*…, 300/571.

[182] Martin C. Libicki, “Cyberspace is not a Warfighting Domain,” 25 January 2012, 14.

[183] The Canadian Press, “Blockbuster Canada to close remaining stores,” accessed on 6 April 2013, http://www.cbc.ca/news/business/story/2011/08/31/blockbuster-canada-close.html.

[184] Aaron Colter, “Can pay-what-you-want downloads save the music industry?,” Digital Trends, 14 March 2012, accessed on 6 April 2013, http://www.digitaltrends.com/music/can-pay-what-you-want-downloads-save-the-music-industry/.

[185] Michael Geist, “Is There a There There? Toward Greater Certainty for Internet Jurisdiction,” University of Ottawa Faculty of Law, 2001, 9.

There are several reasons why physical to virtual comparisons can lead to false assumptions. As previously mentioned, much of the speculation has and is being made by non-experts. Lay-persons repeating technical information are susceptible to err. Some of the warnings come from groups with vested interests in building the IT security industry.[186] Representatives from these groups are expected to emphasize the risks and dangers to promote investments. This appears to have been the case with the exaggerated denial of service attack against *Spamhaus* at the end of March 2013.[187] Also, our experience with cyberspace as a species is arguably less than 20 years. That is enough time to be comfortable interacting with the new tools we have created and enough time for individuals to have developed particular skills as programmers or engineers.[188] Two decades is not long enough to have developed a perception comparable to that which alerts us to dangers in the physical World. The resulting speculation contributes to the fear of the unknown.[189]

The production of a comprehensive resource plan is beyond the scope of this paper but a few thoughts are pertinent. War fighting activities in the electromagnetic spectrum have taken place for one century. In that time, US and NATO doctrine has divided Electronic Warfare into three categories: Electronic Attack, Electronic Protection and Electronic Warfare Support.[190] Reliable use of the electromagnetic spectrum is

[186] Thomas Rid, “Cyber War will Not Take Place…, 22.

[187] Sam Biddle, “That Internet War Apocalypse Is a Lie,” Gizmodo, accessed on 7 April 2013, http://gizmodo.com/5992652/that-internet-war-apocalypse-is-a-lie.

[188] Malcolm Gladwell, describes the 10,000 hour principle required for a person to reach the apex of proficiency in any skill. See Gladwell, Malcolm. *Outliers: The story of success*. ePenguin, 2008. Chap 2.

[189] Jeffrey Winters, “Why We Fear the Unknown,” Psychology Today, accessed on 7 April 2013, http://www.psychologytoday.com/articles/200305/why-we-fear-the-unknown.

[190] United States, *Joint Doctrine for Electronic Warfare* Joint Publication 3-51 (Washington: n.p.) 2000, I-3.

essential to everything from deployable microwave linked command and control networks to the GPS signals that guide some smart bombs. The CAF employ operators and technicians specialized in the tactics, techniques and procedures of EM denial and exploitation. Electronic attacks are an integral part of the targeting cycle that synchronizes artillery, aviation, UAV and other activities in the battle space. The required EW capabilities and EM effects are achieved without the need for doctrine elevating the electromagnetic spectrum to the status of a domain.

SUMMARY

Cyberspace has grown to proportions that far exceed the boundaries of the Internet. The ubiquity of IT has propelled cyberspace trans-culturally from first to third World locations around the globe. The resulting social and commercial exchange creates opportunities for both licit and illicit activities in addition to military activities.

Cyberspace is fundamentally different from land, sea, air and space. The IT sandwich made of hardware, firmware and software layers create a complex artificial environment that few people truly understand. First, this virtual space is impermanent. System administrators are regularly updating software, adding hardware and changing settings with corresponding effects to the space. The complexity of each layer, market driven prioritization of feature delivery over security, and sourcing from dubious manufacturers create many vulnerabilities that adversaries can use to their advantage. The cyber terrain is also subject to the influence of commercial software and hardware providers.

The impermanence of cyberspace compels a centralized control and execution structure that is unlike the physical domains. Vulnerabilities require a high level of skill to identify and may only be useful for one attack. Those that can be used in zero day exploits have an unknown useless-after date. Also, the possibility of interference between different actors (allied or otherwise) suggests a central control and execution command structure is required for operations in cyberspace.

Military doctrine has struggled with the non-obvious means of influence since the 1990s. Cyber war is an extension of the theories that evolved from Information Warfare, Command and Control Warfare and Network Centric Warfare. While there is agreement that force and influence can be projected through cyberspace, the examples thus far have not been considered armed attacks. Even the kinetic effects resulting from *Stuxnet* were not described as an armed attack by the targeted state. The ephemeral nature of electronic signatures from cyber-attacks creates an attribution problem that shares more with special operations than the projection of force in the physical domains. This supports the employment of cyber capabilities in a supporting role to enable war fighting on land, sea, in air and space. The next chapter will explore some potential military actions and projection of force through cyberspace.

> *I cannot help fearing that men may reach a point where they look on every new theory as a danger, every innovation as a toilsome trouble, every social advance as a first step toward revolution, and that they may absolutely refuse to move at all.*
>
> *- Alexis de Tocqueville*

CHAPTER 3 – THE NEXT CYBER THREATS

The concern expressed by Alexis de Tocqueville above does not appear to have materialized yet. In his second book examining American democracy de Tocqueville suggested that a population enjoying the comforts of economic success would lose their appetite for revolutions, lest the resulting changes upset their contentment.[191] There is disagreement on what constitutes a revolution in military affairs but there is much evidence that first World populations continue to embrace new technology.[192] Perhaps de Tocqueville should have advised more caution about embracing change.

Cyberspace is delivering information, entertainment and opportunity to individuals, interest groups and governments. This new domain is also delivering threats that are misunderstood and both under and overestimated. People prone to worst-case speculation reference the science fiction films *The Terminator* or *The Matrix* where plots centre on technology turning against humanity. Those who wish to minimize concerns over cyber threats remind us that much effort and expense was applied to the Y2K problem with little evidence that any calamity was averted.[193] The reality is somewhere

[191] Alexis de Toqueville *Democracy In America Volume II*, (Project Gutenberg EBook #816, January 21, 2006), Chapter XXI: Why Great Revolutions Will Become More Rare.

[192] Elinor Sloan, "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities," *Canadian Military Journal*: Autumn 2000, 7.

[193] Tony Long, "Dec. 31, 1999: Horror or Hype? Y2K Arrives and the World Trembles," Wired.com accessed on 10 February 2013, http://www.wired.com/science/discoveries/news/2007/12/dayintech_1231.

in-between. While computers are now capable of besting the greatest chess masters and Jeopardy champions their actions are still limited by programming.[194] Unlike "Data," the android from the science fiction television series *Star Trek: The Next Generation*, today's computers are not sentient. Paul Rosenzweig, a former Deputy Assistant Secretary of the US Department of Homeland Security agrees. For the foreseeable future, cyber threats will result from the actions of people described by Rosenzweig as "malfeasant actors who seek to take advantage of [the] globalized web for their own reasons."[195]

Governments and corporations may be accepting risks without an adequate reference for the consequences. This chapter will demonstrate that cyber war is at its infancy and that new, innovative threats to individual and public interests are looming. These new risks will need to be considered and managed with skill sets that are not readily apparent in conventional safety and security services. Continuous attention must be applied to understanding the scope and nature of these threats so that policy and measures can be developed to address the impending security challenges. In order to describe the cyber threats in a credible manner, real World examples will be presented of cyber-attacks that have and can occur. The familiar cyber-attack examples of Estonia in 2007[196] and *Stuxnet* in 2010[197] demonstrate an evolution from the crude denial of service

[194] See: Chessbase News, "Kramnik vs Deep Fritz: Computer wins match by 4:2," http://www.chessbase.com/newsdetail.asp?newsid=3524, and Associated Press, "Computer beats Jeopardy!," http://www.cbc.ca/news/technology/story/2011/01/14/computer-jeopardy.html. Both accessed on 19 April 2013.

[195] Paul Rosenzweig, "Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World," Lawfareblog.com accessed on 24 February 2013, http://www.lawfareblog.com/2013/01/cyber-warfare-how-conflicts-in-cyberspace-are-challenging-america-and-changing-the-world/.

[196] Mark Lander and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," Last Accessed on 19 December 2012, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0.

attacks on web based services to the multi-faceted and highly sophisticated attack on uranium centrifuges. Predictions regarding near future threats will be based on experimental results that have potential military applications. Whether or not there is Canadian policy to permit the use of such action by the CAF is a secondary argument that will not be developed in this paper. Canada is a current target of cyber-attacks and is likely to remain one in the future.[198] It would be wise to consider the possibility of future attack scenarios and prepare mitigating strategies before they occur.

THE WEAKEST LINK

On 3 July 1988 an Airbus A300 operated by Iran Air was flying over the Strait of Hormuz when it was hit by two missiles fired from United States Navy guided missile cruiser USS Vincennes. The decision to fire, issued by the ship's Commanding Officer was based on the incorrect belief that the airliner was an Iranian F-14 fighter plane attacking the Vincennes.[199] The incident killed all 290 persons aboard the airliner and fueled tensions between the United States and Iran which remain high 25 years later.[200]

Surely the intelligence, surveillance and reconnaissance systems employed on modern military vessels cannot be subject to the same limitations that existed 24 years ago. Let's consider the state of some modern military systems. Defensive systems like

[197] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, February 2011, accessed on 10 February 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[198] Bill Curry, "Serious Flaws in Ottawa's Defence Against Cyber Attacks: Auditor General," accessed on 14 February 2013, http://www.theglobeandmail.com/news/politics/ottawa-notebook/serious-flaws-in-ottawas-defence-against-cyber-attacks-auditor-general/article4630798/.

[199] Department of Defense, "Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655on 3 July 1988," Letter CM-1485-88, 18 August 1988, 6, accessed on 14 February 2013, http://www.dod.mil/pubs/foi/International_security_affairs/other/172.pdf.

[200] David Cenciotti, "U.S. – Iran war games…24 years ago (Iran Air Flight 655 shot down by USS Vincennes)," 30 January 2012 accessed on 14 February 2013, http://theaviationist.com/tag/iran-air-flight-655/.

Phalanx and Goalkeeper provide ships with protection from incoming missiles and aircraft. Goalkeeper, currently in use with the navies of Belgium, Netherlands and the United Kingdom, was developed by the Dutch in 1975. This weapon system uses a seven barrel gun that fires 4,200 rounds of 30 mm ammunition per minute with a range of 4500 meters. This autonomous weapon requires no human intervention once activated and has been in service since 1979. With 30 years of operational use it will soon be undergoing a radar and fire control system upgrade to keep it in service until 2025.[201] Canada employs the Phalanx on its frigates, destroyers and replenishment ships in addition to other automated weapon systems such as the Bofors 57mm anti-aircraft and anti-ship naval gun. [202] While the technology of these systems can and has been upgraded they are not perfect and their human operators are prone to err.

The Royal Canadian Navy anticipates the arrival of “Autonomous Intelligent Systems” capable of independent combat without the input of a human operator.[203] This technology will certainly be one step closer to reality with the X-47B stealth drone. The prototype manufactured by Northrop Grumman is planned to conduct autonomous aircraft carrier take offs and landings, arguably the most difficult landings for human pilots to execute.[204] The utility of unmanned systems in combat is well established with

[201] Richard Scott, “Go-Ahead for Goalkeeper Update,” Janes International Defense Review, January 2013, 10.

[202] Royal Canadian Navy, “The Fleet,” accessed on 18 February 2013, http://www.navy.forces.gc.ca/cms/1/1-a2_eng.asp.

[203] Department of National Defence. Securing Canada’s Ocean Frontiers…, 36.

[204] Damian Gayle, “U.S. Navy 'stealth drone' takes to the sea for tests: The autonomous X-47B is hoped to be first carrier-borne unmanned aircraft,” Daily Mail Online accessed on 18 February 2013, http://www.dailymail.co.uk/sciencetech/article-2240394/X-47B-stealth-drone-hoped-carrier-borne-unmanned-aircraft.html.

the use of unpiloted aerial vehicles (UAV) and robots in Iraq.[205] Described by some as the dawn of transhuman warfare, robot mules, remote manipulators and unmanned combat aerial vehicles (UCAV) have replaced both soldiers and pilots for specific tasks in Afghanistan.[206] While these systems are costly, they can exceed some human capacities for performance and endurance and a nation does not become outraged when one is destroyed by the enemy. The use of UAVs shifted from reconnaissance and surveillance to laser target designation to target engagement with hellfire missiles. No great leap is required to imagine a variety of UCAVs programmed to fly a fixed flight pattern high above a battle space waiting to detect and destroy an adversary UAV. The evolution from UAVs to UCAVs was sufficiently quick that Anti-UAV UCAVs may not be far off.

The use of automated systems has been common practice for many years with the operation of commercial airliner.[207] Autopilots control the aircraft for the majority of the flight and can safely execute landings.[208] Pilots demonstrate their indispensability when abnormal situations arise such as when Captain Chesley "Sully" Sullenberger executed an emergency landing into the Hudson River after his Airbus A320 collided with a flock of geese in 2009. Sullenberger stated that computer-assisted flight systems were active during the landing but the “flight software prevented him from keeping the plane's nose a

[205] Defense Update “PackBot Tactical Robot,” accessed on 18 February 2013, http://www.defense-update.com/products/p/pacbot.htm.

[206] David Axe, “One in 50 Troops in Afghanistan Is a Robot,” Wired, accessed on 19 February 2013, http://www.wired.com/dangerroom/2011/02/1-in-50-troops-robots/.

[207] Stephen Pope, “FAA Encourages Pilots To Hand Fly More,” Flyingmag.com accessed on 20 February 2013, http://www.flyingmag.com/news/faa-encourages-pilots-hand-fly-more.

[208] Thom Patterson, “Who's really flying the plane?” CNN.com accessed on 20 February 2013, http://www.cnn.com/2012/03/24/travel/autopilot-airlines.

little higher during the last four seconds before he ditched"[209] resulting in a harder impact. The combination of flight control systems, software and digital instruments results in a system so complex that unanticipated errors can occur from a myriad of sources.[210] Conceivably, it would be possible for a technically savvy adversary to alter the software that reads the compass or GPS or the lines of code that govern the direction of the flight control surfaces.[211] Hugo Teso, a security consultant, claims to have created a smartphone app that could alter the operating system of a commercial airliner.[212] This could provoke a crash just as lethal as any missile. One could readily argue that a pilot would notice that the plane was not following the expected flight path and therefore assume full manual control. What happens if there is no pilot? UAVs are being adopted for a variety of uses in the United States. Border and customs services and police forces are interested in using systems such as the Predator drones for area surveillance. Predators are already authorized for use in the airspace above North Dakota.[213]

A UAV infected with malicious code could become the next weapon to duplicate the attacks of September 11, 2011. The Predator drone weighs a fraction of the weight and fuel carried by the Boeing 757 and 767 used by terrorists against the twin towers of the World Trade Centre. Nonetheless, the 1000 kilogram drone and flying at 200

[209] Thom Patterson, "Who's really flying the plane?"…

[210] M. Sghairi, A. de Bonneval, Y. Crouzet, J.-J. Aubert and P. Brot, "Challenges in Building Fault -Tolerant Flight Control System for a Civil Aircraft," International Journal of Computer Science, Vol 35 issue 4 accessed on 20 February 2013, http://www.iaeng.org/IJCS/issues_v35/issue_4/IJCS_35_4_07.pdf.

[211] Iran claims to have taken control of a RQ-170 Sentinel in this manner. See AviationIntel accessed on 19 April 2013, http://aviationintel.com/2011/12/16/iran-says-it-spoofed-the-rq-170-sentinel-into-thinking-it-was-home-others-say-it-was-captured-in-afghanistan/.

[212] Andy Johnson, "Disturbing app could let hackers take control, crash planes," CTV News accessed on 19 April 2013, http://www.ctvnews.ca/sci-tech/disturbing-app-could-let-hackers-take-control-crash-planes-1.1235093.

[213] RT, "Domestic drone justice: US court green-lights police UAV use," RT.com accessed on 20 February 2013, http://rt.com/usa/domestic-drone-court-ruling-743/.

kilometers per hour could do serious damage against a soft target like a commercial building or a sports stadium full of spectators.[214]

The introduction of robotic swarm technology could amplify the opportunity for cyber warriors. Researchers from Brussels have demonstrated technology permitting flying drones and robots to collaborate in a variety of tasks.[215] Swarm technology demonstrated by researchers at Boeing and the John Hopkins University[216] allow UAVs to cooperate via data interlinks. This technology would be useful for police to monitor large areas. Without the benefits of swarm data interlinks there would be task duplication and more potential for mid-air collisions. However, the level of data exchange required to collaborate creates an opportunity to distribute malicious code to each of the UAVs in a group. Rather than directing one single UAV to crash into a target, an adversary could crash every UAV in a swarm after the first one is infected with malicious code. Several UAVs crashed into a power plant, fuel refinery or airport could have serious consequences.[217]

[214] US Airforce, “MQ-1B Predator,” accessed on 20 February 2013, http://www.af.mil/information/factsheets/factsheet.asp?fsID=122.

[215] John Biggs, “Watch A Swarm Of Robots Team Up With Flying Drones To Solve Real-World Problems,” Tech Crunch accessed on 20 February 2013, http://techcrunch.com/2012/10/24/watch-a-swarm-of-robots-team-up-with-flying-drones-to-solve-real-world-problems/.

[216] Skyler Frink, “UAV swarm technology emerges to perform varied applications,” accessed on 21 February 2013, http://www.militaryaerospace.com/blogs/aerospace-defense-blog/2012/08/uav-swarm-technology-emerges-to-perform-varied-applications.html.

[217] Many countries have listed infrastructure that they consider vital to the preservation of normal activity. Terrorists may want to attack these targets referred to as critical infrastructure because the damage will be greater than other potential targets. Department of Homeland Security, “Critical Infrastructure Protection and Resilience Month 2012,” accessed on 21 February 2013, http://www.dhs.gov/cipr-month-2012.

Equipment manufacturers and operators are quick to endorse the safety of UAVs, auto pilots and weapon systems.[218] Ronald Arkin, a roboticist at the Georgia Institute of Technology has suggested that autonomous technological systems can safely be assigned highly complex tasks. Chief among the list of multifaceted challenges is the application of rules of engagement. Professional soldiers are taught the foundation of the Geneva Convention and Just War tradition so they can make ethical shoot and don't shoot decisions. Arkin is "convinced that they [autonomous systems] can perform more ethically than human soldiers are capable of."[219] Yet Dr Paul Mitchell, Professor of Defence Studies at the CAF College, makes a convincing case that the "ethical governor" described by Arkin is a distant possibility, possibly unachievable and perhaps undesirable in application to warfare.[220]

Frequently, the presence of a human is listed as the last line of reason in a multi-tiered safety sequence. If all the technology fails, the pilot or system operator can assume control and make the proper decision. Robert Quinn, vice president of Foster-Miller which manufactures the weapon carrying robot named SWORDS, describes the human in the loop as a "line in the sand."[221] Noah Shachtman, editor of the national security blog of *Wired* magazine, named the *Danger Room*, believes that people from the military

[218] Ronald C. Arkin, "Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture," U.S. Army Research Office, Technical Report GIT-GVU-07-11, 7.

[219] *Ibid*.

[220] Paul T. Mitchell, ""Three Laws Safe?" Autonomous Robots and Warfare," Canadianmilitaryhistory.ca, 15 October 2012, accessed on 21 February 2013, http://www.canadianmilitaryhistory.ca/three-laws-safe-autonomous-robots-and-warfare-by-dr-paul-t-mitchell/.

[221] P. W. Singer, *Wired for War…*, 124.

technology field state the “person in the loop” mantra in order to keep people calm about the idea of autonomous weapon systems.[222]

There are three principle flaws with the “human in the loop” argument. The first defect is that system autonomy is a central feature in advanced weapon systems because they eliminate the limitations of humans. The missiles designed to strike war ships or military aircraft approach so quickly that a human would be incapable of responding to multiple, simultaneous threats. When placed in their autonomous mode of operation, the Phalanx will fire at incoming objects that fail to broadcast the recognized “friendly” signal. Similarly, chaff or flairs can be fired automatically when aircraft counter measure systems detect a missile. The Army Active Protection System applies similar technology to US Army vehicles in use in high threat environments like Iraq and Afghanistan.[223] A missile counter measures system that relied on human input after sounding an alarm could not offer the same level of protection. The second flaw is that in some cases the purpose of installing the automated system is to reduce the need for humans. In non-critical work like assembly lines, automated systems have replaced many workers.[224] Autopilots have not yet reduced the requirement for airline pilots but they do reduce crew fatigue.[225] Finally, the third flaw is best articulated by ancient Romans: “To err is human.”[226] Recalling that it is the Captain of the USS Vincennes who ultimately gave the

[222] P. W. Singer, *Wired for War…*, 124.

[223] Global Security, “IAAPS - Integrated Army Active Protection System.” Accessed on 22 February 2013, http://www.globalsecurity.org/military/systems/ground/iaaps.htm.

[224] Mats Kaarbo, “Will Automation Lead to Economic Collapse,” accessed on 23 February 2013, http://www.ted.com/conversations/13603/will_automation_lead_to_econom.html.

[225] Anupam Agarwal, “A comprehensive review of problems associated with long duration flying and some suggested remedies,” Ind J Aerospace Med 52(2), 2008, 24.

[226] “To err is human” is an older saying found in the works of Seneca and others dating back at least to Roman times. See: http://www.goodreads.com/quotes/244523-errare-humanum-est-sed-perseverare-diabolicum-to-err-is-human.

order to fire on the Iranian airliner; people make mistakes. The formal investigation report from the incident includes a letter from the Chairman, Joint Chiefs of Staff to the Secretary of Defense where he writes the "[uncertainties and conflicting information] are the realities of combat and the commanding officer, if he is to function effectively, must be given some latitude to deal with them."[227] The report also states that "the AEGIS system itself, it [sic] performed as designed and subsequent analysis indicated that the sensor data collected was accurate."[228]

People are particularly prone to error when they are influenced by incorrect data and the manipulation of data is where cyber warriors can excel. Paul Rosenzweig, author of *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*, explains that the ubiquity of cyberspace and pervasiveness of information technology has a fundamental impact on how we conduct business, protect national interests and establish common defence.[229] Even if a human is kept in the loop, our reliance on data constitutes a vulnerability that cyber warriors can exploit.

LEGITIMATE TARGETS

The current variety of publicly acknowledged threats covers a wide spectrum. China has been accused by Mandiant, an information technology security company, of sponsoring the theft of intellectual property since 2006.[230] The categories of the sectors compromised by malware and highlighted in Mandiant's report of January 2013 include

[227] United States of America Department of Defense, *Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988*, 1988, 6.

[228] *Ibid*.,.7

[229] Paul Rosenzweig, "Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World," New York Praeger Press 2013, Chap 1.

[230] Mandiant, *APT1- Exposing One of China's Cyber Espionage Units* (n.p.: Mandiant, 2013) 20.

technology, energy, resources, banking and public administration. If true, this scale of state sponsored industrial espionage could have considerable economic and security consequences.[231] However, state level espionage is far from new. Sun Tzu emphasized the advantages that came with knowledge and described several categories and techniques for employing spies.[232] Notwithstanding the advantages that may occasionally come from accurate intelligence, Clausewitz would insist that espionage is not a form of warfare.[233]

The distributed denial of service (DDoS) attacks that paralyzed Estonian government, media and financial services in April 2007 have been referred to by some as Web War 1.[234] This variety of attack pools geographically distributed computer resources belonging to private, corporate and/or state interests and directs them to request service from a specific internet address. The corresponding server can be overwhelmed by an excessive demand brought to bear on it. In the case of Estonia, the power of thousands of computers, known as zombies or bots once infected with malware was sequentially directed to specific vulnerabilities in Estonian Information Technology infrastructure.[235] DDoS attacks are considered rudimentary by cyber security experts.[236] Botnets are

[231] The SecDev Group, *Canada and Cyberspace 2012: Key Issues and Challenges for DFAIT*, 26 October 2011, i.

[232] Sun Tzu and Lionel Giles, *The Art of War*. Internet Classics Archive: 1994. VI. 25.

[233] See Clausewitz, Carl von, Charles Keller, and David Widger, *On War*. Gutenberg EBook, 2006, 21/27. Also Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies, vol 35, no 1, 5–32, February 2012.

[234] Matt Murphy, "War in the fifth domain," The Economist, Last Accessed on 19 December 2012, http://www.economist.com/node/16478792.

[235] Mark Lander and John Markoff, Digital Fears Emerge After Data Siege in Estonia, Last accessed on 19 December 2012, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0.

[236] Adam Samson, "Three Bank Websites Threatened in Ongoing Cyber 'Operation'," accessed on 24 February 2013, http://www.foxbusiness.com/industries/2012/10/08/three-bank-websites-threatened-in-ongoing-cyber-operation/.

available for anyone to hire from the criminals who control them.[237] These attacks can make services temporarily unavailable but customer and other data is generally not at risk and service is quickly restored following the event. The attacks can be defused by increasing the server capacity or filtering the incoming requests. Officials from this technically advanced Baltic state labelled the crippling attacks an act of war. However, the damage was essentially limited to a loss of business in the amount of €10 million for the country's main bank and possibly a loss of public confidence.[238]

The vulnerability of public infrastructure has been demonstrated in other, more destructive ways. In 2002 the Washington Post reported that a hacker had accessed the control systems of the Roosevelt Dam in Arizona.[239] While there is debate regarding the damage that the hacker could have done in this case,[240] the spillway is capable of releasing 4,200 cubic meters of water each second. In one test experts have also effectively demonstrated the ability to physically damage hydro-electric generators through cyber-attacks.[241] In another example from 2000, Vitek Boden, a disgruntled and former employee from the water and sewage treatment plant of Queensland, Australia hacked the control system and dumped putrid sludge into the area's rivers over a two

[237] Joan Goodchild, "Digital black market offers cheap botnets for hire, stolen credit card info," CSO, accessed on 25 February 2013, http://www.csoonline.com/article/657159/digital-black-market-offers-cheap-botnets-for-hire-stolen-credit-card-info.

[238] Ethan Lindsey, "Cost of 'Web War I': 10 Million Euros," Last Accessed on 19 December 2012, http://www.thenewnewinternet.com/2010/12/08/cost-of-web-war-i-10-million-euros/.

[239] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," WashingtonPost.com, June 27, 2002, Last Accessed on 19 December 2012, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

[240] Robert Lemos, "Cyberterrorism: The real risk," Last Accessed on 19 December 2012,http://www.crime-research.org/library/Robert1.htm.

[241] Richard Clarke, William Barnes and Robert Knake,Cyber War: The Next Threat to National Security and what to do about it(Harper Collins e-books, 2010), Chap Three 59 of 61.

month period.[242] There is some evidence that Al Qaeda has been interested in the control software used by the digital switches that run communications, transportation, water and power grids.[243]

While terrorists may want to target smart power grids and water supplies these may prove to be unlikely targets for war against a conventional adversary. Assuming that the criteria for *jus ad bellum* are present, *jus in bello,* the laws of armed conflict, do not change in cyber space. The principles of discrimination between civilians and combatants, minimization of suffering and proportionality when attacking are no less applicable to cyber war.[244] Therefore, a state that recognizes the Geneva Convention would not apply a cyber strategy that targets a predominantly civilian population. It is interesting to consider that in 2012 the United Nations declared internet access to be a basic human right for the freedom of expression that it facilitates.[245] Military targeting boards in future conflicts may decide that telecommunications and internet infrastructure are to be protected from collateral damage just as water and food supplies are protected today.[246]

[242] Court of Appeal of the Supreme Court of Queensland, "R v Boden, QCA 164," (Australia: 2002)

[243] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared…

[244] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: University Press, 2012), 280.

[245] United Nations, "Internet Freedom: Law and Regulation," UNESCO accessed on 25 February 2013, http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-expression-on-the-internet/internet-freedom-law-and-regulation/.

[246] United Nations, "Universal Declaration of Human Rights," Article 25, accessed on 25 February 2013, http://www.un.org/en/documents/udhr/index.shtml.

Stuxnet was a far more sophisticated example of a state sponsored cyber weapon.[247] The designers of this malware employed four distinct system vulnerabilities, including the first documented Siemens Programmable Logic Controller (PLC) to maximize the opportunities for success.[248] The result was a highly discriminating computer worm that caused uranium centrifuges to fail at the Natanz nuclear enrichment facility. American and European IT security experts described *Stuxnet* as "far more complex — and ingenious — than anything they had imagined."[249] Mr. Langner, head of a small IT security company, examined the worm and compared it to a marksman's shot.[250] The malware lay dormant until it detected the precise configuration of the Natanz centrifuges. Once activated, it accelerated the centrifuges until they self-destructed while sending a false indication that the systems were running properly. Analysts from Symantec stated that "Stuxnet has highlighted direct-attack attempts on critical infrastructure are possible and *not just theory or movie plotlines* [emphasis added]."[251]

Decision makers and others who are not deployed to the conflict zone need to recognize that they could be personally exposed to cyber-attacks. Robert Ford has the unfortunate distinction of being the first person killed by a robot on 25 January 1979.[252] The future holds possibilities much more sinister than that unfortunate industrial accident.

[247] Paul Wagenseil, "Obama, Bush Behind Stuxnet Worm, Report Says," Technewsdaily.com, June 01 2012, accessed on 25 February 2013, http://www.technewsdaily.com/7824-obama-bush-stuxnet-report.html.

[248] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec, February 2011 accessed on 25 February 2013, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[249] William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear DelayJanuary," nytimes.com accessed on 25 February 2013, 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all&.

[250] *Ibid*.

[251] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier…

[252] P. W. Singer, Wired for War…, 195.

The laws of armed conflict require attacks to distinguish between military objectives and civilians or civilian infrastructure.[253] Key leaders can be legitimate military targets even if they are civilians. Likewise, the operators of UAVs may feel that they are not exposed to risk because they are 7000 miles away from where their Reaper drones are flying and where their missiles are being fired at targets.[254] As discussed in chapter 2, distances in cyberspace are not measured the way they are in the land and air domains. A technically savvy adversary may begin targeting individuals or groups who are currently not being threatened. The laws of armed conflict might be permissive to facilitate this targeting through cyber-attacks. Future cyber warriors may themselves be attacked by their equivalents from an adversary state.

Vulnerabilities can be found in many systems that people rely on for safety and convenience. Most smart phones sold today are capable of identifying their position so the user can be provided with maps and navigation assistance. That same technology can allow an outsider to know where they are. Some will insist that this data is protected and unavailable to potential adversaries. Unfortunately, many apps, like *Angry Birds* and *Dictionary.com* track the locations of the devices they are installed on so that data may be available to many unexpected people.[255] A smart phone cannot kill its owner but knowing the owner's location can make the task much easier for the adversary.

[253] Geneva Academy, "International humanitarian law," accessed on 26 February 2013, http://www.geneva-academy.ch/RULAC/international_humanitarian_law.php.

[254] Elizabeth Bumiller, "A Day Job Waiting for a Kill Shot a World Away," New York Times, 29 July 2012, accessed on 27 February 2013, http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all&_r=0.

[255] Peter Greenberg, "Surprise Location-Tracking Apps & Your Digital Security," accessed on 26 February 2013, http://www.petergreenberg.com/2013/02/11/surprise-location-tracking-apps-your-digital-security/.

Automobiles could become a weapon in numerous ways. The OnStar service offered by General Motors permits remote operation of door locks, speed and position tracking, and can disable a vehicle.[256] If an adversary wanted to target a driver or passenger these tools could be used to stop the vehicle where they were waiting to attack it. Perhaps they could cause an accident by deploying an air bag or activating the breaks when the vehicle is at speed and in a curve. McAfee, a well established IT Security company, has cautioned that the trend of enabling modern cars with programmable logic controllers introduces such risks.[257] PLCs are the devices that personalize seat and mirror positions, entertainment system settings and other customizations when a specific driver is identified by the RFID tag imbedded in their key. Researchers from the University of California and the University of Washington have demonstrated that vehicle safety systems can readily be hacked when they were permitted access to the vehicle interior. Such an act could leave a logic bomb that would jeopardize the safety of vehicle occupants at a later date. These researchers also demonstrated that some vehicle systems could be accessed through Bluetooth. Researchers from Rutgers and the University of South Carolina demonstrated that the wireless link from tire pressure monitoring systems could also be compromised from a distance. Suspension of disbelief may be required to imagine a threat from tire pressure monitors but a compromised Bluetooth entertainment system could permit an adversary to listen to the sensitive conversations occurring inside a vehicle. Google is currently testing self-driving cars and both Nevada and California

[256] OnStar, “Remote Services,” accessed on 26 February 2013, https://www.onstar.com/web/portal/securityexplore?tab=1.

[257] Stuart McClure, “Caution: Malware Ahead-An analysis of emerging risks in automotive system security,” accessed on 26 February 2013, http://www.mcafee.com/us/resources/reports/rp-caution-malware-ahead.pdf.

have passed laws permitting driverless vehicles on their roads.[258] Even if the production model car with the self-drive feature is years away there are several manufacturers currently including self-parking technology in their cars.[259] That means the throttle, transmission, steering and break are already being controlled by PLCs. Professor Christof Paar from the University of Massachusetts recognizes these threats and stated that “most people would rather have malicious software running on their laptop than inside their car braking system.”[260]

The ubiquity of smartphones may be an indicator of humanity’s path toward a Borg-like future complete with its vulnerabilities. In the movie Star Trek: First Contact, the Borg are a cybernetically enhanced group of humanoids interconnected by technology. Star Trek fans may recall that the Borg were also vulnerable to a virus that Icheb was to carry to the Collective.[261] Many people are similarly connected by the tweets, Facebook and Foursquare updates from contacts that are delivered instantly to their smartphone. These devices may soon be replaced by computers worn on the wrist, not much bigger than a watch.[262] Google and Vuzix have produced miniature computers

[258] Heather Kelly, “Self-driving cars now legal in California,” CNN, Tue October 30, 2012, accessed on 26 February 2013, http://www.cnn.com/2012/09/25/tech/innovation/self-driving-car-california.

[259] Ford, Lexus, Lincoln, Mercury and Toyota were offering the self parking feature on nine different 2010 models. See Lee Hawkins, “The Skinny on Self-Parking,” The Wall Street Journal, 18 March 2010. Accessed on 26 February 2013, http://online.wsj.com/article/SB10001424052748703734504575125883649914708.html

[260] Stuart McClure, “Caution: Malware Ahead…, 9.

[261] Star Trek: Voyager Episode 139 “Child’s Play” 19th episode of the sixth season.

[262] Donald Melanson and Michael Gorman, “Our augmented selves: The promise of wearable computing,” Engadget, 21 December, 2012, accessed on 27 February 2013, http://www.engadget.com/2012/12/21/our-augmented-selves-the-promise-of-wearable-computing/.

with displays that are worn like a pair of glasses.[263] All of these devices have the potential to be compromised through their WiFi, Bluetooth or GSM wireless links.

People are also benefitting from life-saving or enhancing technology in the form of insulin injectors, pacemakers, neuro-stimulators and retinal prosthesis.[264] This technology referred to as implantable medical devices (IMD) call for monitoring and occasional recalibration. Normally these services are performed in a doctor's office but some manufacturers have included IP addresses in their IMDs to permit remote monitoring for patients in isolated areas.[265] Benjamin Jun, Chief Technical Officer of Research Cryptography in San Francisco believes it is risky to connect these devices to the Internet.[266] Researchers from Harvard School of Medicine have demonstrated that Internet enabled pacemakers are vulnerable to malicious code.[267] The attack is similar to updating the firmware on a mobile phone. Researchers have also demonstrated that the insulin system worn by hundreds of thousands of diabetics is vulnerable to cyber-attack.[268] Defenders of the technology argue that the risk is minimized by the proprietary nature of IMD communication protocols and that each device possesses a unique identifier. They suggest it would be extremely difficult for an outsider to learn the IP address of a specific person's pacemaker. This author believes that some nations will be

[263] Sam Biddle, "Vuzix M100 Hands-On: Google Glass' First Real Competitor Sucks," Gizmodo, 6 January 2013 accessed on 27 February 2013, http://gizmodo.com/wearable-computers/.

[264] Implantable Devices, implantable device.com, accessed on 5 March 2013, http://www.implantable-device.com/.

[265] Robert Vamosi, *When Gadgets Betray Us – The Dark Side of Our Infatuation With New Technologies* (New York: Basic Books, 2011), 38.

[266] *Ibid*.

[267] *Ibid*., 41.

[268] Nidhi Subbaraman, "Next health hazard: Hackable medical implants," NBCNews.com, 27 February 2013 accessed on same day, http://www.nbcnews.com/technology/technolog/next-health-hazard-hackable-medical-implants-122796#/technology/technolog/next-health-hazard-hackable-medical-implants-122796.

very interested in knowing if an adversary state leader has an IMD. This data could potentially be obtained from the medical records at the doctor's office, the implant manufacturer's records or perhaps from the Health Information System to be implemented by Health Canada.[269] If any of these databases is hacked heads of state, military commanders or simple UAV pilots with IMDs could drop dead on the first day of an armed conflict through malware added by an adversary.

Just how far the cyber-medical threat extends is difficult to judge at this point in time. Engineers from Brown University announced their creation of an IMD capable of detecting brain activity. Described as "a significant advance for brain-machine interfaces,"[270] the device is fully implantable and designed to relay the signals from up to 100 neurons and transmit them via a wireless broadband signal. Several of these devices have been working in animal test subjects for more than one year. Arto Nurmikko, professor of engineering at Brown University and supervisor for the project stated the device "has features that are somewhat akin to a cell phone, except the conversation that is being sent out is the brain talking wirelessly."[271] Tim Hemmes has personally tested similar technology with Researchers at the University of Pittsburgh School of Medicine.[272] Hemmes sustained a spinal cord injury seven years ago that left him unable to move his body below the shoulders. Using brain-computer interface technology,

[269] Health Canada, "What We Do," accessed on 5 March 2013, https://www.infoway-inforoute.ca/index.php/about-infoway/what-we-do.

[270] David Prutchi, "Brown University Develops Fully-Implantable Brain-Computer Interface," March 1, 2013 accessed on 4 March 2013, http://www.implantable-device.com/2013/03/01/brown-university-develops-fully-implantable-brain-computer-interface/#more-1695.

[271] David Prutchi, "Brown University Develops Fully-Implantable…

[272] Science Daily, "Paralyzed Man Uses Thoughts Alone to Control Robot Arm, Touch Friend's Hand, After Seven Years," accessed on 4 March 2013, http://www.sciencedaily.com/releases/2013/02/130208124818.htm.

Hemmes was first taught to control a computer cursor and then how to manipulate a robotic arm developed by Johns Hopkins University's Applied Physics Laboratory. Clearly this technology could provide disabled people with renewed quality of life and possibly independence. It is unclear how much thought the researchers have given to securing the signals between the brain implants and the prosthetic robot limbs. It is likely that someone could assume control over the limbs by transmitting a signal more powerful than the one coming from the brain implant. This would not be difficult considering the low power available from the small, rechargeable batteries used to power IMDs.[273] The highly speculative question that some may pose is if the brain implant can be hacked in the opposite way. Will future cyber-warriors be able to create a Manchurian Candidate from an individual augmented with a cerebral IMD?[274]

SUMMARY

The technology that cyber space is made from creates a shadowy realm that is difficult for many to understand. The faithful assume that engineers and programmers have taken the steps necessary to keep us all safe. The wary recognize that complex systems can contain unexpected vulnerabilities that threaten technologically dependant societies.

The mass production and miniaturization of computers has thrust them into our pockets, our automobiles and, for some, into our bodies. The conveniences they offer have made them so popular as to be inescapable for the average person. This new domain

[273] Implantable Device, “Power Sources,” accessed on 4 March 2013, http://www.implantable-device.com/category/implantable-components/power-sources/.

[274] In the novel *The Manchurian Candidate,* Richard Condon suggested a person could be brainwashed into assassinating a political leader on command, 1959, McGraw-Hill.

is employed by many and understood by few. Our adversaries are likely to recognize that this time of change offers many opportunities.

Cyber threats ultimately lead back to the same source that the ancients faced. Adversary states can be cunning, imaginative and resourceful. Some adversaries are prepared to study our society and technology to locate the vulnerabilities. As indicated in chapter 2, adversary states may even be supplying that technology. However, as demonstrated by the USS Vincennes example, sometimes the vulnerability is the person who controls the switch. The techniques of misinformation have changed since Sun Tzu authored his laws of war but the aim is the same. We become so accustomed to trusting the information presented on our digital displays that we are susceptible to being misled by them. Our adversary can exploit that tendency.

The essential characteristic of cyberspace that must be understood is that the complexity of the system creates the possibility for numerous vulnerabilities. The architects building cyberspace have not and perhaps cannot anticipate all the possibilities when adding to this domain. Adversaries may choose to study and identify the exploitable aspects of cyberspace that permeates first World nations. The ubiquity of cyberspace throughout private, corporate and government environments presents military opportunities that may be difficult for adversaries to ignore. A prudent nation would partner government resources with corporate concerns to identify and mitigate the vulnerabilities that are found.

CONCLUSION

The traditional domains of warfare evolved as technological innovations introduced new ways for people and nations to exert physical force against each other. Cyberspace is the newest environment to support human interaction and it is pertinent to examine its recent acceptance as a domain of military operations.

The different environmental influences in the physical domains have compelled dissimilarities in the manner in which land, sea, air and space power is applied to achieve military effects. However there are also consistencies in the doctrine that applies to each domain. Each of the domains possessed a dimensional quality that military forces seek to control. The nature of that control can be limited in scope or duration but the common purpose is to establish freedom of action for friendly forces and deny the same to the adversary. Military operations in any of the established domains can create effects in the other domains. Lastly, the operational functions of Command, Sense, Act, Shield and Sustain can be conducted in each domain.

There are many examples of cyber-attacks that could contribute to military operations. The collection of information from Trojans supports the intelligence gathering process. The Distributed Denial of Service Attacks inflicted on Estonia in 2007 can be repeated to paralyze an adversary. Malware like Stuxnet could be used to deny the use of crucial systems, vehicles with automated control systems or even target key persons in a variety of ways.

However, cyberspace is missing several attributes resident in the physical domains. First, the virtual World is an impermanent environment. Hardware and software changes can occur at any time from the actions of friendly, adversary, commercial and other actors. The absence of dimensions or boundaries in cyberspace invites fratricide. The volatility of the environmental landscape is an obstacle to military planning and calls for a centralized command and centralized execution operational approach which does not apply to land, sea, air or space power. It may not be possible to establish control of the cyber environment it the way it is understood in the physical World. The success of malware and network infiltration depends greatly on stealth which creates an attribution problem for the conduct of military operations. Finally, the cyber environment fails to offer an undisputed form of armed attack.

The current threats and future possibilities offered by the virtual World are a compelling incentive for investment in cyber capabilities. The Mandiant Report suggests Canadian economic and security interests are vulnerable to cyber threats. Clearly there is sufficient cause to investigate the requirement for and develop national defensive cyber capabilities. It is also likely that an offensive cyber capability could contribute to future military operations and national security objectives. However, Cyberspace does not warrant the full domain status that is doctrinally consistent in the four physical domains of military operations.

BIBLIOGRAPHY

Agarwal, Anupam. “A comprehensive review of problems associated with long duration flying and some suggested remedies.” Ind J Aerospace Med 52(2), 2008, 21 to 26.

Alberts, David et al. *Understanding Information Age Warfare*. n.p.:Ccrp Publication Series, 2001.

AluKd. “First Nikon Firmware Hack Out: Limitless (kinda) Video.” DP Review.com, accessed on 7 April 2013. http://forums.dpreview.com/forums/post/41094074.

Anderson, Nate. “Confirmed: US and Israel created Stuxnet, lost control of it.” accessed on 6 April 2013, http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

Apple iPhone School. “What is Jailbreaking?.” Appleiphoneschool.com. accessed on 7 April 2013. http://www.appleiphoneschool.com/what-is-jailbreaking/.

Ariane B. “3D Virtual Worlds.” accessed on 3 April 2013. http://arianeb.com/more3DWorlds.htm.

Arkin, Ronald C. “Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture.” U.S. Army Research Office, Technical Report GIT-GVU-07-11.

Arthur, Charles. “China's Huawei and ZTE pose national security threat, says US committee.” accessed on 7 April 2013. http://www.guardian.co.uk/technology/2012/oct/08/china-huawei-zte-security-threat.

Associated Press. “Malware infecting PCs on production line, Microsoft says.” http://www.cbc.ca/news/technology/story/2012/09/13/tech-ap-malware-microsoft.html.

Associated Press. “U.S., Canada decline to sign UN telecoms treaty.” accessed on 13 January 2013, http://www.cbc.ca/news/World/story/2012/12/13/un-us-internet.html.

Australia. Court of Appeal of the Supreme Court of Queensland, “R v Boden, QCA 164,” (Australia: 2002).

Axe, David. “One in 50 Troops in Afghanistan Is a Robot.” Wired. accessed on 19 February 2013. http://www.wired.com/dangerroom/2011/02/1-in-50-troops-robots/.

Axe, David. “Real U.S. Stealth-Tech Advantage: Its Assembly Lines.” 6 July 2011, Accessed on 6 February 2013, http://www.wired.com/dangerroom/2011/07/stealth-advantage/.

Babad, Michael. “Chinese hackers suspected of raiding Nortel for decade,” The Globe and Mail, Accessed on 19 December 2012. http://www.theglobeandmail.com/report-on-business/top-business-stories/chinese-hackers-suspected-of-raiding-nortel-for-decade/article536443/.

BBC News, Estonia fines man for ‘cyber war,’ Last updated on Friday, 25 January 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm.

Biddle,Sam. “That Internet War Apocalypse Is a Lie.” Gizmodo. accessed on 7 April 2013. http://gizmodo.com/5992652/that-internet-war-apocalypse-is-a-lie.

Biddle, Sam. “Vuzix M100 Hands-On: Google Glass’ First Real Competitor Sucks.” Gizmodo. 6 January 2013 accessed on 27 February 2013. http://gizmodo.com/wearable-computers/.

Biggs, John. “Watch A Swarm Of Robots Team Up With Flying Drones To Solve Real-World Problems.” Tech Crunch accessed on 20 February 2013. http://techcrunch.com/2012/10/24/watch-a-swarm-of-robots-team-up-with-flying-drones-to-solve-real-World-problems/.

Bott, Ed. “The malware numbers game: how many viruses are out there?” ZNet accessed on 5 April 2013. http://www.zdnet.com/blog/bott/the-malware-numbers-game-how-many-viruses-are-out-there/4783.

Broad, William J., John Markoff and David E. Sanger. “Israeli Test on Worm Called Crucial in Iran Nuclear DelayJanuary.” nytimes.com accessed on 25 February 2013. http://www.nytimes.com/2011/01/16/World/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all&.

Brown, Peter J. “Solar Weather Effects on Satellites.” Intelsat accessed on 9 February 2013. http://www.intelsat.com/resources/tech-talk/solar-weather.asp.

Bumiller, Elizabeth. “A Day Job Waiting for a Kill Shot a World Away.” New York Times. 29 July 2012. accessed on 27 February 2013. http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all&_r=0.

Canada. Department of Finance. “Your Tax Dollar: 2010-2011 Fiscal Year.” accessed on 25 January 2013, http://www.fin.gc.ca/tax-impot/2011/html-eng.asp.

Canada. Department of National Defence. B-GA-400-000/FP-000, *Aerospace Doctrine.* Ottawa: DND Canada: 2010.

Canada. Department of National Defence. B-GJ-005-000-FP-001. *Canadian Military Doctrine.* Ottawa: DND Canada, 2011.

Canada. Department of National Defence, B-GJ-005-200-FP-000, *Joint Intelligence Doctrine*. Ottawa: DND Canada, 2003.

Canada. Department of National Defence. B-GJ-300-001/FP-001, *Land Operations* Ottawa: DND Canada: 2008.

Canada. Health Canada. "What We Do," accessed on 5 March 2013, https://www.infoway-inforoute.ca/index.php/about-infoway/what-we-do.

Canada. National Defence. "Projects." accessed on 26 January 2013, http://www.forces.gc.ca/site/pri/2/index-eng.asp.

Canada. Department of National Defence. *Securing Canada's Ocean Frontiers – Charting the Course from Leadmark.* Ottawa: DND Canada, 2005.

Canada. Government of Canada. *Canada's Cyber Security Strategy*. Ottawa: Her Magesty the Queen in Right of Canada, 2010.

Canada. Royal Canadian Air Force, "Air Force History," accessed on 13 January 2013, http://www.rcaf-arc.forces.gc.ca/v2/hst/page-eng.asp?id=526.

Canada. Royal Canadian Navy. "The Fleet," accessed on 18 February 2013, http://www.navy.forces.gc.ca/cms/1/1-a2_eng.asp.

Canadian Wings. "The History of Canada's Air Force," accessed on 13 January 2013, http://www.canadianwings.com/history/beginning.php.

Canan, James. *War in Space.* New York: Harper & Row, 1982.

Cardelli, Luca. "Bad Engineering Properties of Object-Oriented Languages." Digital Equipment Corporation, Systems Research Center, accessed on 2 April 2013, http://lucacardelli.name/Papers/BadPropertiesOfOO.html.

Carr, Jeffrey. "The Myth of the CIA and the Trans-Siberian Pipeline Explosion." accessed on 5 April 2013. http://www.infosecisland.com/blogview/21566-The-Myth-of-the-CIA-and-the-Trans-Siberian-Pipeline-Explosion.html.

Cenciotti, David. "U.S. – Iran war games…24 years ago" (Iran Air Flight 655 shot down by USS Vincennes)." 30 January 2012 accessed on 14 February 2013. http://theaviationist.com/tag/iran-air-flight-655/.

Centruy of Flight. "Aces of World War One." accessed on 8 February 2013, http://www.century-of-flight.net/new%20site/frames/WORLD WAR 1%20aces_frame.htm.

Chessbase News. “Kramnik vs Deep Fritz: Computer wins match by 4:2.” accessed on 24 February 2013, http://www.chessbase.com/newsdetail.asp?newsid=3524.

Clarke, Richard A. and Robert Knake. *Cyber War: The Next Threat to National Security and what to do about it*, Harper Collins e-books, 2010.

Clausewitz, Carl von, Charles Keller, and David Widger,On War.Gutenberg EBook, 2006. http://www.gutenberg.org/files/1946/1946-h/1946-h.htm.

Colter, Aaron. “Can pay-what-you-want downloads save the music industry?” Digital Trends. 14 March 2012, accessed on 6 April 2013. http://www.digitaltrends.com/music/can-pay-what-you-want-downloads-save-the-music-industry/.

Curry, Bill. “Serious Flaws in Ottawa’s Defence Against Cyber Attacks: Auditor General.” accessed on 14 February 2013. http://www.theglobeandmail.com/news/politics/ottawa-notebook/serious-flaws-in-ottawas-defence-against-cyber-attacks-auditor-general/article4630798/.

Cyber Media. “From the Labs: Information Technology.” accessed on 2 April 2013, http://www.technologyreview.in/computing/38506/.

DeBlois, Bruce M. “Beyond the Paths of Heaven - The Emergence of Space Power Thought.” School of Advanced Airpower Studies. September 1999. ix. Accessed on 19 April 2013. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA421934.

Defense Update.“PackBot Tactical Robot.” accessed on 18 February 2013. http://www.defense-update.com/products/p/pacbot.htm.

deGrasse, Neil Tyson. “The Case for Space,” Foreign Affairs, March/April 2012, 22-33.

Dempsey, Amy. “Guelph tech firm accused of making tools to censor Internet abroad now embroiled in controversy with Australian telecom.” June 28, 2012, accessed on 13 January 2013, http://www.thestar.com/news/canada/article/1218965--guelph-tech-firm-accused-of-making-tools-to-censor-internet-abroad-now-embroiled-in-controversy-with-australian-telecom.

de Toqueville, Alexis. *Democracy In America Volume II*. Project Gutenberg: EBook #816, January 21, 2006.

Dignan, Larry. “Why is security usually an afterthought?” accessed on 7 April 2013. http://www.zdnet.com/blog/security/why-is-security-usually-an-afterthought/865.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*, Cambridge: University Press, 2012.

Donaldson, A. B., “Meeting Record and Decision Sheet - PMB 11/12.” Ottawa: NDHQ, 7 June 2012.

Douhet, Giulio translated by Dino Ferrari. *The Command of the Air*. Washington: Air Force History and Museums Program, 1998.

Dutton, Peter, Robert S. Ross and Oystein Tunsjo. *Twenty-First Century Seapower*. New York: Routledge, 2012.

Falliere, Nicolas, Liam O Murchu, and Eric Chien.“W32.Stuxnet Dossier.” Symantec Security Response. February 2011. accessed on 10 February 2013. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Fédération Aéronautique Internationale. “FAI Sporting Code Section 8 – Astronautics.” 2009.

Frink, Skyler. “UAV swarm technology emerges to perform varied applications.” Accessed on 21 February 2013. http://www.militaryaerospace.com/blogs/aerospace-defense-blog/2012/08/uav-swarm-technology-emerges-to-perform-varied-applications.html.

Fruhlinger, Joshua. “95 percent of all returned gadgets still work, Americans don't read manuals.” Engadget accessed on 2 April 2013. http://www.engadget.com/2008/06/03/95-percent-of-all-returned-gadgets-still-work-americans-dont-r/.

Gangale, Thomas. “Who Owns Geostationary Orbit?” 2005. Accessed on 9 February 2013 http://pweb.jps.net/~gangale/opsa/ir/WhoOwnsGeostationaryOrbit.htm

Gayle, Damian. “U.S. Navy 'stealth drone' takes to the sea for tests: The autonomous X-47B is hoped to be first carrier-borne unmanned aircraft.” Daily Mail Online accessed on 18 February 2013. http://www.dailymail.co.uk/sciencetech/article-2240394/X-47B-stealth-drone-hoped-carrier-borne-unmanned-aircraft.html.

Gellman, Barton. “Cyber-Attacks by Al Qaeda Feared.” WashingtonPost.com, June 27, 2002, Accessed on 19 December 2012. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

Geist, Michael. “Is There a There There? Toward Greater Certainty for Internet Jurisdiction.” University of Ottawa Faculty of Law, 2001.

Geneva Academy. “International humanitarian law.” accessed on 26 February 2013. http://www.geneva-academy.ch/RULAC/international_humanitarian_law.php.

Gervis, Robert. *The Meaning of the Nuclear Revolution: Statecraft and the Prospest of Armageddon*, Ithica, NY: Cornell University Press, 1989.

Gibson, William. *Neuromancer.* Ace Books. Jan 2010.

Giles, Jim. "Are States Unleashing the Dogs of War." NewScientist, 16 December 2010, accessed on 13 January 2013, http://www.newscientist.com/article/mg20827915.100-are-states-unleashing-the-dogs-of-cyber-war.html.

Gilmartin, Danee. "Did Pharaohs Get Seasick?: Khufu Boat Museum: Giza, Egypt." 1 March 2010, accessed on 29 January 2013, http://museumchick.com/2010/03/khufu-boat-museum-giza-egypt-felucca.html.

Gladwell, Malcolm. *Outliers: The story of success*. ePenguin, 2008.

Global Security. "IAAPS - Integrated Army Active Protection System." Accessed on 22 February 2013. http://www.globalsecurity.org/military/systems/ground/iaaps.htm.

Global Research. "US-Israeli Stuxnet Cyber-attacks against Iran: "Act of War"." accessed on 5 April 2013. http://www.globalresearch.ca/us-israeli-stuxnet-cyber-attacks-against-iran-act-of-war/5328514.

Goldman, Jeff. "Anonymous Hackers Seek Recognition of DDoS Attacks as Legitimate Form of Protest." accessed on 13 January 2013, http://www.esecurityplanet.com/hackers/anonymous-hackers-seek-recognition-of-ddos-attacks-as-legitimate-form-of-protest.html.

Goodchild, Joan. "Digital black market offers cheap botnets for hire, stolen credit card info." CSO. accessed on 25 February 2013. http://www.csoonline.com/article/657159/digital-black-market-offers-cheap-botnets-for-hire-stolen-credit-card-info.

Gorman, Siobhan and Julian E. Barnes. "Cyber Combat: Act of War," accessed on 7 April 2013. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

Gray, Colin. *The Leverage of Sea Power*, New York: The Free Press, 1992.

Gray, Melissa. "Chinese space debris hits Russian satellite, scientists say." CNN accessed on 19 April 2013. http://www.cnn.com/2013/03/09/tech/satellite-hit.

Greenberg, Peter. "Surprise Location-Tracking Apps & Your Digital Security." accessed on 26 February 2013. http://www.petergreenberg.com/2013/02/11/surprise-location-tracking-apps-your-digital-security/.

Handel, Michael I. *Masters of War: Classical Strategic Thought*. London: Newbury House, 2001.

Haney, Eric L with Brian M. Thomsen. *Beyond Shock and Awe – Warfare in the 21st Century*. New York: Berkley Caliber, 2006.

Hawkins, Lee. "The Skinny on Self-Parking." The Wall Street Journal. 18 March 2010. Accessed on 26 February 2013. http://online.wsj.com/article/SB10001424052748703734504575125883649914708.html.

Heng, Li. "Gadgets used by ancient Chinese spies," ECNS Last Accessd on 19 December 2012. http://www.ecns.cn/feature/2011/12-23/4891.shtml.

Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Journal of Strategic Security, Volume IV Issue 2 2011, 49-60.

Hildinger, Erik. *Warriors of the Steppe: A Military History of Central Asia 500 BC to 1700 AD*. Cambridge, MA: Da Capo Press, 2001.

History of Sky Lantern. accessed on 5 February 2013. http://www.chineseskylantern.com/.

Hughes, Wayne. "Naval Manoeuvre Warfare." Naval War College Review. Vol L. No 3. Summer 1997. 25-49.

Implantable Device. "Power Sources." accessed on 4 March 2013, http://www.implantable-device.com/category/implantable-components/power-sources/.

Johnson, Andy. "Disturbing app could let hackers take control, crash planes." CTV News accessed on 19 April 2013. http://www.ctvnews.ca/sci-tech/disturbing-app-could-let-hackers-take-control-crash-planes-1.1235093.

Juhl, Felix and Borchert, Heiko. "Exploiting the potential of cyber operations." Jane's Defence Weekly 48, no. 26 (June 29, 2011): 22. Military & Government Collection, EBSCOhost (accessed January 24, 2013).

Kaarbo, Mats. "Will Automation Lead to Economic Collapse." accessed on 23 February 2013. http://www.ted.com/conversations/13603/will_automation_lead_to_econom.html.

Kehler, Robert. "Shaping the Joint Fight in Air, Space and Cyberspace," *Joint Force Quarterly*, issue 49, 2nd Quarter 2008.

Kelly, Heather. “Self-driving cars now legal in California.” CNN. 30 October 2012. accessed on 26 February 2013. http://www.cnn.com/2012/09/25/tech/innovation/self-driving-car-california.

Kennedy, Susan. “Common Web Application Vulnerabilities.” accessed on 2 April 2013, http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Pages/Common-Web-Application-Vulnerabilities1.aspx.

Klink, Jonas. “Remote Controls – a Historical Background,” CSE510 Washington University. accessed on 5 April 2013. http://www.cs.washington.edu/education/courses/cse510/05sp/lab1/Lab%201%20Jonas%20Klink.pdf.

Lander, Mark and John Markoff. “Digital Fears Emerge After Data Siege in Estonia.” Last Accessde on 19 December 2012. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0.

Lawrence, Philip.*Preparing for Armageddon A Critique of Western Strategy*. Sussex: Weatsheaf Books Ltd, 1988.

Lee, James G. “Counterspace Operations for Information Dominance.” Paper for master’s degree. School of Advanced Airpower Studies. Air University. Maxwell AFB, Ala., 1996.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff. “Brief History of the Internet.” accessed on 13 January 2013, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Lemos, Robert. “Cyberterrorism: The real risk,” Last Accessed on 19 December 2012. http://www.crime-research.org/library/Robert1.htm.

Libicki, Martin C. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009.

Libicki, Martin C. “Cyberspace is not a Warfighting Domain.” 25 January 2012.

Libicki, Martin C. “The Specter of Non-Obvious Warfare.” Strategic Studies Quarterly, Fall 2012.

Libicki, Martin C. “What Is Information Warfare?” National Defense University. October 1995.

Lindsey, Ethan "Cost of 'Web War I': 10 Million Euros." Last Accessed on 19 December 2012. http://www.thenewnewinternet.com/2010/12/08/cost-of-web-war-i-10-million-euros/.

Long, Tony. "Dec. 31, 1999: Horror or Hype? Y2K Arrives and the World Trembles." Wired.com accessed on 10 February 2013. http://www.wired.com/science/discoveries/news/2007/12/dayintech_1231.

Lonsdale, David J. *The nature of war in the information age: Clausewitzian Future*. Vol. 9. Routledge, 2004.

Lüthje, Boy. "IT and the Changing Social Division of Labor: The Case of Electronics Contract Manufacturing." Draft paper for Conference on Transforming Enterprise, Washington, D.C., January 27-28, 2003.

Mandiant. *APT1- Exposing One of China's Cyber Espionage Units.* n.p.: Mandiant. 2013.

Mann, Martin. "Plain Facts about Fallout Shelters." Popular Science, December 1961, 56-60.

Manzo, Vincent. "Deterrence and Escalation in Cross-domain Operations Where Do Space and Cyberspace Fit?" JFQ, issue 66, 3rd Quarter 2012, 8-14.

Mathers, Lt Col Russell F. "Cyberspace Coercion in Phase 0/1: How to Deter Armed Conflict." US Naval War College. 2007. accessed on 3 April 2013. http://www.dtic.mil/dtic/tr/fulltext/u2/a476693.pdf.

Matrosov, Aleksandr, Eugene Rodionov, David Harley and Juraj Malcho. *Stuxnet Under the Microscope Rev 1.31*, eset, 2011.

McCaffery, Dan. *Battlefields in the Air: Canadians in the Allied Bomber Command*. Toronto: Lorimer, 1995.

McClure, Stuart. "Caution: Malware Ahead-An analysis of emerging risks in automotive system security." accessed on 26 February 2013. http://www.mcafee.com/us/resources/reports/rp-caution-malware-ahead.pdf.

Melanson, Donald and Michael Gorman. "Our augmented selves: The promise of wearable computing." Engadget. 21 December. 2012. accessed on 27 February 2013. http://www.engadget.com/2012/12/21/our-augmented-selves-the-promise-of-wearable-computing/.

Bradley Mitchell. "OSI Model - Open Systems Interconnection model." accessed on 7 April 2013. http://compnetworking.about.com/cs/designosimodel/g/bldef_osi.htm.

Mitchell, Paul T. ""Three Laws Safe?" Autonomous Robots and Warfare." Canadianmilitaryhistory.ca. 15 October 2012. accessed on 21 February 2013. http://www.canadianmilitaryhistory.ca/three-laws-safe-autonomous-robots-and-warfare-by-dr-paul-t-mitchell/.

Moore, H.D. "Whitepaper: Security Flaws in Universal Plug and Play: Unplug, Don't Play." Security Street, accessed on 2 April 2013. https://community.rapid7.com/docs/DOC-2150.

Moyer, Edward. "War-torn Syria sees restoration of Net after two-day outage," CNET Last Accessed on 19 December 2012. http://news.cnet.com/8301-13578_3-57556619-38/war-torn-syria-sees-restoration-of-net-after-two-day-outage/.

Murgesh, Keshav. "Innovation to drive growth in IT." accessed on 6 April 2013, http://www.business-standard.com/article/companies/innovation-to-drive-growth-in-it-113021500085_1.html.

Murphy, Brian. "Canada Joins Western Nations in Rejecting UN Internet Treaty." 14 Dec 2012, accessed on 13 January 2013, http://www.ctvnews.ca/sci-tech/canada-joins-western-nations-in-rejecting-un-internet-treaty-1.1079239.

Murphy, Matt."War in the fifth domain," The Economist, Last Accessed on 19 December 2012. http://www.economist.com/node/16478792.

Murphy, S., T. McDonald, R. Mills, and E. Leigh Armistead. 2010. "An Application of Deception in Cyberspace: Operating System Obfuscation." *Inspec*, EBSCO*host* (accessed January 24, 2013).

Musil, Stephen. "Anonymous declares war on Syrian government," CNET Last Accessed on 19 December 2012. http://news.cnet.com/8301-1009_3-57556333-83/anonymous-declares-war-on-syrian-government-web-sites/.

NASA, "Brief History of Rockets," accessed on 8 February 2013, http://www.grc.nasa.gov/WWW/k-12/TRC/Rockets/history_of_rockets.html.

NASA, "International Space Station," accessed on 6 April 2013, http://www.nasa.gov/mission_pages/station/structure/launch/index.html.

NATO Cooperative Cyber Defence Centre of Excellence. "The Tallinn Manual." Last accessed on 19 December 2012. http://www.ccdcoe.org/249.html.

O'Connell, Robert. *Tide of the Second Horseman: The Birth and Death of War*. Oxford: Oxford University Press, 1995.

Oh, Jeong Wook (Matt). "Recent Java exploitation trends and malware." Black Hat USA 2012 Las Vegas. accessed on 2 April 2013, https://media.blackhat.com/bh-us-

12/Briefings/Oh/BH_US_12_Oh_Recent_Java_Exploitation_Trends_and_Malware_WP.pdf.

OnStar. “Remote Services.” accessed on 26 February 2013. https://www.onstar.com/web/portal/securityexplore?tab=1.

Oregon State University. “Thinking Object Oriented.” accessed on 2 April 2013, http://web.engr.oregonstate.edu/~budd/Books/oopintro2e/info/chap01.pdf.

Parsch, Andreas. “Lockheed Martin UGM-133 Trident II.” accessed on 6 February 2013, http://www.designation-systems.net/dusrm/m-133.html.

Patterson, Thom. “Who's really flying the plane?” CNN.com accessed on 20 February 2013. http://www.cnn.com/2012/03/24/travel/autopilot-airlines.

Phys Org, World's first 'cyber superweapon' attacks China, Last updated on September 30, 2010. Accessed on 31 January 2013, http://phys.org/news205050403.html.

Pope, Stephen. “FAA Encourages Pilots To Hand Fly More.” Flyingmag.com accessed on 20 February 2013. http://www.flyingmag.com/news/faa-encourages-pilots-hand-fly-more.

Prutchi, David. “Brown University Develops Fully-Implantable Brain-Computer Interface.” March 1, 2013 accessed on 4 March 2013. http://www.implantable-device.com/2013/03/01/brown-university-develops-fully-implantable-brain-computer-interface/#more-1695.

Raytheon. “Excalibur Precision Guided Extended Range Artillery Projectile.” accessed on 9 February 2013, http://www.raytheon.com/capabilities/products/excalibur/index.html.

Reynolds, Clark G. *Command of the Sea – The History and Strategy of Maritime Empires Part Two*. Malabar: Robert E. Krieger Publishing Company. 1983.

Rid, Thomas. “Cyber War Will Not Take Place.” Journal of Strategic Studies, vol 35, no 1, 5–32, February 2012.

Romero, Joshua J. “How Many People Have Been In Space?” Scienceline, accessed on 8 February 2013, http://scienceline.org/2007/03/ask-romero-people_in_space/.

Rosenberg, Nathan.“Innovation and Economic Growth,” Stanford University, 2004.

Rosenzweig, Paul. “Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World.” Lawfareblog.com accessed on 24 February

2013. http://www.lawfareblog.com/2013/01/cyber-warfare-how-conflicts-in-cyberspace-are-challenging-america-and-changing-the-World/.

Roskill, S.W. *History of the Second World War, The War at Sea 1939-1945, vol 1: The Defensive*. London: HMSO, 1954.

RT. "Domestic drone justice: US court green-lights police UAV use." RT.com accessed on 20 February 2013. http://rt.com/usa/domestic-drone-court-ruling-743/.

Samson, Adam. "Three Bank Websites Threatened in Ongoing Cyber 'Operation'." accessed on 24 February 2013. http://www.foxbusiness.com/industries/2012/10/08/three-bank-websites-threatened-in-ongoing-cyber-operation/.

Saini, Deepac."How Keyloggers are Used to Hack Any Type of Online Account." accessed on 3 April 2013. http://hackerspirit.blogspot.ca/2012/07/how-keyloggers-are-used-to-hack-any.html.

Science Daily. "Paralyzed Man Uses Thoughts Alone to Control Robot Arm, Touch Friend's Hand, After Seven Years." accessed on 4 March 2013. http://www.sciencedaily.com/releases/2013/02/130208124818.htm.

Scott, Richard. "Go-Ahead for Goalkeeper Update." Janes International Defense Review, January 2013, 10.

Sghairi, M., A. de Bonneval, Y. Crouzet, J.-J. Aubert and P. Brot. "Challenges in Building Fault -Tolerant Flight Control System for a Civil Aircraft." International Journal of Computer Science, Vol 35 issue 4 accessed on 20 February 2013. http://www.iaeng.org/IJCS/issues_v35/issue_4/IJCS_35_4_07.pdf.

Singer, P. W. *Wired for War*. New York: The Penguin Press, 2009.

Sloan, Elinor. "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities." *Canadian Military Journal*: Autumn 2000.

Star Trek: Voyager Episode 139 "Child's Play" 19th episode of the sixth season.

Stiennon, Richard. *Surviving Cyber War*, Plymouth: Government Institutes, 2010.

Subbaraman, Nidhi. "Next health hazard: Hackable medical implants." NBCNews.com. 27 February 2013 accessed on same day. http://www.nbcnews.com/technology/technolog/next-health-hazard-hackable-medical-implants-122796#/technology/technolog/next-health-hazard-hackable-medical-implants-122796.

Sun Tzu and Lionel Giles, *The Art of War*. Internet Classics Archive: 1994.

The Australian. “Security experts admit China stole secret fighter jet plans,” Accessed on 19 December 2012, http://www.theaustralian.com.au/news/World/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154.

The Brookings Institution. “The Costs of the Manhattan Project.” accessed on 22 January 2013 http://www.brookings.edu/about/projects/archive/nucweapons/manhattan.

The Canadian Press. “Blockbuster Canada to close remaining stores.” accessed on 6 April 2013. http://www.cbc.ca/news/business/story/2011/08/31/blockbuster-canada-close.html.

The Froehlich/Kent *Encyclopedia of Telecommunications* vol. 15., New York: Marcel Dekker, 1997. 231-255. Accessed on 5 April 2013. http://www.cert.org/encyc_article/.

The SecDev Group, *Canada and Cyberspace 2012: Key Issues and Challenges for DFAIT*, n.p.: SecDev, 26 October 2011.

Till, Geoffrey, *Seapower – A Guide for the Twenty-First Century*, London: Frank Cass, 2004.

Times of India. “PLA sets up cyber base, assures it's not for war.” 23 July 2010 accessed on 13 January 2013, http://articles.timesofindia.indiatimes.com/2010-07-23/china/28321900_1_cyber-war-cyber-security-base.

Tyson, Neil deGrasse.“The Case for Space,” *Foreign Affairs*, March/April 2012, 22-33.

Tzu, Sun and Lionel Giles, *The Art of War*. Internet Classics Archive: 1994.

United Nations. “Internet Freedom: Law and Regulation.” UNESCO accessed on 25 February 2013. http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-expression-on-the-internet/internet-freedom-law-and-regulation/.

United Nations. “Universal Declaration of Human Rights.” Article 25, accessed on 25 February 2013. http://www.un.org/en/documents/udhr/index.shtml.

United States. Air Force. “MQ-1B PREDATOR.” accessed on 20 February 2013. http://www.af.mil/information/factsheets/factsheet.asp?fsID=122.

United States. Department of Defense. “Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655on 3 July 1988.” Letter CM-1485-88. 18 August 1988. accessed on 14 February 2013. http://www.dod.mil/pubs/foi/International_security_affairs/other/172.pdf.

United States. Department of Defense. *Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988*. 1988.

United States, Department of Defense. *Joint Doctrine for Electronic Warfare* Joint Publication 3-51. Washington: n.p. 2000.

United States. Department of Homeland Security. “Critical Infrastructure Protection and Resilience Month 2012.” accessed on 21 February 2013. http://www.dhs.gov/cipr-month-2012.

United States. Strategic Command. “U.S. Cyber Command.” accessed on 13 January 2013, http://www.stratcom.mil/factsheets/Cyber_Command/.

Vamosi, Robert. *When Gadgets Betray Us – The Dark Side of Our Infatuation With New Technologies.* New York: Basic Books. 2011.

Viner, Jacob. "Power and Plenty as Objectives of Foreign Policy in the Seventeenth and Eighteenth Centuries.” World Politics. Vol. 1. no. 1, October 1948.

Wagenseil, Paul. “Obama, Bush Behind Stuxnet Worm, Report Says.” Technewsdaily.com, 1 June 2012 accessed on 25 February 2013. http://www.technewsdaily.com/7824-obama-bush-stuxnet-report.html.

Wall, David S. “Policing Cybercrimes.” accessed on 3 April 2013. http://www.cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf.

Wautelet, Michel.*Les Cyberconflits - Internet, Autoroutes de l’information et cyberespace: Quelles menaces?*Bruxelles: GRIP, 1998.

Welch, Dylan. “Foreign spies with cyber eyes on our government,” Lase Accessed on 19 December 2012, http://www.smh.com.au/it-pro/government-it/foreign-spies-with-cyber-eyes-on-our-government-20110923-1kpgs.html.

Wells, Herbert George. *The War in the Air*. Project Gutenberg EBook #780. 2008.

Winters, Jeffrey. “Why We Fear the Unknown.” Psychology Today. accessed on 7 April 2013. http://www.psychologytoday.com/articles/200305/why-we-fear-the-unknown.

Wolf, Walter. “21st Centruy EM Domain Capabilities.” The Journal of Electronic Defense. October 2011.

Wylie, J.C. *Military Strategy: A General Theory of Power and Control.* New York: Rutgers. 1967.