National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBERWARFARE – A UNIQUE CHALLENGE FOR THE CANADIAN FORCES

Major L.M. Doyle

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 – MAITRISE EN ÉTUDES DE LA DÉFENSE

CYBERWARFARE – A UNIQUE CHALLENGE FOR THE CANADIAN FORCES

By Major L.M. Doyle
Par le major L.M. Doyle

Word Count: 17 526

Compte de mots : 17 526

TABLE OF CONTENTS

TABLE OF FIGURES

ABSTRACT

The nature of warfare has already changed. The proliferation of information has put a primacy on decision support tools; enabling commanders with timely and accurate information so they can make timely and effective decisions. Cyberwarfare is a relatively new concept and has limited historical examples to study and making it difficult to develop concrete conclusions. However, it is clear that a successful approach to Cyberwarfare will require senior leaders to be creative and to challenge the status quo of traditional military ways of training and conducting operations.

This paper will prove that cyberwarfare is a challenge that cannot necessarily be approached with conventional military processes. The unique nature of cyberwarfare requires leaders to look at the Command and Control, the Force Generation and the Force Employment of cyber forces through an original lens to optimize effects at the tactical, operational and strategic levels. In order to prove this, this paper will first establish that cyberwarfare has led to a Revolution in Military Affairs (RMA) and define the foundation of the RMA. It will then show that this specialized capability is an ideal fit with a decentralized framework and streamlined Command and Control, founded on trust and understanding. It will show that soldiers in the cyber domain will be trained differently and that leaders will need to appreciate this and be versed to certain degree technically. Finally, the paper will compare cyberpower to a range of familiar military capabilities ranging from nuclear weapons to electronic warfare, to see what characteristics are similar and how it should be optimally employed.

INTRODUCTION

Society has changed significantly since the first computers were networked to form the Internet. The ability to rapidly process information has transformed the way we communicate, the way we study and the way we fight. It isn't the first period of change; Murray and Knox identify five revolutions that have changed the face of war.[1] Each change in political climate or technology has had impacts on the nature of warfare. Whether it was the French Revolution that led to the merger of politics and warfare, the Industrial Revolution which lead to mass production and mobility enhancements or the advent of nuclear weapons and the beginning of deterrence, they have all shaped and changed warfare.[2] In an age that is now being defined by information, we should expect nothing else.

The nature of warfare has already changed. The proliferation of information has put a primacy on decision support tools; enabling commanders with timely and accurate information so they can make prompt and effective decisions. Network Centric Warfare is a concept that has gained significant momentum and is based around distributing information and decision making power to speed up the process. Information technology has also influenced war through the media. With the 24/7 news coverage and real-time reporting, war essentially is able to come into an individual's living room during the evening news. Popular support for mounting casualty numbers is difficult to attain, which influences politicians to look for ways to exert their political

---

[1] MacGregor Knox and Williamson Murray, "Thinking about Revolutions in Warfare," in *The Dynamics of Military Revolution, 1300-2050*, eds. MacGregor Knox and Williamson Murray (Cambridge, UK: Cambridge University Press, 2001), 6.

[2] Ibid.

will with minimal risk to soldiers. Attrition warfare appears to be unpalatable to both political leaders and the population creating an opportunity for a military tool like cyberwarfare to fill that void.

Cyberwarfare is a product of the Information Revolution. It can be a weapon that attacks an adversary's decision making process, it can achieve kinetic effects through non-kinetic means and it can enable the conventional methods of warfare. This paper will prove that cyberwarfare is a challenge that cannot necessarily be approached with conventional military processes. The unique nature of cyberwarfare requires leaders to look at the Command and Control, the Force Generation and the Force Employment of cyber forces through an original lens to optimize effects at the tactical, operational and strategic levels. In order to prove this, this paper will first establish that cyberwarfare has led to a Revolution in Military Affairs (RMA) and define the foundation of the RMA. It will then show that this specialized capability is an ideal fit with a decentralized framework and streamlined Command and Control, founded on trust and understanding which is similar to the employment of Special Operations Forces. It will show that soldiers in the cyber domain will be trained differently and that leaders will need to appreciate this and be versed to certain degree technically. Finally, the paper will compare cyberpower to a range of other military capabilities ranging from nuclear weapons to electronic warfare, to see what characteristics are similar and how it should be optimally employed.

Chapter one will be focussed on the RMA that has occurred with the advent of cyberwarfare. This chapter will look at common definitions of cyberwarfare and establish key concepts for the remainder of the paper. It will show how the environment and many of the interactions between organizations is unprecedented and how that has transformed the nature of

warfare. In order to illustrate and provide a concrete example, the deployment of the Stuxnet virus on the Iranian nuclear facility at Natanz will be used as a case study, ultimately proving the RMA.

The second chapter will build on the fact that the nature of war has changed and the military must look at ways to adapt. The military is generally a cumbersome organization that has strong ties to history and tradition and generally changes very slowly. This is not a good ideal for a dynamic environment like cyberspace so this chapter will look at examples in the private sector of successful organizations; particularly investigating theories and companies that have looked to decentralize responsibilities to gain efficiencies. There are similar theories in the military context that will also be studied such as mission command and the employment of cyber forces will be compared that the employment of special operations forces because of some of the similarities that exist between the two capabilities. Ultimately, this chapter will show that cyber forces are optimized to work in a decentralized fashion that is founded on trust. This will make cyber forces efficient and responsive to threats.

Having established the importance of trust in order to optimize the employment of cyber forces, this chapter will look at cultivating that trust across the cyber domain, through the development of cyber-warriors and leaders. There are several demographic trends that have a serious impact on the workplace, which will also affect the military. The nature of cyber is also a primarily intellectual activity which is unique to an organization that is founded on physical tasks and structured to support soldiers who excel in those areas. This chapter will look at how we are able to mitigate the fact that much of the leadership will be unfamiliar with many of the technical concepts and show that in order to employ cyber capabilities, leaders must be versed to a certain

degree technically. It will also look at the current development model and how it is not optimized for the cyber-warrior.

Chapter four will look at the employment of cyber as a capability. In the academic world there is a huge range in opinion on what the actual capabilities of cyberwarfare are. On one side, it is a weapon that can have strategic effect on par with nuclear weapons. On the other side, there have been no destructive effects that have been demonstrated to date therefore it is no more than a supporting asset. This chapter will argue that it is a weapon that can be used as a primary instrument as well as a critical enabler that can provide access to targets that was previously unattainable.

CHAPTER 1

> *"If an information revolution that may parallel in magnitude the advent of the modern state, the mobilization of whole peoples through secular ideology, the mechanization of killing through science and technology, and the ultimate terror of thermonuclear annihilation is indeed in the process of enveloping the world, then the resulting uncontrollable onrush of events will sweep nations and military organizations before it."*
>
> - Williamson Murray and MacGregor Knox, Thinking about Revolutions in Warfare

Military Revolutions, Revolutions in Military Affairs (RMA) and Military Technical Revolutions (MTR) are all concepts that are frequently defined and debated. Renowned military historians Williamson Murray and MacGregor Knox differentiated a Military Revolution from an RMA in that an RMA can be driven and influenced by the military, whereas a true revolution can be equated to an "earthquake" that cannot be avoided and "fundamentally changes the framework of war."[3] The essence of the debate amongst military scholars is differentiating the evolutionary changes from the revolutionary changes. One contemporary discussion is based on the information age and the way that the proliferation of information has changed warfare to this point and how it will continue to shape the wars of the future.

---

[3]Ibid, 6-7.

How do you define the information age? There are many components resident in any given civilization; economy, politics, education, technology, warfare, to name a few. Periodically throughout history there are certain factors that dominate the spectrum of these dimensions. Renowned defence researcher, David S. Alberts tackles the definition of what differentiates one "age" from another: "*Ages* are proclaimed when something happens to cause a discontinuity in multiple dimensions that affect civilization."[4]

This chapter is the foundation of this paper and it will look to focus on the revolutionary changes to society due to the information revolution, not necessarily to identify when it began. What effect does the focus of information have on the economy, on politics, on the way we learn and teach, on the proliferation of technology and of course on warfare? Alberts continues "Changes in the processes of value creation are at the core of broad-based discontinuities."[5] The economics of information are the key from Albert's perspective. The combination of information availability, virtual interactions and the elimination of distance as an impediment have given an increased value and importance to information in all dimensions of society.[6]

The proliferation of Information technology throughout society and specifically in the military has led to a Revolution in Military Affairs. In order to get to that conclusion, this chapter will look at the rise of the cyber domain in society, the characteristics of the cyberwarfare and how the cyber domain has impacted the nature of warfare.

---

[4] David S. Alberts and Richard E. Hayes, *Power to the Edge* (Department of Defence, CCRP, 2003), 71.
[5] Ibid.
[6] Ibid.

Defining Cyberwarfare

In 2009 the Government of Canada felt it was necessary to publish a strategy across the government for the protection against cyber-attacks. In that, they articulated one of many different definitions on cyberspace: "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship."[7] The US Department of Defence defines it as follows: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[8] The US Air Force doctrine reinforces that the cyber domain is man-made and therefore unique to the other four domains of land, sea, air and space. And that "Activities in cyberspace can enable freedom of action for activities in the other domains, and activities in the other domains can create effects in and through cyberspace."[9]

The Cyber dimension of warfare is one that we are only beginning to understand, but suffice to say it is not bounded in a clear-cut fashion like air, land or sea.[10] The equivalents to roads, air or sea-lanes are data routes that are virtual and constantly changing. Only recently have

---

[7] "Canada's Cyber Security Strategy " http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx (accessed 4/14/2013, 2013).

[8] David M. Franklin, "*US Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority*," (National Defense Univ Washington DC, Inst for National Strategic Studies 2010), 21.

[9] Department of Defense, United States Air Force, *Air Force Doctrine Document 3-12* , (2010), 1.

[10] Isaac R. Porche III and Jerry M. Sollinger, "An Enemy without Boundaries," *Proceedings Magazine, U.S. Naval Institute* Vol. 138/10/1,316 (October 2012), 1.

opinions on where cyber fits within international legislature such as the Law of Armed Conflict and the Geneva Conventions. With few examples to draw on to date, the employment of "cyber weapons" is a decision with strategic implications. US political consultant on information strategy James Farwell and noted cyber security academic Rafal Rohozinski described the changing dynamic of war in their paper *Stuxnet and the Future of Cyber War*:

> …attribution is a matter of interpretation. The present de facto application of an onerous standard of evidence means states can sidestep culpability even for an event occurring in a segment of cyberspace over which they exert sovereign regulatory authority and jurisdiction. The traditional Law of Armed Conflict requires that one identify an attacker. In cyber war, that is difficult to do. Where attacks emanate externally, outside a targeted nation, there are huge questions about the responsibility of the victim to identify the physical location of a computer or network.[11]

Cyberspace and the cyber domain are some common terms that are associated with the information age. Cyberspace deals with the area (both physical and virtual) where the Internet and the associated components are resident. Martin Libicki describes cyberspace as "…a thing of contrasts: It is a space and is thus similar to such other media of contention as the land and sea. It is also a space unlike any other, making it dissimilar. Cyberspace has to be appreciated on its own merits; it is a man-made construct."[12] Libicki defines three layers that make up cyberspace: the physical, syntactical and the semantic layers.[13] Although from a technical perspective,

[11] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War " *Survival* 53, no. 1 (2011), 31.

[12] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 214.
[13] Ibid.

Libicki's layers could be confused with the Open Systems Interconnect (OSI) Model,[14] Libicki's simplification is helpful in understanding the overall complexity and interconnectivity that is cyberspace and also when it comes time to understand the vulnerabilities and threats in a cyber-environment: the layers help elucidate the potential strategies for cyber defence or the vulnerabilities to cyber-attack.

The physical layer is straight forward and is composed mostly of the hardware – the computers, peripherals, servers, wires and other infrastructure. The syntactic layer is essentially the layer that contains all of the direction and instructions; computer code in other words. It contains the "…the protocols through which machines interact with one another—device recognition, packet framing, addressing, routing, document formatting, database manipulation, etc."[15] The semantic layer contains the contents to enable human interaction with the system. It is both the information that manipulates the system like instructions and the information that is displayed to the readers. It is a combination of information required in order to manipulate the system, such as instructions, other information is actually there to be processed as it is seen, as information. Despite the numerous definitions that convey a similar message, there is much of this domain that is still misunderstood.

[14] The OSI, or Open System Interconnection, model defines a networking framework for implementing implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the back up the hierarchy. Layer 1: OSI Physical Layer, Layer 2: OSI Data link Layer, Layer : OSI Network Layer, Layer 4: OSI Transport Layer, Layer 5: OSI Session Layer, Layer 6: OSI Presentation, Layer Layer 7: OSI Application Layer. http://www.escotal.com/osilayer.html

[15] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 214.

Former director of the National Security Agency (NSA) and Central Intelligence Agency (CIA) General (Ret'd) Michael Hayden describes the nature of cyberwarfare as being inherently complex and difficult to understand. He talks about the importance of precise language and the reality that there are many people who talk about the nature of cyberwarfare, but few who actually understand it.[16] "Rarely has something so important and talked about with less clarity and less apparent understanding that this phenomenon."[17]

In 2009 the CF published the Integrated Capstone Concept (ICC). The purpose of the ICC was to: "provide the Defence Institution with an over-arching concept, informing a body of operating, integrating, and enabling concepts that will shape how the CF will meet the challenges of the complex future security environment."[18] The ICC touches on many of the concepts discussed to this point, in particular, the importance of globalization and how it relates to the security environment: "The proliferation of new technology facilitates and enables creative and dynamic means for people and systems to interact. This interaction builds interconnectedness, interdependence, and relationships, and it forms the basis of the complexity in the future security environment."[19] Further, the ICC emphasizes that "The marketplace drives innovation and technology within cyberspace. All aspects of this domain – including the Internet, telecommunications networks, computer systems and software – are in a process of continuous

---

[16] Michael V. Hayden, "The Future of Things "cyber"," *Strategic Studies Quarterly* 5, no. 1 (2011), 3.

[17] Ibid.

[18] Canada, Department of National Defence, "*CF Integrated Capstone Concept*", Chief of Force Development (2010), iii.

[19] Ibid., 7.

change."[20] While the ICC clearly demonstrates that cyberspace is on the "radar" of the CF, it is certainly an area where much remains unknown and limited examples exists to follow.

Hayden asks the question "How do we deal with the unprecedented?"[21] He opines that the lessons that have been learned throughout the other domains of war do not easily translate to cyber and "casually applying well-known concepts from physical space like deterrence where attribution is assumed to cyberspace where attribution is frequently *the* problem is a recipe for failure."[22] Despite being a central figure in the US Defense and Security apparatus, he concedes that he and his peers often did not have the comfort level with the myriad of legal and policy issues surrounding cyber-related issues to inform an operational course of action.[23] To appreciate some of the unique challenges that exist in preparing for cyber war it is important to identify some of the characteristics and where they are derived. The first of which is the global economy and how it is both dependent on the cyber infrastructure and the catalyst for cybercrime.

Relationship with Cybercrime

Because of the dependency of the economy on the Internet, cybercrime becomes a military defence issue for countries, as economic interests can be attacked through electronic means. Former head of the CIA and recently retired US Secretary of Defense (SecDef) Leon Panetta reaffirmed this during a recent speech: "Cyberspace has fundamentally transformed the

[20] Ibid.

[21] Michael V. Hayden, "The Future of Things "cyber"," *Strategic Studies Quarterly* 5, no. 1 (2011), 3.
[22] Ibid.
[23] Ibid.

global economy. It's transformed our way of life, providing two billion people across the world with instant access to information to communication, to economic opportunities…yet, with these possibilities, also come new perils and new dangers."[24] An illustration of the dangers is banking. Many of the traditional methods of transferring money and making payments have been overtaken by the opportunity to conduct the same business from a computer terminal. Individuals and institutions transfer billions of dollars daily "over the wire", which has become a huge target for cyber criminals. Recent statistics indicate that 232 computers are infected with malware every minute[25], estimates of money lost are upwards of $200 billion annually with an additional $100 billion in recovery cost.[26] With this lucrative opportunity many of the top developers (or hackers) are being recruited by organized crime and in unprecedented fashion, some governments have developed working relations with these organized crime groups. Farwell and Rohozinski amplify the relationship between governmental development and organized crime: "States are capitalising on technology whose development is driven by cybercrime, and perhaps outsourcing cyber-attacks to non-attributable third parties, including criminal organisations."[27]

---

[24] Leon Panetta, *Defending the Nation from Cyber Attack*, (2012).

[25] RSA, *RSA 2012 CYBERCRIME TRENDS REPORT the Current State of Cybercrime and what to Expect in 2012*,(2012), 8.

[26] "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually " http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (accessed 4/8/2013, 2013).

[27] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011), 24.

The most publicized example is the Russian Business Network (RBN), who have been accused conducting contracted cyber-attacks for both state and non-state organizations.[28] There work ranges from creating massive amounts of email spam to coordinating and executing cyber attacks against critical infrastructure in Estonia in 2007 and Georgia in 2008. Although Moscow has denied any knowledge or responsibility for the attacks, much of the evidence online shows that if it was not a request to the RBN to conduct the attacks it was likely an order.[29] An interesting anecdote to the 2007 attacks on Estonia was that they came to an abrupt stop almost exactly one month after they started, leading many to believe that is the time that was paid for. This emphasizes the revolutionary changes in war and how crime and the economy are more intertwined with national security than ever before. With so much at stake many of today's bright minds are enticed to working for organized crime. Whether these individuals are working directly for organized crime or selling their products to crime organizations, individuals can have a significant effect on this new type of warfare. An individual in the cyber domain arguably is able to have a greater effect than with any previous weapons system. This contributes to the unique nature of warfare in the cyber domain.

The Power of the Individual

Historically, the more powerful the weapon, the more likely that it is possessed by an organization with means and motive; usually powerful states. In the case of weapons in

---

[28] Alexander Klimburg, "Mobilising Cyber Power," Survival, 53, 2011, p. 49 as referenced in "A Walk on the Dark Side," The Economist, 2007.

[29] Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* CSBA, 2012), 24-25.

cyberspace, extremely powerful weapons can be possessed by individuals with limited resources. A case study by Kevin O'Connor from the SANS Institute, discusses the potential of such empowered individuals through the exploits of the online hacker known as "Jester". The Jester is a hacker with strong ties to the US military and likely has a history with the US Special Forces, either as a soldier or a civilian contractor. [30] Clearly influenced by his service with the military, one of his aims was "…to disrupt Jihadi activity through cyber-attacks, ultimately trying to halt the proliferation of IEDs and save coalition soldier's lives."[31] However, over a two year period he attacked over 200 targets, displaying his ability to adapt his tactics as well as his willingness to challenge states, individuals and corporations depending on the specific goal. In one attack, he conducted a denial of service attack against the website WikiLeaks after the website chose to expose classified information that he felt potentially put American soldier's lives in danger.[32] Another completely different event occurred in March 2011, when he manipulated Libyan media (the Tripoli Post) in an effort to erode the morale of the local population and weaken Gaddafi's popular support.[33]

O'Connor lobbies in his conclusion that the example of the Jester shows that the cyber domain "…is one that favors David over Goliath." While, there are numerous examples that prove the contrary, it does show that the advantage in cyberspace goes to the attacker. The

---

[30] T. J. O'Connor, "The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare" The SANS Institute), 2.

[31] Ibid., 2.

[32] Ibid., 13-14.

[33] Ibid., 18;

ability to be self-sufficient and not dependent on other actors affords anonymity that is extremely difficult for a big organization and may only be achieved through a significant investment in additional resources. [34] This theory ties in extremely well with the vulnerabilities that the cyber domain creates. Because the syntactical layer can be spoofed, modified or used as proxy it is very difficult to define recognizable borders. Infrastructure used to conduct cyber-attacks could be used from friendly or neutral countries, if you are in fact able to identify the origin.

Porche, Sollinger and MacKay articulate how the cyber domain is completely different from the air, land and sea as there are no clear boundaries.[35] "People often speak of "defending U.S. cyberspace" in much the same way they do of defending the country's borders. The difficulty is that cyberspace really has no boundaries. The data, services, and applications in cyberspace flow across routers and servers that span the globe."[36] The two major challenges that the authors derive from the nature of the cyber domain is that because there are no boundaries, there are no clear areas that you should be anticipating an attack, so attacks can come from anywhere. Second, the domain is completely dynamic. Many of the routes that exist are virtual, so data will rarely travel through the same *physical* path. Even at the physical layer, the components are being changed so often that understanding where you are is inherently complex.[37] As O'Connor pointed out the advantage of being small in the cyber arena through the Jester example, Porche et al confirm significant advantage to be an attacker in cyberspace and not a defender as the initiative in a cyber-attack is critical.

---

[34] Ibid., 25;
[35] Porche III and Sollinger, *An Enemy without Boundaries*, 1.

[36] Ibid.
[37] Ibid., 2.

West Point cyber-focussed academics Major Matthew Miller, Lieutenant Colonel Jon Brickey and Colonel Gregory Conti take the concept of defence a step further and suggest that the millions of dollars spent on cyber defence will have limited success against a motivated adversary.[38] "Perfect defense is impossible; the astronomic complexity of the software and hardware woven into our information systems and networks is beyond human comprehension."[39] In an environment that is so complex, a single flaw is all that is required to breach the defence, so the heavy barriers of a virtual "Maginot Line" are still susceptible to attack where there are vulnerabilities in that defence.[40] Putting it in concrete terms, Miller et al estimate that "defenders must field 1,000times the resources (money, people, time, compute power, etc.) to reach parity with attackers in cyberspace; this is not a winning proposition for the defender."[41]

In fact, some would argue that because it is next to impossible to defend against cyber-attacks than it would be more efficient to deal with recovery, rather than prevention Hayden ponders if the "…the web so skewed toward advantage for the attacker that we are reaching the point of diminishing returns for defending a network at the perimeter (or even beyond) and should now concentrate on how we respond to and recover from inevitable penetrations?"[42] Although, Hayden doesn't provide a direct answer to the question, there are limited examples of where cyber-attacks have had a lasting effect. The example that is often used to demonstrate the effects that can be achieved is Stuxnet.

---

[38] Matthew Miller, Jon Brickey and Gregory Conti, "Why Your Intuition about Cyber Warfare is Probably Wrong," *Small Wars Journal*, (Nov 29 2012), 1.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Hayden, *The Future of Things "cyber"*, 3

Stuxnet – A Case Study in Cyberwarfare

In 2006, the United States created a cyber-program to disrupt the Iranian development of nuclear capabilities. New York Times writer David Sanger describes the intent being twofold: "First was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there was a smarter, more elegant way to deal with the Iranian nuclear problem than launching an airstrike that could quickly escalate into another Middle East War..."[43] The program was called Olympic Games and its target was the Iran's principle nuclear facility in Natanz.[44] The piece of the program that has become well publicized was the malicious code that was introduced to the Natanz environment called Stuxnet. Although, never confirmed by any governments, Stuxnet is believed to be a computer worm that was designed and engineered by a combination of US and Israeli cyber organizations which exploited a number of faults that existed in open-source software.[45] In fact, Farwell and Rohozinski describe Stuxnet as being "less sophisticated than billed"[46] and a "…Frankenstein patchwork of existing tradecraft, code and best practices drawn from the global cyber-crime community".[47] Stuxnet went from being part of a Top Secret program to a virus that was available for all to see when it escaped from the controlled environment in Natanz and continued to replicate across the Internet.[48] By

---

[43] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power* Broadway, (2012), 190.
[44] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *New York Times* (June 1, 2012).
[45] Farwell and Rohozinski, *Stuxnet and the Future of Cyber War*, 28
[46] Ibid., 25.

[47] Ibid.
[48] Sanger, *Obama Ordered Wave of Cyberattacks Against Iran*

escaping its targeted environment, Stuxnet has become one of the only examples to analyze cyberwarfare and has also led to as many additional questions as it has to answers.

The first question that needs to be asked has to do with the ability to conduct these attacks with limited resources. Looking at O'Connor's example of the Jester, and Miller et al's view on the cost of defending in the cyber domain it would appear like a target rich environment for lone wolf hackers and non-state actors with limited resources to conduct powerful cyber-attacks. David Betz, Senior Lecturer at the Department of War Studies at King's College London disagrees with that idea. Betz believes that "analyses of Stuxnet point to it being the product of a well-resourced government…with precise insider knowledge of the target it was seeking."[49] This implies that the states involved had to dedicate extremely rare, expert technical resources to one problem while concurrently developing an understanding of the physical aspects of the plant through other means. In the case of Stuxnet, that involved Israeli HUMINT operators with access to the Iranian scientific community and were absolutely crucial in gaining access to a closed network.[50] On top of this there was extensive research that needed to be conducted on the exact cetrifuges, to confirm that a change to the operational instructions would in fact have the effect that was anticipated.[51] Something that has been advertised as being the cheap option clearly has costs that are not necessarily considered, but are certainly necessary for the cyber option to be effective. Understanding that the program started in 2006 and the main effects were seen in

[49] David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies* 35, no. 5 (2012), 695.

[50] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power*, 195.

[51] Ibid., 199.

2010[52], this is indeed a significant investment. The resources also extended outside of the typical military industrial complex, which gets into another unique aspect of the cyber domain.

The code used for Stuxnet was largely commercial code in an effort to remain "unattributable" as was directed by President Obama.[53] The virus was delivered unknowingly into the closed network at Natanz by Siemens technicians that regularly maintained the programmable controllers to the centrifuges.[54] It is certainly warfare that is inherently more complex in nature and revolutionary by way of the interconnectivity of relationships, but did these collaborations achieve the result that Stuxnet was intended for?

From open source reporting the US estimates that it essentially caused the Iran Nuclear program a setback of 18 – 24 months.[55] However, the actual damage that occurred has been widely disputed throughout various circles and it is questionable if the disruption was actually of strategic importance. Scholars, including Libicki and Betz argue that if cyber is to command strategic importance it will need to be able to produce effects similar to and ideally greater than conventional weapons. Libicki also highlights that "[P]eople have worried about cyberwar for most of the last 20 years, and in all that time, not one person is known to have been killed by a cyber-attack."[56]

---

[52] Sanger, *Obama Ordered Wave of Cyberattacks Against Iran*
[53] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power*, 202.
[54] Ibid., 196.

[55] Sanger, *Obama Ordered Wave of Cyberattacks Against Iran*
[56] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011, 2011), 135.

Libicki views cyber in a similar vein to Electronic Warfare (EW) in that it is an enabler to kinetic effects and can be used in a disruptive fashion in order to achieve other effects on the battlefield rather than as a standalone weapon that has lasting physical effects on its own.[57] Betz believes that this is exactly how Stuxnet was able to achieve the effects that it did, through a "*combination* of other resources in order to achieve a strategic effect." Looking at Stuxnet, it appears that the end result was more disruption than destruction, which may well have been the intent. Anonymity of the attacker is another area that has been considered a distinct advantage in a cyber-attack scenario, and was prescribed in no uncertain terms by Obama when he declared the attack needed to be "unattributable."[58] , but did Stuxnet prove that it is possible to deliver the ultimate blow in a non-attributable fashion?

The cyber option for Natanz, was apparently chosen in part to prevent the Israelis from conducting a more kinetic option which could have potentially been the first blow in a regional conflict.[59] Farwell and Rohozinski surmise that the decision likely came down to a cost-benefit analysis, where the chance of success of the cyber-attack with minimal risk to forces and the ability to mask the aggressor outweighed an option of an overt kinetic attack, where the confirmation of success would be clear.[60] Betz believes that cyber weapons can have physical effects and uses the global economic dependence on the Internet as an example of a target that would achieve strategic effect, but he argues that the concept of anonymity in cyber warfare is

---

[57] Ibid.

[58] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power*, 202.

[59] Ibid., 190.

[60] Farwell and Rohozinski, *Stuxnet and the Future of Cyber War*, 28

not as helpful as it might seem. He refers back to Clausewitzian theory and the fact that war "*requires* commitment"[61] and the absence of commitment, leaves the door open for reconstitution. Destruction through cyber means would likely have a different effect than a kinetic strike. Where an airstrike could completely destroy the building and its contents, the destruction from a cyber-attack could be recreated in a shorter period of time. This is hard to concede in the case of Stuxnet because once the virus left the controlled environment at Natanz and was discovered on the Internet, the Iranians could determine who the aggressor was and take action. Although it could have potentially had a similar strategic effect, in all likelihood the immediacy of a kinetic attack and complete destruction from a kinetic attack are likely more significant than the effects of a stand-alone cyber-attack.

Although there are few conclusions that are universally agreed upon with respect to Stuxnet, the fact that it is ground-breaking is one of them. Hayden may have said it best : "Previous cyberattacks had effects limited to other computers…This is the first attack of a major nature in which a cyberattack was used to effect physical destruction…Somebody crossed the Rubicon,"[62]

Conclusion – Chapter 1

Eliminating the technology involved in the attack, the ambiguous nature of it is certainly something that could not be explained when looking at contemporary military doctrine. The nature of warfare has changed. There is no longer a clear enemy and that enemy may or may not

[61] Betz, *Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed*, 695

[62] Sanger, *Obama Ordered Wave of Cyberattacks Against Iran*

be representing a military or even a state.[63] The code used for Stuxnet was largely commercial code, meaning that there is potential that parts of the attack were "outsourced" to agencies within the government or even commercially.[64] Farwell and Rohozinski identify the unprecedented relationship between governmental development and organized crime: "States are capitalising on technology whose development is driven by cybercrime, and perhaps outsourcing cyber-attacks to non-attributable third parties, including criminal organisations."[65] The confluence of all of these factors makes it hard to compare with the revolution during World War 1 when fire in depth changed everything.[66] It is warfare that is inherently more complex in nature and revolutionary in comparison.

The rise of information technology has clearly been a catalyst for change in society and has opened the door for a new type of warfare. The challenges are unique and original and will only be solved with creative solutions. The CF will not be exempt to any of these challenges and in many ways due to the nature of the institution, those challenges will be amplified. In the following chapter, the structure of the CF will be analyzed and compared with private organizations that have chosen innovative ways to structure an organization as well as some military theories that look to change the current paradigms.

---

[63]Farwell and Rohozinski, *Stuxnet and the Future of Cyber War* , 27

[64]Ibid., 23.

[65]Ibid.

[66] Jonathan B. A. Bailey, "The First World War and the Birth of Modern Warfare," in *The Dynamics of Military Revolution, 1300-2050*, eds. MacGregor Knox and Williamson Murray (Cambridge, UK: Cambridge University Press, 2001), 132.

Recalling the “earthquake” analogy used by Murray and Knox, the advent of cyber technologies coupled with a world that is increasingly focused on the economy has fundamentally changed the framework of war. The effect has been a focus on non-lethal technologies and minimizing casualties where possible, which is a transformational shift in mindset. The technical changes themselves have been game-changing, but the effect that they have had on the nature of conflicts has led to a Military Revolution. Cyberwarfare is not driven by the military; it is a direction that must be pursued and cannot be avoided.

CHAPTER 2

Change is difficult in any organization. The topic has been studied significantly and strategies to ease the process have been published with varying degrees of success. The CF has certainly not been immune to the challenge of change. The military is generally considered to be less agile and more cumbersome with respect to the change process, leading to a slower adaptation to cutting edge concepts.

The previous chapter highlighted the impact of technology throughout society and in particular with respect to war to the revolution in military affairs due to the advent of the cyber domain. Understanding the financial success that has been realized in the private sector through innovation, it would be irresponsible to ignore the military application of these lessons as there are many parallels that can be drawn. Military organizations are unique when compared to organizations of a similar size and structure in the public and private sectors. Many of the customs, traditions and methods of doing business have been proven effective in the most difficult circumstances and they have been carried forward to the present day. The military also promotes those who achieve success in that environment, meaning that military professionals experience a sense of comfort from following the lessons learned and using historical answers to support current decisions.

Despite being an organization that is traditionally resistant to change, the military has a great deal to learn from the private sector in the employment of cyber forces. Understanding this, cyber forces are optimized to perform in a decentralized environment where command and control is conducted in a streamlined fashion. The nature of the cyber conflict is such that tactical

operators can potentially have effects reaching the operational and strategic level. In order to draw this out, this chapter will look at some innovative examples in the private sector. It will look at Special Operations Forces (SOF) that perform completely different functions than cyber, but can be considered similar due to the operational and strategic effects that they have.

The Military Institution

History is extremely important to the military as an institution. There are few organizations that see their history influence them as much as the military on a daily basis. Looking at a uniform, you can often find the professional history of an individual, including deployments, honors and awards and specialty qualifications. The battle honors of units are well publicized and celebrated, often to the point where specific battlefield tactics are become part of the living history of the unit. With this connection to historical events also come ties to historical practices that, in their current form, often act as an impediment to change.

The CF published *Duty with Honor* originally in 2003 and there have been several iterations of the publication since then. The intent of the publication was to act "…as a cornerstone document within the Canadian Forces professional development system."[67] The "profession of arms" is the cornerstone of *Duty with Honor* and a critical concept to understand. The purpose of the profession of arms is to apply lawful force on behalf of the government of Canada. The binding criterion within the CF is the unlimited liability that all members of the

[67] Canadian Forces Leadership Institute, *Duty with Honor : The Profession of Arms in Canada 2009*Chief of Defence Staff by the Canadian Defence Academy - Canadian Forces Leadership Institute, 2009), preface - General Natynczyk.

profession of arms have accepted. The culture of the CF in turn is explored as well as the importance of a central ethos that unites members of the profession of arms.[68] However, many of the characteristics that serve to strengthen the CF as an institution also serve to make it rigid and inflexible.

The first characteristic that strengthens the institution is military identity. Clearly, there are a number of different aspects of an individual's military identity; environment, trade, qualifications, operational experience and rank to name a few.[69] The establishment of a clear military identity is instrumental in cultivating a hierarchy of loyalty throughout the CF.[70] History and heritage also play a huge role in understanding the military culture and its general reluctance to change. As *Duty with Honor* highlights*:* "Knowing Canada's military history, heritage and traditions reinforces the profession by demonstrating and valuing the importance of intangibles."[71] The intangibles described in *Duty with Honor include* battle honors and recognizing that significant contribution and also includes the motivational value that traditions and ceremony achieve.[72] "Commemorating the proud history of Canada's armed forces, while preserving customs and traditions that enhance cohesion and esprit de corps, are vital requirements for maintaining and sustaining Canadian military professionalism."[73] Intangibles also include ethos, which are essentially that set of codified beliefs that members are bound. Some of the CF ethos that are highlighted in *Duty with Honor include:* "All accept that no one is

[68] Ibid.

[69] Ibid., 55.
[70] Ibid.
[71] Ibid., 60.
[72] Ibid.
[73] Ibid.

exempt from being ordered into harm's way…the obligation to bear arms as required…that the core military values — duty, loyalty, integrity and courage —are at the heart of the profession of arms."[74] Clearly, the importance of tradition and loyalty are key parts of the CF culture, but they are both characteristics that can impede change. One recent example of a major change in the CF is CF Transformation. Being a recent and major structural change it is a perfect case study to lead into a discussion on future changes with respect to the employment of cyber forces.

LGen Michael Jeffery retired from the Canadian Army in 2003 as the Chief of the Land Staff. In 2007, he was asked to study the effects of CF Transformation, the process led by Gen Rick Hillier to improve the overall effectiveness of the CF on operations by restoring the commander as the central figure during operations. In his summary article for the Canadian Military Journal, he confirmed that military organizations are often conservative when it comes to making decisions and change in this environment is usually driven by a catalyst or forcing function.[75] The catalyst could be an event, often a defeat in battle or a failure in operations, or it could be a transformational leader that drives the change, which he believes was the case with Gen Hillier. Jeffery also emphasizes doctrine and training designed to inculcate members with loyalty to the unit and their fellow soldiers as well as a sense of tradition. He describes the effort to effect change as being "direct conflict with the underlying values of the culture."[76]

[74] Ibid., 56.

[75] Michael K. Jeffery, "Inside Canadian Forces Transformation," (2010), 9.
[76] Ibid., 13.

However, CF Transformation does show that the CF is capable of change. In fact, this was not minor or cosmetic change, according to Jeffery it was: "a paradigm shift in command philosophy that would reassert command to its rightful place, with an appropriate subordination of the staffs."[77] Incidentally, the command and control hierarchical structure is one of the areas that are often identified when looking at opportunities to capitalize on the advantages of information technology (IT). As Canadian Defence researcher's Dr Ross Pigeau and Carol McCann identify in their work on defining Command and Control: "Historically, a military's chain of command has been the principal ways both for providing and for constraining command opportunity."[78] They thought it necessary to define the words command and control as the terms are often used, but frequently with different intent. In the article they defined the terms as such: "Control: those structures and processes devised by command to enable it and to manage risk. Command: the creative expression of human will necessary to accomplish the mission."[79] This is one way of looking at Command and Control, but it is certainly not a universally accepted definition.

Per the Pigeau and McCann definition of command, the style and organization are not explicitly outlined, meaning that as long as there was an expression of will at some point and the result is achieved, there could be numerous ways to arrive at the desired result. However, they specify that there are three dimensions of command capability; competency, authority and

[77] Ibid., 15.

[78] Ross Pigeau and Carol McCann, "Re-Conceptualizing Command and Control," *Canadian Military Journal* 3, no. 1 (2002), 60.

[79] Ibid., 56.

responsibility.[80] Other definitions, such as that of Dr Paul Mitchell of the Canadian Forces College observe a much more rigid command and control model which is hierarchical in nature and driven from the top down. The authority is clearly defined and flows: "From the sovereign takes an unambiguous path from head of state, to chief of defence, to private soldier."[81] Jeffery pointed out, the open-ended nature of Pigeau and McCann's definition is in conflict with the culture of the CF, as it implies that a person that is able to express their will is essentially in command. This may refer to emergent examples, but it does not correspond well with the rigid chain of command that is practiced in the CF. However, in the cyber context, technical expertise is critical to the resolution of tasks, and the most technically proficient soldiers may not be the highest ranking. Cyber isn't the only example where expertise is resident at the level of the operator. With the vast amounts of information available, there are a number of proponents of decentralized activity in order to be more efficient and effective. The preeminent example in the western military today is mission command.

Mission Command

The definitions of mission command are fairly consistent across the different nations. NATO describes mission command in *Allied Joint Publication 01(AJP-01)*:

> Through mission command, commanders generate the freedom of action for subordinates to act purposefully when unforeseen developments arise, and exploit favourable opportunities. Mission command encourages the use of initiative and promotes timely decision-making. Commanders who delegate authority to

[80] Ibid., 57.

[81] Paul Mitchell, "*Media and the Military: Operational Weapon Or Tactical Schtick?* " Null, CFC, Canada, (2012), 10.

> subordinate commanders need to state clearly their intentions, freedoms and constraints, designate the objectives to be achieved and provide sufficient forces, resources and authority required to accomplish their assigned tasks.[82]

In a service paper at the UK War College in Shrivenham, Col Bryan Watters definition is similar, though he clearly draws out the principles of mission command as: Unity of Effort (across the organization), Decentralization, Trust (mutual, deep and enduring), Mutual Understanding and timely and effective decision making.[83] Retired US Gen Martin Dempsey,former Chairman of the Joint Chiefs of Staff published a white paper in April 2012 prior to his retirement which shares a consistent view with Watters. The paper describes the tenets of mission command and focuses on the strengths of the technique and the investment required at each level in order to achieve success.[84] With an appreciation of the essence of mission command, it is clear to see why in an information focused world this would be advantageous for commanders in accomplishing tasks in a more efficient way.

Dempsey insists that first and foremost, mission command is centred around the commander and it requires leaders that are adaptable at each level of command.[85] From the Canadian perspective, this is consistent with the intent of CF Transformation, as Gen Hillier reasserted the commander as the central figure.[86] Mitchell reinforces the vital role that unity of

---

[82] NATO, *AJP 01(D) Allied Joint Doctrine*, (1 December 2010), 6-3, para 0612.
[83] Colonel Bryan Watters, "Mission Command – Mission Leadership (Creating the Climate for Maximising Performance) – A Corporate Philosophy " (Service paper, Shrivenham, UK), 3.
[84] Martin E. Dempsey, "MISSION COMMAND," *Army* 61, no. 1 (Jan 2011, 2011), 3.

[85] Dempsey, *MISSION COMMAND*, 3
[86] Jeffery, *Inside Canadian Forces Transformation*, 14

command plays. With a clear commander and a supporting staff, the ambiguity can be minimized creating a much more efficient organization. [87] Dempsey sees the information age accelerating the pace of change and consequently creating an increasingly dynamic security environment. He believes that the counter is to speed up the tempo of operations through decentralizing the decision making and conduct of the operations.[88] As he states: "Smaller, lighter forces operating in an environment of increased uncertainty, complexity and competitiveness will require freedom of action to develop the situation and rapidly exploit opportunities."[89] The importance of the commander communicating a clear intention and having that unequivocally understood is critical to having a force function in the most efficient and effective manner. The second major piece of mission command theory is trusting people at each level to complete their task based on the intent.

Trust as A Force Multiplier

Without an advanced level of trust throughout an organization, Mission Command cannot be effective; commanders are reluctant to delegate and more likely to centrally hold onto responsibilities. The concept of trust as a force multiplier is not an idea unique to the military. Steven R. Covey takes it a step further in his book *The Speed of Trust*. Covey sees trust as *the* critical piece in creating confidence in an organization. Covey sees the level of trust being directly proportional to speed and inversely proportional to cost. His formula is simple and described as follows: "The formula is based on this critical insight – trust always effects two

[87] Mitchell, *Media and the Military: Operational Weapon Or Tactical Schtick?*, 11
[88] Dempsey, *MISSION COMMAND*, 3-5
[89] Ibid., 4.

outcomes, speed and cost. When trust goes down, speed will also go down and costs will go up…when trust goes up, speed will also go up and costs will go down…"[90] Covey sites numerous examples in our daily lives, such as the lack of trust following 9/11 attacks on the US leading to increased security measures which slowed down travel and raised cost dramatically.[91] He mentions the significant regulations that were introduced through the Sarbanes-Oxley Act in response to the scandals at Enron and WorldCom. The regulations that have attempted to protect investors have increased the administration cost by an estimated $35 billion annually by dramatically increasing the time.[92] For the corollary example, Covey sites Warren Buffet as a universally trusted business partner, who was able to acquire a $23B company from Walmart during a two hour meeting, eliminating typical negotiations that could take months and reducing the legal fees to a fraction of what a similar deal would command.[93] And for a more basic example, he recounts a vendor in New York who trusted patrons to leave the money in a box, rather than using a cash register for each transaction. The time that was not spent on collecting money and giving change allowed for more customer throughput and greater profits, but was based on the assumption that people were trustworthy enough to pay what they owed without anyone confirming.[94] Although trust can be very powerful, it needs to be earned. Covey maintains that trust is comprised of two key pieces, character and competence, which can be

---

[90] Stephen R. Covey and Rebecca R. Merrill, *The SPEED of Trust: The One Thing that Changes Everything* Free Press, (2006) 43.

[91] Ibid.

[92] Ibid., 43-44.

[93] Ibid., 45.

[94] Ibid., 46.

broken down further.[95] The theory articulated by Covey is certainly applicable in a military context. It is important for leaders to understand that they can earn and lose trust and equally important that it can be developed, regained or lost at any time. There is a scale and it can be influenced. This understanding is especially pertinent as Mission Command doctrine becomes more prevalent in the CF and the foundation is trust at each level.

Conceptual Foundations, the CF publication on leadership, breaks it down in a slightly different fashion. Value based leadership is the goal and trust is one of the secondary outcomes.[96] In this linear approach, it fails to capture the importance of trust in a cyclic fashion. Covey sees trust developed in five waves; starting with building self-trust through the establishment of credibility, then building relationship trust through consistent behavior, then organizational trust which is generated through consistent alignment through the organization, then comes market trust, founded on reputation and finally comes societal trust which speaks to the contribution that an organization makes to the greater society. [97] In a military context, an organization that is given trust and succeeds will gain further trust for future and more complex tasks and further autonomy to complete them. Organizations that have recently received such autonomy have been SOF.

Special Operations Comparison

The nature of special operations epitomizes the need to establish high levels of trust. The tasks are complex and have high-reaching effects and they are executed by small teams of

[95] Ibid., 50.

[96]Canada, *Leadership in the Canadian Forces: Conceptual Foundations*, ed. Department of National Defence (Ottawa, ON: Canadian Forces Leadership Institute, 2005), 19.

[97] Covey and Merrill, *The SPEED of Trust: The One Thing that Changes Everything* , 63-66

specialists who are expert at their mission. Navy SEAL Commander Bill McRaven defined Special Operations in his book on the theory of Special Operations, *Spec Ops*: " A special operation is conducted by forces specially trained, equipped, and supported for a specific target whose destruction, elimination, or rescue (in the case of hostages), is a political or military imperative."[98] Special operations are typically military organizations that are suited to operate in a mission command type environment, where the chain of command is streamlined and execution of tasks is decentralized to small teams of soldiers. McRaven amplifies: "A successful special operation defies conventional wisdom by using a small force to defeat a much larger or well-entrenched opponent."[99] Former Canadian Special Operations Forces (CANSOF) Commander MGen D. Michael Day and Deputy Col Berndt Horn reinforce the importance of a command centric environment, mutual understanding and they highlight that the effectiveness of CANSOF is due in large part to the people that make up CANSOF and not the high-tech equipment and specialized training.[100] The nature of the trust and the corresponding command and control relationship is something that other like organizations can emulate. Many of the characteristics outlined in McRaven's definition, could be transposed into something similar for cyber. Cyber warriors must be specially trained and equipped and their targets are going to have in either military or political imperatives. Again, the foundation of how they are able achieve these effects is based on trust.

---

[98] William H. McRaven and William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare : Theory & Practice* (Novato, CA: Presidio, 1995), 2.

[99] Ibid., 1.

[100] D. Michael Day and Bernd Horn, "Canadian Special Operations Command: The Maturation of a National Capability," (2010), 70.

The development of trust in SOF is achieved over time, but is aided initially by the unique and challenging selection and training process that all soldiers must pass through. This process is a choice that all of the special operators are making, so it is a commitment on their part right up front to meet the challenges that they face. Day and Horn reinforce the importance of the selection and training within CANSOF and how it translates to mission success: "– those who volunteer and who are ultimately chosen to serve in SOF as a result of highly refined selection procedures and standards –are what provide the SOF edge. That is the key element for mission success."[101] The training and selection aspect is not insignificant as it not only leads to a stronger organizational cohesion but it plays into the individual trust required "as no other military instrument of power is more sensitive" to the effects of attrition because of that extensive training.[102] James Kiras , author of *Special Operations and Strategy,* notes that following a helicopter accident during the Falklands in 1982, the Special Air Service Regiment lost 20 of its soldiers and estimated that it would take at least ten years to be able to re-generate that capability due to the training and experience of the soldiers. [103] The training and experience on operations perpetuates the development of trust inside the organization which strengthens the credibility outside. And similar to the private sector, the credibility and reputation of a unit leads to a greater sense of confidence.

Again, we're able to compare the similarities of organizations within the military to the private sector. As Covey relates it back to the business world: "Only as corporations focus on

---

[101] Ibid.

[102] James D. Kiras, *Special Operations and Strategy: From World War II to the War on Terrorism (Cass Series: Strategy and History)* (New York, NY: Routledge, 2006), 60.

[103] Ibid.

trust and integrity - on congruence rather than compliance - will they really be able to promote true organizational credibility and trust."[104] His critical parts that make up integrity are humility and courage, which incidentally are two individual character traits that define special operations and lead to a higher level of trust within these units. McRaven defines the six principles of special operations and how they fit into the different aspects of an operation: "A simple plan, carefully concealed, repeatedly and realistically rehearsed and executed with surprise speed and purpose."[105] The importance of the final principle, purpose, and how it relates to Covey's theory is critical. McRaven defines purpose as "…understanding and then executing the prime objective of the mission regardless of emerging obstacles or opportunities."[106] The purpose is understood from the mission commander down to every soldier on the objective. With this mutual understanding of the purpose, soldiers are empowered to make decisions based in a decentralized fashion. Day and Horn take this to the contemporary operating environment and having forces that thrive in what they describe as "volatility, uncertainty, complexity and asymmetric (VUCA)".[107] VUCA is also a descriptor that works well in the cyber domain. As with SOF, soldiers or cyber-warriors will likely be in a position to make decisions in that environment that they will need to be prepared to make and trusted to make. They will need to have a clear understanding of the intent of the commander as well as where their areas of responsibility start and finish. If they can be trained and empowered to make the decisions, the effects realized will be more significant.

---

[104] Covey and Merrill, *The SPEED of Trust: The One Thing that Changes Everything* , 92

[105] McRaven and McRaven, *Spec Ops: Case Studies in Special Operations Warfare : Theory & Practice*, 11

[106] Ibid., 21.

[107] Day and Horn, *Canadian Special Operations Command: The Maturation of a National Capability*, 70

Although optimized to work in this environment and with decentralized command and control, it is important to note that SOF follows a similar chain of command to that of conventional forces. Moreover, decentralization and autonomy come with caveats in the SOF context. McRaven warns that increasing the size of the organization, increases the complexity and makes it more difficult for : "… large forces to develop a simple plan, keep their movements concealed, conduct detailed full-dress rehearsals (down to the individual soldier's level), gain tactical surprise and speed on target, and motivate all the soldiers in the unit to a single goal."[108] Cyber forces are similar to SOF in that it is a small, highly specialized subset of soldiers where tasks are potentially of strategic and political importance, so McRaven's argument for SOF is applicable to a trained cyber organization as well.

While SOF and other specialized organizations tend to be the extreme of mission command within the military, there are numerous organizations in the private sector that have attempted to flatten the organization. General Electric has experienced a high degree of organizational success in its Durham, NC aircraft engine plant where it has worked with a mission command structure. The plant is responsible for assembling jet engines for Boeing 777 aircraft and has 170 employees and only one boss. Each of the other employees is qualified to one of three levels, one being entry level and three being the highest qualified technician in the plant. Level two technicians are able to complete all of the same tasks as level one technicians plus additional tasks and level three technicians are qualified on all of the tasks in the plant. Pay rates of all of the employees are known as they are tied to the qualifications and schedules are

[108] McRaven and McRaven, *Spec Ops: Case Studies in Special Operations Warfare : Theory & Practice*, 8

determined by the employees, ensuring that each team, that is charged with assembling an engine from start to finish, has the requisite qualifications to complete the task.[109] The most interesting part of this unique arrangement is the success that was achieved. When the plant was given a new type of engine to produce, it quickly adapted and two months after starting the Durham plant was producing the engine at 12-13% less cost than the plant that had been making the engine for years. As the author Charles Fishman indicates: "Trust is a funny thing. It is the mystery -- and the genius -- of what goes on at GE/Durham. And it is the reason why the plant offers so many lessons about why people work, how teams succeed, and what workplace democracy really means."[110] The non-contributing layers have been removed from the Durham plant and the focus of the organization is to produce engines. The only way that this is possible to achieve is through an advanced level of trust across the plant.

The Durham plant was not based around blind trust, but rather on the understanding of specific skillsets required and knowing that each member of the team was capable of accomplishing the task at hand. The trust at this level is based on the levels of technicians and the understanding that with that qualification, they are able to complete specific tasks. This is a similar effect that is achieved in the SOF environment and operators are trusted to complete tasks based on the qualifications that they have and the understanding there was a scrutinized selection process and rigorous training component behind the qualification. However, the concept of the flat organization has been challenged by numerous academics, including Jo Freeman.

---

[109] Charles Fishman, "Engines of Democracy," *Fast Company* 28, no. 174 (1999), 1-2.
[110] Ibid., 2.

Structurelessness

Freeman argued the concept as it pertained to women's rights organizations in the early 1970s with her piece *The Tyranny of Structurelessness*. Freeman claimed that there was no such thing as a "structureless" organization. She says:

> This means that to strive for a structureless group is as useful, and as deceptive, as to aim at an "objective" news story, "value-free" social science, or a "free" economy. A "laissez faire" group is about as realistic as a "laissez faire" society; the idea becomes a smokescreen for the strong or the lucky to establish unquestioned hegemony over others[111]

So essentially, an informal structure masks the power of the emergent leaders and removes the formal responsibility of that leader.[112] Freeman submits that there are occasions when an informal organization can come together to have success and can be quite effective, but there are four conditions that will be present for this to take place: it is task oriented in that the function of the group is limited; it is relatively small and homogeneous; there is a high degree of communication; and specialization is minimized.[113] Special Operations organizations and the GE example, both exhibit the some of the four conditions. The argument for cyberwarfare could also be made, however the diversity and technical expertise will certainly require more specialization within cyber teams. Applying some of the concepts to a larger group is a greater challenge, but David S. Alberts and Richard E. Hayes have done just that in a number of different research works for the Department of Defense. They have used the advantages of trust and using

---

[111] Jo Freeman, "The Tyranny of Structurelessness," *Berkeley Journal of Sociology* (1972), 152.

[112] Ibid.
[113] Ibid., 157.

decentralized methods of accomplishing tasks and looked to exploit advances in technology to mitigate some of the challenges in communications.

The Alberts and Hayes Model

One model that has looked to combine the power of trust with the availability of information in a military context was developed by Alberts and Hayes. Alberts and Hayes characterize the emergence of the information age as an "opportunity to leverage new sources of power to meet the challenges we face."[114] They caution against taking the path of least resistance and identify two distinct routes for consideration:

> One road, often called "modernization," is the straightest and most clearly signed. Traveling this road is clearly within the comfort zone of the institution (DoD) and most of its members. Unfortunately, this road will lead us only to incremental improvements and, ultimately, to a dead end… The other, less traveled road (actually it may appear more as a path) leads to a disruptive transformation of command and control (C2) that is central to all military organizations and processes, the first since the early to mid-19th century. This transformation must focus on C2, where information is translated into actionable knowledge. Without a transformation of C2, it is far less likely that we will be able to meet the challenges that lie ahead.[115]

They highlight the importance of transforming the mechanism that is C2 in order to "achieve the one organizational characteristic that is sure to stand us in good stead for the foreseeable future – *agility*".[116] As Alberts and Hayes identified in their *Network Centric Warfare* book in 1999: "One of the major lessons learned is that without changes in the way an organization does

---

[114] Alberts and Hayes, *Power to the Edge*, 3
[115] Ibid., 4.
[116] Ibid., 4.

business, it is not possible to fully leverage the power of information."[117] So, where many organizations are asking how can technology improve our processes, they could be asking how we can adapt our processes to take full advantage of the technology.

To influence a change in C2, it is first critical to understand the breadth of C2 and that it spans the four domains of war: physical, cognitive, emotional and information.[118] Alberts and Hayes developed a Value Chain in order to understand how information affects the different domains and how they may be exploited to improve operational outputs. Represented in Figure 2.1, the physical domain is where the actions are ultimately executed, the information domain includes the creation, sharing and processing of information, the cognitive domain is where decisions are made based on beliefs, values and perceptions and finally the social domain, is comprised of social interactions, systems or procedures for collaboration in order to share resources, awareness and understanding.[119]

---

[117] David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare : Developing and Leveraging Information Superiority*, 2nd Edition ed.Department of Defence, CCRP, 1999), 87.

[118] Alberts and Hayes, *Power to the Edge*, 14

[119] Ibid.

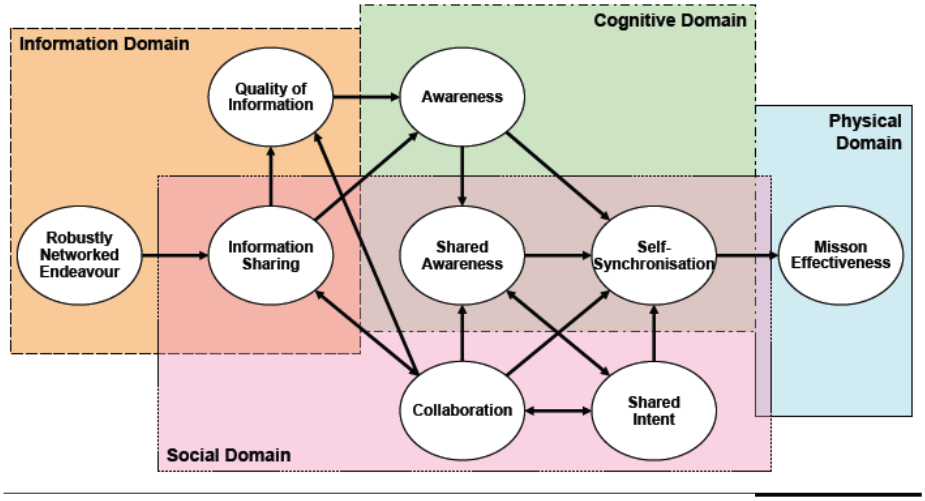

Figure 2.1. Network Centric Operations Value Chain
Source : Alberts, *Power to the Edge*, 14

As information becomes more and more pervasive and influential throughout the battle space, it is critical to understand ways that these complex challenges can be mitigated through agile C2. In a 2001 report to Congress on Network Centric Warfare (NCW), the power of harnessing this information was further stressed: "NCW represents a powerful set of warfighting concepts and associated military capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner."[120] The theory behind NCW is that decision quality information can be pushed across the battlespace

[120]Alberts, Garstka and Stein, *Network Centric Warfare : Developing and Leveraging Information Superiority*, si.

to whoever requires to make a decision and thus speeds up battle procedure leading to a military advantage.

Network Centric Warfare

As the foundation of many of their principles, Alberts and Hayes define NCW as follows:

> NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking—network-centric thinking—and applying it to military operations. NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[121]

The tendency with NCW is to think about the technical network, but clearly the way forward is to think of Networks as they pertain to human interaction and organizations. Alberts and Hayes cover this by saying: "NCW is more about networking than networks. It is about the increased combat power that can be generated by a network centric force…effective linking or networking of knowledgeable entities that are geographically or hierarchically dispersed. [122] In the report to Congress, Alberts et al emphasized a transformation from "today's platform-centric force into a network-centric one."[123] It also spelled out the tenets by which NCW would be identified:

---

[121] Ibid., 87.
[122] Ibid., 6-7.

[123] Department of Defense, United States of America, *Network Centric Warfare : Department of Defense Report to Congress* (DOD CCRP, 2001), si.

1. A robustly networked force improves information sharing
2. Information sharing enhances the quality of information and shared situational awareness
3. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
4. These, in turn, dramatically increase mission effectiveness[124]

Of course, a robustly networked force can only be achieved if there is interoperability between all of the different parties.[125] Interoperability is essentially the ability to work together and must be achieved in each of the four domains.[126] Interoperability is not a binary concept and in their book *Power to the Edge*, Alberts and Hayes, define four levels of interoperability. Using Command and Control on one axis and the increase of Situational Awareness on the other, a progression is mapped out in the Figure 2 below[127]:

[124] Ibid.
[125] Alberts and Hayes, *Power to the Edge*, 107
[126] Ibid., 109.
[127] Ibid., 281.

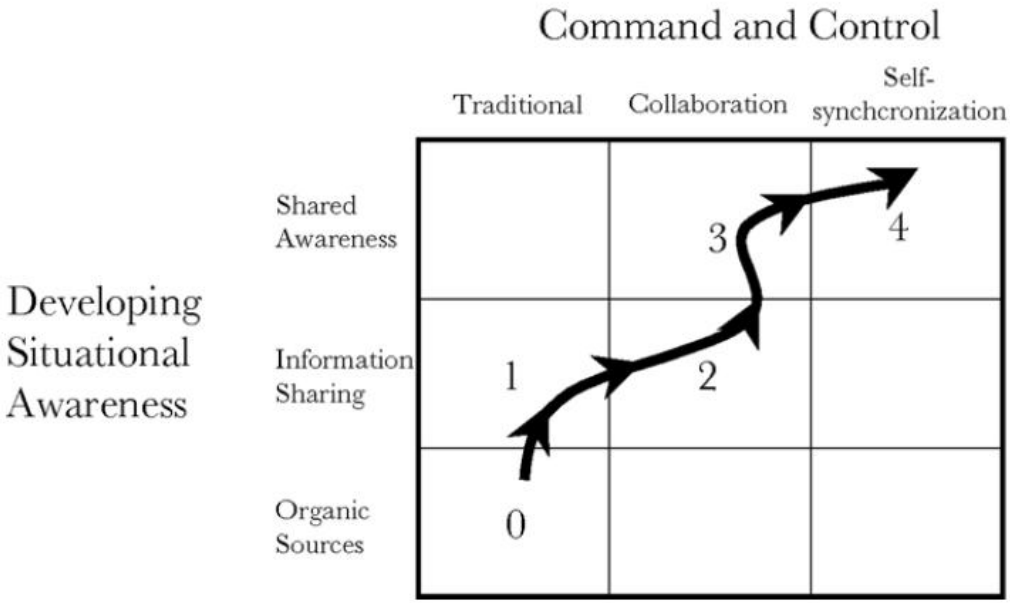

Figure 2.2. NCW Maturity Model
Source: Alberts, *Power to the Edge*, pg 109

In the maturity model presented in Figure 2, the goal is self-synchronization. Self-synchronization is a type of interaction between organizations based on highly decentralized C2 and autonomous action.[128] The idea of self-synchronization is only possible if there are certain tenets that are followed. They are :

1. Clear and consistent understanding of command intent;
2. High quality information and shared situational awareness;
3. Competence at all levels of the force; and

[128] David S. Alberts, Reiner K. Huber and James Moffat, *NATO NEC C2 Maturity Model* (Department of Defence, CCRP, 2010), 281.

4. Trust in the information, subordinates, superiors, peers, and equipment.[129]

It is also important to emphasize at this point that although the ideal of self-synchronization implies autonomous interactions, the authors clearly state the importance of commanders. However, in emphasizing the importance of the command intent and trust in the subordinates, they advocate that Commanders should be giving guidelines within which the tasks should be accomplished rather than providing the detail of how to do it.[130] There are clearly many similarities with this theory as with the various definitions of mission command discussed previously. Taking it a step further, self-synchronization is not to be regarded as a doctrine that will be used in every situation or by every commander, but it is a tool that can be extremely effective in solving problems in today's complex environment.[131] In a cyber context, a network defence specialist who clearly understands the limits within which they have the authority to operate will be more responsive in dealing with threats to the network.

The concepts of NCW and self-synchronization are both key in what Alberts and Hayes define as *the edge*. *Power to the Edge* is about optimizing traditional processes and conventional ways of thought. By providing individuals with increased access to information and eliminating non-contributing layers or "unnecessary constraints", they are empowered and the organization becomes more agile.[132] Commanders become responsible for setting the conditions for success

---

[129] Alberts and Hayes, *Power to the Edge*, 27.
[130] Ibid.
[131] Ibid.

[132] Ibid., 5.

and demonstrate their control through an expression of clear intent, a capacity to allocate resources dynamically and the establishment of parameters that allow forces to fight autonomously.[133] As they highlight in *Power to the Edge* "…our organizations, architectures and systems will no longer constrain the way that we accomplish command and control."[134]

In fact, in an effort to change the mindset and adapt the thinking behind C2, Alberts and Hayes proposed eliminating the terms Command and Control and using the terms Focus and Convergence.[135] They argued that older terms had lost their relevance over time, but because they were so ingrained in both the military psyche and doctrine, they were actually tied to the entire process.[136] So, command relationships are based around historical hierarchical examples, in order to ensure that there is *Command and Control* at each level, when there may be more efficient or effective ways to get there. They define the terms as follows:

> *Focus* as a replacement for command speaks directly to what command is meant to accomplish while being agnostic with respect to the existence of someone in charge or particular lines of authority. Similarly, *convergence* speaks directly to what control (the verb) is meant to achieve without asserting that control as a verb is possible or desirable. The combined term, *Focus & Convergence*, speaks to the existence of a set of dynamic interactions between the two functions.[137]

[133] Rules of engagement, standard operating procedures and other guidelines are examples of the parameters that would be considered in preparing a force to act autonomously. Ibid.

[134] Ibid., 32.

[135] David S. Alberts, "Agility, Focus and Convergence: The Future of Command and Control," *The International C2 Journal* 1, no. 1 (2007), 3.

[136] Ibid., 15-16.

[137] Ibid., 18.

C2 Agility is the desired effect through an optimized C2 (Focus and Convergence)[138] process. Agile organizations "are the result of an organizational structure, command and control approach, concepts of operation, supporting systems, and personnel that have a synergistic mix of the right characteristics"[139] The six components of agility are: adaptation, flexibility, robustness[140], innovation, responsiveness and resilience.

Operationalizing C2 Agility

In follow-on work in "Operationalizing C2 Agility"[141], Alberts defines C2 Agility: "…an entity's C2 Agility reflects an organization's or a Collective's ability to adapt its C2 or management approach to efficiently cope with or exploit changes in operational circumstances."[142] Adaptation of a C2 model or framework implies that there are several different ways to approach C2. Alberts and Hayes also identify a C2 approach space which they use to differentiate C2 approaches by three variables:

1. The degree to which information is distributed among entities;
2. The patterns of interactions among entities;
3. The degree to which decision rights are delegated by entities to the collective (the nature and extent to which decisions rights held by individual entities are transferred to the Collective).[143]

---

[138] Of note, replacing C2 with Focus and Convergence is really only prominent in one particular article. Even in articles by Alberts, following the one in question, they revert back to the terms Command and Control (C2).

[139] Alberts and Hayes, *Power to the Edge*, 303

[140] The attribute robustness has been replaced in the most recent literature by Versatility. Because this paper will make reference to earlier work, it will remain consistent throughout and refer to robustness. David S. Alberts, *The Agility Advantage : A Survival Guide to Complex Enterprises and Endeavours*Department of Defence, CCRP, 2011), 122.

[141] David S. Alberts, Reiner K. Huber and James Moffat, "Achieving Agile C2 by Adopting Higher Levels of C2 Maturity," *International Command and Control Research & Technology Symposium* (2012), 24 Nov 2012, 3.

[142] Ibid.

[143] Alberts, Huber and Moffat, *NATO NEC C2 Maturity Model*
, 51-63.

Using the variables, Alberts et al established five classes of C2 along the spectrum of agility; Conflicted C2, De-conflicted C2, Coordinated C2, Collaborative C2 and Edge C2.[144] They define the evolution of an organization with respect to the variables as maturity; where an increase in maturity along the spectrum meant a more agile organization.[145] An important distinction is that moving from one class to another does not mean a transformation in approach rather an additional C2 capability or approach then becomes available. For example, an organization capable of functioning in at the Collaborative C2 level is also capable of using a de-conflicted style if the situation dictates. The transition from one level to another is mapped out most easily in the Figure 2.3 below :

[144] Ibid.

[145] Alberts, Huber and Moffat, *Achieving Agile C2 by Adopting Higher Levels of C2 Maturity*, 24 Nov 2012, 10.

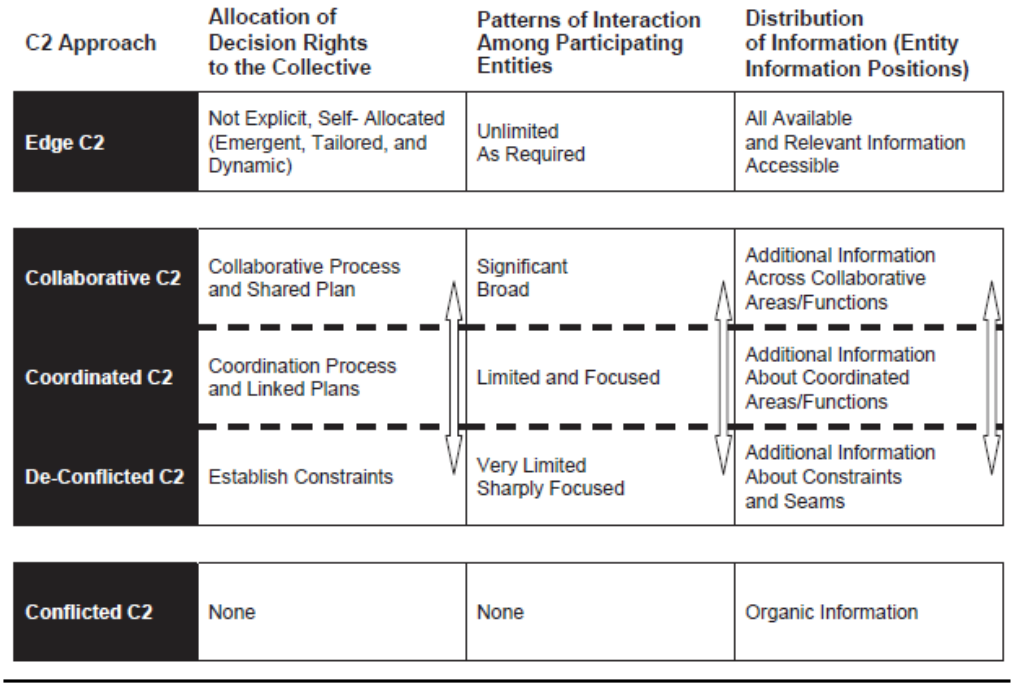

Figure 2.3. The different C2 approaches and how they relate to the C2 approach space
Source: Alberts, *Achieving Agile C2 by Adopting Higher Levels of C2 Maturity"*, pg 8

The spectrum can be visually represented by Figure 2.4 below:

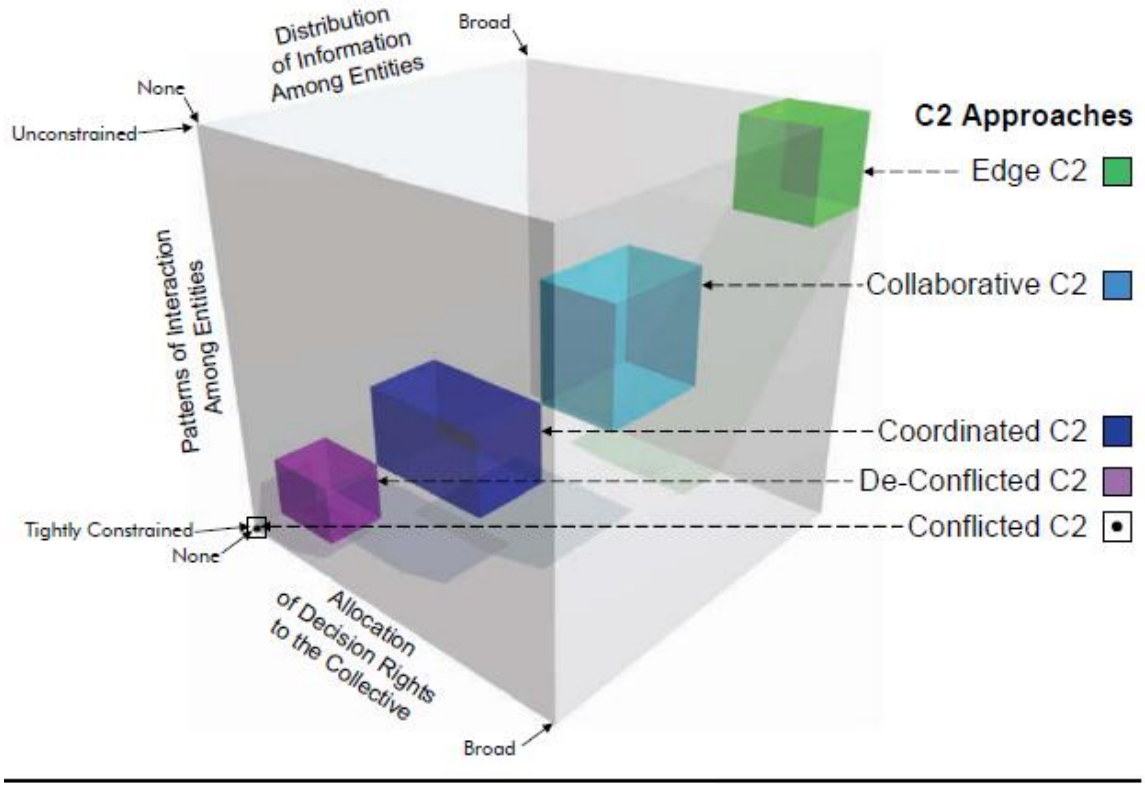

Figure 2.4. C2 Approaches and the C2 Approach Space
Alberts, *The Agility Advantage*, 316

In cyberwarfare, once the capability is developed and the trust is recognized throughout the organization, it should be capable of being a collaborative C2 organization, with some tasks that are self-synchronizing. Clearly, organizations of complete self-synchronization are exceedingly rare. Looking back at Freeman's article, two of the four conditions could be challenged with respect to cyberwarfare within the military context. While it would be difficult to consider the function of "cyber" as limited, under the larger umbrella, there will be more focussed tasks which will be conducted by experts in that domain; intrusion detection as an

example. However, the other conflicting characteristic is the specialization. Due to the complexity of the field, there will need to be experts in certain areas and because of the resources within the military that will make it difficult to have depth within a given specialization. For all of the positives that Alberts and Hayes identify in the Command model and the advantages highlighted by Covey and the GE example, there are many detractors from the "edge organization theory" as well as the central role that information plays in the conduct of command. NCW has been challenged since its inception, to the point where there are numerous variations of the term such as Network Enabled Operations, Network Enabled Warfare, which attempt to minimize the focus on the Network or simply change a term that has a negative connotation.

Counter to Network Centric Warfare

Martin Van Creveld distills the problem down to one sentence: "The history of command can thus be understood in terms of a race between the demand for information and the ability of command systems to meet it."[146] Van Creveld is skeptical of the advantage of technology and believes that in many ways the world has become too dependent on IS/IT. He sees the major challenge from commanders is differentiating the information required to make decisions from the massive amounts of data that is collected.[147] Van Creveld refers to the tactical level and the concept of "every soldier is a sensor". The concept makes sense, however, at the unit level, the staff does not possess the necessary tools or have the capacity to collect, collate and disseminate

[146] Allan D. English, Howard Coombs and Richard H. Gimblett, *Networked Operations and Transformation: Context and Canadian Contributions* (Montreal: McGill-Queen's University Press, 2007), 90.
[147] Ibid., 90-91.

the information. Despite his cautious view, Van Creveld believes that command "is predicated on communication, dissemination of intent, creation of shared awareness and decentralized decision making."[148] He identifies five principles for organizing command systems, which are extremely consistent with mission command:

1. Delegate decision making as low as possible to promote freedom of action
2. Organizations should encourage decentralization of decision making by structuring units at the lowest level to be capable of self-sufficiency in operations
3. Reporting and information systems need to work reciprocally throughout the organization
4. HQ must not rely on units to send information but maintain an active search capability outside HQ to supplement this information
5. formal and informal networks of communications must be maintained[149]

Other detractors from the NCW have similar arguments; too much information, encouraging micro-management and providing information for the sake of information. The irony is that these concepts contradict the problems that NCW is supposed to solve and the theories of the edge organization. Micro-management should not happen because the responsibilities have been decentralized and there is a level of trust that has been delegated to the subordinate commanders. Also, in an edge organization the theory is that the interactions between entities become natural so you learn where you need to go for information to solve specific issue. As Alberts says in *Power to the Edge,* a completely networked environment "fully enables all of the attributes of reach, richness, and quality of interactions, allowing the utility of the information exchange to be significantly increased…"[150]

[148] Ibid., 91.
[149] Ibid.

[150] Alberts and Hayes, *Power to the Edge*, 82

Conclusion

A revolutionary capability like cyber needs to be regarded in a unique manner. Solutions that have previously worked in a military setting will not necessarily be applicable to an environment like cyber. Military organizations are not traditionally flexible and adaptable, but to optimize the employment of cyberwarfare there needs to be creativity that is applied. Fortunately there are examples in the private sector and also in the military that are relevant to cyberwarfare.

Concepts that the private sector use to increase productivity and the bottom line can be leveraged in a military setting. The value or the "Speed" of trust is something that can be leveraged in the cyber environment. The nature of the cyber conflict is such that high level commanders will be required to make decisions on low level tactical actions. A streamlined process and a mutual understanding are crucial to be responsive and effective. This is a similar relationship to how SOF and from a command relationship perspective, the CF should explore the similarities more. The specialization of cyber operators is also a key characteristic in decentralizing of responsibilities. Whether it is Covey, Alberts and Hayes or Freeman, they all emphasize the importance of competence of the individuals in establishing trust.

Developing this foundation of trust is critical in order to leverage the effects of a decentralized cyber force. This trust can only be gained by developing an expert cadre of cyber soldiers and leaders. Similarly, there must be a common understanding between superior and subordinate organizations so that the military intent is what is actually executed by the operators. The next chapter will look at challenges in developing that trust as it is a unique endeavor. On top of the aspects of cyberwarfare, there are implications with the population demographics that

will impact the development of cyber-warriors and the interaction with leaders who employ cyber capabilities.

CHAPTER 3

A key piece of the continued growth of cyber as a domain is the understanding of how to develop and generate cyber-warriors. It is essential for leaders to do more than just observe the changing times, they must understand the changing times. Although the technological changes are what are pervasive in the media, some would argue that the demographic changes will have a more profound impact on our future.[151] At the very least, it will be a major factor that will compound the technical revolution in society and the RMA from a military perspective.

Within society there are a number of different theories which look at current demographics and information technology and how to optimize the development in this environment. People are working longer, there is a wider range of ages within the workforce and there is a gap of technical knowledge. These are all pieces that influence the dynamic between information technology and how people are able to use it. Whether or not the demographic trends are driving the gap in disparity of technical knowledge or they are one factor that is influencing it is a question that has been asked within the education profession, but the parallels can certainly be made with the military and specifically the CF.

This chapter will show that understanding who the potential cyber-warriors are will play a critical role in the education and training of cyber-warriors. In order to understand how the development of cyber-warriors is different from other soldiers it is important to understand the

---

[151] Mark McCrindle, *New Generations at Work: Attracting, Recruiting, Retaining and Training Generation Y* (NSW, Australia: McCrindle Research, 2006), 4.

demographics across the workforce. The current demographics of personnel in the CF and entering the CF will have a major impact on the development of cyber war in the CF.

Current Demographic Trends

Demographically, the world is going through unprecedented times. Figure 3.1 represents the age pyramid in the Canadian population. The predominant group, commonly referred to as the "baby boomers", is between the ages of 40 and 60. Over 50% of the workforce is over the age of 40.[152] This group is also currently making up the majority of the senior leadership positions across the workforce, making it difficult for the younger workers to break in. Australian social researcher Mark McCrindle looked at the relationships between demographic groups and technology and while his research is exclusively Australian, the trends are similar in Canada and other Western countries. He notes that the current situation in the workplace is completely unique as there are four generations in the workplace at the same time. This will prove to be more complex due to the pairing with the focus on information technology and the rapidly changing environment.[153]

---

[152] Adecco, "Managing today's Multigenerational Workforce," http://www.adecco.ca/en/knowledge-centre/employers/documents/whitepapers/managing-multigenerational-workforce.pdf (accessed 02/13,), 3.

[153] McCrindle, *New Generations at Work: Attracting, Recruiting, Retaining and Training Generation Y*, 4

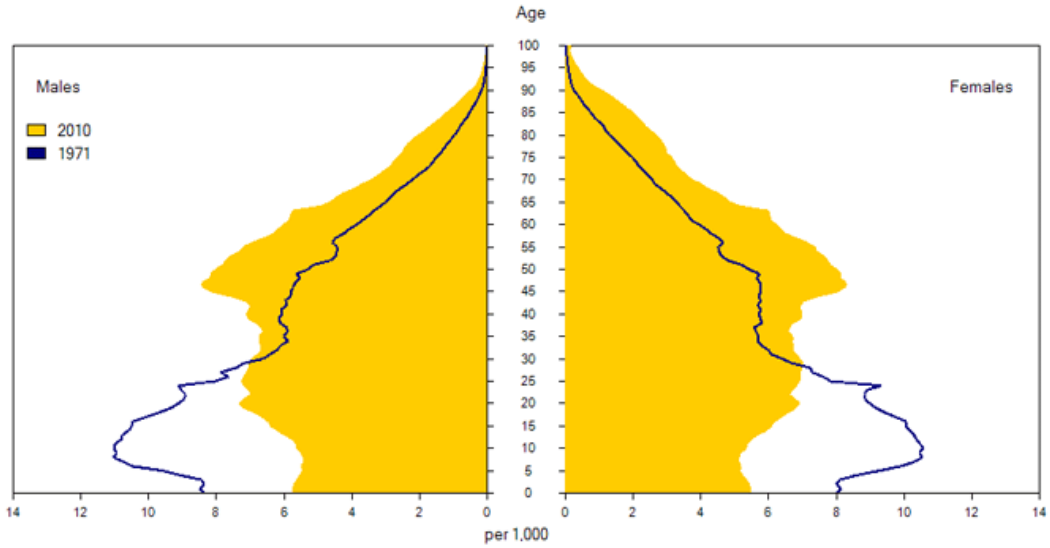

Figure 3.1 Age pyramid of population estimates as of July 1, 1971 and 2010, Canada
Government of Canada, http://www.statcan.gc.ca/pub/91-215-x/2010000/i003-eng.htm

However, technology has forced some new trends. Education in the cyber domain is the overriding factor in gaining expertise, consequently, experts in the field have both advanced and current education. This depth of knowledge doesn't necessarily correspond with work experience causing conflicting factors for technical leadership positions. McCrindle notes that while it isn't unique to have a mix of generations in the workplace, today the roles that individuals are filling are not necessarily based upon their age and experience. So in the past where a team lead would likely be the most senior and experienced member, today it could be a recent university graduate.[154]

[154] Ibid., 6.

While other organizations also experience challenges with getting, the problem is magnified in the military as it is a bottom-entry organization. The progression model requires individuals to pass through each of the different gateways, which takes time. In a commercial context it would not be uncommon to skip levels and get promotions faster, creating a greater diversity of age at the leadership level. The effect that this will have in the short term will be magnified by the confluence of the technological revolution and the current demographic phenomena of the baby boomers.[155]

In North America, another recent trend has been for individuals to extend their time in the workforce and not retire in the window that has previously been predicted. Pairing that with the population bubble that exists from age 40-60 and it is evident that the largest sector of the society has decided to work longer than had been predicted. There are several factors that have influenced this, but more than any was the decline of the global markets starting in September 2008. Ironically, the CF anticipated a completely opposite situation in 2002, stemming from the Auditor General's findings on military recruitment and retention. The predictions in that report anticipated a challenge in trying to promote both skilled officers and non-commissioned members as well as retain skilled members because of negative recruiting vs retention numbers.[156] One of the measures that was instituted to help mitigate the risk of a mass exodus was to raise the Compulsory Retirement Age (CRA) from 55-60 as well as rework the terms of

[155] Adecco, *Managing today's Multigenerational Workforce*, 16.

[156] Office of the Auditor General, "Chapter 5, National Defence – Recruitment and Retention of Military Personnel", *2002 Report of the Auditor General of Canada to the House of Commons* (Ottawa, Canada: Office of the Auditor General, April 2002, accessed 13 Feb 13), 13. Available from http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20060502ce.html/$file/20060502ce.pdf ;

service so members would be eligible to collect pension after 25 years of service rather than 20.[157] However, the mass exodus of the senior members did not occur. The results of a follow-up study in 2006 show that although the recruiting numbers have improved, they are barely capable of meeting the targeted intake numbers.[158] To summarize the overall effect, the leadership in the CF is comprised of people between the ages of 40 and 60. Not only is that group staying around longer and occupying critical positions, but they are a group that is not often considered to be expert in the information technology field. Some, like Prensky, believe that this is a generational difference that will only be resolved when the older generation accepts this and adapts.

Generational Differences

In 2001, educational expert, Marc Prensky penned a two-part article entitled *Digital Natives, Digital Immigrants*. The article is focused on education and the importance of adapting methods of instruction that were largely based on lecturing and learning to better fit with changing technologies. Prensky intended to show that without adapting the education system to the way that the current generation is learning, the education system has failed. However, in many ways, the lexicon that came out of the article is what is most referenced today. Prensky believes that there is a distinct difference in the way that generations learn based on the environment that they were raised; the generation that has grown up with technology (the digital

[157] Ibid, 13.

[158]Canada, Office of the Auditor General, "Chapter 2—National Defence—Military Recruiting and Retention " *2006 Report of the Auditor General of Canada to the House of Commons* http://www.oag-bvg.gc.ca/internet/English/parl_oag_200605_02_e_14959.html (accessed 4/18/2013, 2013).

natives), and those that have had to learn as the technology develops (the digital immigrants).[159] Prensky skillfully compares the challenges of digital immigrants in adapting to technology with an immigrant who has landed in a new country; forced to learn a completely new language, culture and customs.[160] He explains that as with immigrants into a new society, some are faster and more successful than others, and inevitably, the native "accent" is more apparent in some than others.[161]

The accent is a metaphor that clearly illustrates the transparency of an individual within a given group. In the case of the digital environment of computers, video games and the Internet, the accent manifests itself in digital immigrants through their ability to use the different tools in the way that they were intended. Prensky uses the example of individuals who need to print their email out in order to be able to read them as an example of an immigrant with a "strong accent".[162] Prensky's article was critical in defining some of the characteristics that actually define digital natives; what makes them unique. He highlights things such as being comfortable receiving information quickly, completing multiple tasks simultaneously, using graphical information before text and an aversion to learning through lectures and what he describes as "tell-test" instruction.[163]

---

[159] Marc Prensky, " Digital Natives, Digital Immigrants," *On the Horizon (MCB University Press)*, no. Vol. 9 No. 5 (October 2001), 1.

[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Ibid., 2.

Another implication of the word immigrant is that they are the outsider trying to become part of the society. Looking again at Prensky's example of teaching and learning, this is contrary to everything that we know as a society. Historically, with age came experience and knowledge and generally, the more experienced and knowledgeable members of society helped educate the younger, inexperienced members. This arrangement becomes paradoxical when the teachers are less informed than the students as it pertains to the way forward in a digital environment.[164] As Prensky asks and responds: "Should the Digital Native students learn the old ways, or should their Digital Immigrant educators learn the new? Unfortunately, no matter how much the Immigrants may wish it, it is highly unlikely the Digital Natives will go backwards."[165] Prensky's argument is based around the fact that there is clear dividing line between generations, making it clear on how to approach things in the future. However, there are many others that disagree with that characterization and believe that it is oversimplifying the issue.

Although Prensky's argument offers a clean break and catchy terms, several studies have shown that the data does not match his theory. Smith compiles a number of different research work that contradicts the binary nature of Prensky's theory. His argument likens the "Digital Native" debate to more of a "moral panic" than it is based on empirical data.[166] Smith refers to analysis from Bennett et al which states that there is evidence to prove that there is as much a

---

[164] Ibid., 1.
[165] Ibid.
[166] E. Smith, "The Digital Native Debate in Higher Education: A Comparative Analysis of Recent Literature / Le Débat Sur Les Natifs Du Numérique Dans l'Enseignement Supérieur: Une Analyse Comparative De La Littérature Récente," *Canadian Journal of Learning and Technology / La Revue Canadienne De l'apprentissage Et De La Technologie* 38, no. 3 (2012), 8.

difference in the adaptation of digital learning within the generations as there is between them.[167] He also argues that there is a lack of evidence that supports some of the characteristics that define the "Digital Native" generation.[168]

Does the generational divide actually add any value? Helsper and Enyon, of the London School of Economics, looked to add some scientific data to a discussion that has essentially been based on opinion to date.[169] They believe that it is not helpful to have this debate along generational divides.[170] They concede that age is a factor, but debate if it is any more important than other factors such as breadth of use of IT, experience, self-efficacy and education.[171] One conclusion that came out of their research is that "the stronger the person's education background, the more likely they are to feel confident" in the use of the Internet and IT tools.[172] The other conclusion from Helsper and Enyon is that there are no insurmountable challenges that exist, even though the largest group of Internet users and IT experts is younger.[173]

The rise of information technology has clearly been a catalyst for change in society and it is critical to understand that not everyone is equipped with the same skills or mindset to handle these changes. Trends today appear to be lasting, meaning that these are challenges that are going to have to be dealt with for the foreseeable future. A scale of technical proficiency with

---

[167] Ibid., 7.
[168] Ibid.
[169] Ellen Johanna Helsper and Rebecca Eynon, "Digital Natives: Where is the Evidence?" *British Educational Research Journal* 36, no. 3 (2010), 3-4.
[170] Ibid., 15.
[171] Ibid., 2.
[172] Ibid., 19.
[173] Ibid.

regards to IT, and age is certainly one of the pervading factors. There are a number of creative solutions to integrate generations into a workforce, however not all are applicable to the CF. McCrindle suggests that age is nothing but a number and the key to having an integrated workforce is to ensure that "interaction can take place, where those of different ages can mix and thus where inter-generational perspectives are shared."[174] Utilizing Mission Command and trusting technical experts to accomplish critical tasks as a key player on a team are ways that the military can incorporate some of these ideas, but in many ways the system that raises soldiers is not optimized for this. How can the military generate soldiers to become cyber-warriors?

Whether or not the Digital Native argument is accepted, it is clear that with the in this cyber environment, there will be people that are more adept with technology than others. From a military perspective it's crucial to be able to understand how best to prepare these individuals to optimize the effects that can be achieved. The development of the cyber-warrior will be different than that of the typical soldier as the responsibilities extend to a depth that has rarely been seen in the military. Prensky defined digital wisdom based on two principles; "the use of digital technology to access cognitive power beyond our innate capacity and prudent use of technology to enhance our capabilities."[175] The ability to leverage technology, but not be overwhelmed by it will be critical to soldier development as well. Across the board there is a push to prepare the CF population to respond to the complex challenges of today's environment and the two key aspects

---

[174] McCrindle, *New Generations at Work: Attracting, Recruiting, Retaining and Training Generation Y*, 6.

[175] Marc Prensky, "H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom. " *Innovate 5 (3)* (2009), 1.

of this are education and training. Horn describes training as a response to a predictable situation, whereas education is the ability to use reason to respond to an unpredictable situation. [176] Optimizing training and education for cyber-warriors is fundamental in creating an expert cadre of soldiers that can be trusted with the complex responsibilities within the cyber domain.

Cyber-Warriors

The nature of the cyber domain calls for a much more responsive education cycle as the techniques of cyberwarfare are changing at a rapid rate. Where the development of traditional weapons or tactics, techniques and procedures is usually conducted of a period of years, techniques in the cyber domain will change overnight and it will be imperative to remain current on these changes.[177] This requires a level of understanding of the physical sciences that is much more in depth as well. In the cyber environment, there are often counterintuitive results that can only be understood with a mastery of the basics. Miller states in his essay *Why your Intuition about Cyber Warfare is Probably Wrong :* "Weapons can be reproduced instantly, "bullets" travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen year old can command an army."[178] While there is some exaggeration for effect in his comments, the importance of having a detailed grasp of the environment, by the soldiers that will be responsible for defensive and offensive operations within the environment is not lost.

[176] Bernd Horn, "A Rejection of the Need for Warrior Scholars?" (2011), 49.

[177] Gregory Conti and David Raymond, "Leadership of Cyber Warriors: Enduring Principles and New Directions," *Small Wars Journal* (11 July 2011), 6.

[178] Miller, Brickey and Conti, *Why Your Intuition about Cyber Warfare is Probably Wrong*, 1.

Education must extend outside of the cyber community as well if the CF is going to be in a position to properly defend itself in the cyber domain. As discussed in Chapter 1, unlike conventional military operations, the cyber domain favors the attacker and everyone with access to the networks can be considered a cyber-warrior of some sort.[179] Whether at home, in garrison or on deployment a soldier needs to realize that if they are not cyber conscious, they could be the weakness in the armour that allows a cyber-attacker to gain access. The US has started to inculcate "cyber hygiene" into their basic training courses and often outsourcing some of the responsibilities to private industry who has the reach to keep abreast of new threats, where the military may be limited. [180] If the art of developing a cyber-warrior is the education, then the science is the training.[181] The military is generally an institution that is exceedingly comfortable in this realm, but for the cyber example, traditional methods may not be ideal.[182]

Traditionally, military training has been relatively standardized and looked to institute basic skills through repetition and build physical and mental toughness by depriving candidates of necessities such as food and sleep while having them complete arduous tasks.[183] This will not be the most successful way to develop and judge cyber-warriors or their leaders. The focus of developing a cyber-warrior should be placed on the intellect and technical abilities, rather than the physical. But the training should remain challenging.[184] The top intellectual minds will only

[179] Amber Corrin, "US Military's Basic Training Now Includes Cyber Education," *Defense Systems* (Nov 28, 2011), 1.

[180] Ibid., 4.
[181] Ibid., 3.
[182] Conti and Raymond, *Leadership of Cyber Warriors: Enduring Principles and New Directions*, 7.
[183] Ibid.
[184] Ibid.

be attracted to the highest challenges in their field, so it behooves the military to provide that environment.

Like experts in any community, the cyber experts want to be challenged and will find a place that will offer that to them. In studies on why so many of the top technical minds have been drawn into hacking, the findings were that the individuals were so intrigued by the field that they wanted to continually challenge themselves. They were willing to research and experiment on their own and eventually, the ultimate challenge became to prove their capabilities in a live environment.[185] In order to attract the types of individuals that the CF will need to have success in the cyber domain, we must foster an environment that challenges people and allows them to work at the cutting edge of the capability. The cyber domain touches each of the other four domains of war, so it is critical that responsibility runs across the CF and not just the "Signals" community.[186] Sharing ownership of the problem is one of the challenges to overcome, however some of the others are directly related to the demographics within the CF and some specific traits of cyber-warriors.

Leaders at any level are a result of a variety of experiences that they have had throughout their lives, both professionally and personally. However, based on a combination of the age of senior leadership and the nascent stages of cyberwarfare that has been employed to date, there

---

[185] Zhengchuan Xu, Qing Hu and Chenghong Zhang, "Why Computer Talents Become Computer Hackers," *Communications of the ACM* 56, no. 4 (2013), 69.

[186] Jon Brickey et al., "The Case for Cyber," *Small Wars Journal* (September 13, 2012), 5.

are very few leaders that have actual experience in the cyber domain.[187] Therefore, the experience that has formed these leaders may not hold for training of cyber soldiers. What current leadership may define as important leadership qualities such as presence and physical fitness will be less important than technical expertise in the cyber context.[188] This will also have an effect on the team dynamic; technical expertise will often be the overwhelming factor in solving problems and therefore, emergent leadership within that environment will be more prevalent than in conventional military tasks.[189] However, the importance of technical expertise will need to be balanced with an understanding of the operational side. There is always a danger of specialists becoming submersed in their field and ignoring that they are one component to a larger machine. The mutual understanding piece of mission command doctrine will also depend on a common appreciation of how the chain of command functions, so while the importance of knowledge is critical it cannot be all encompassing for cyber leaders.

As a leader in the cyber domain, understanding where you are able to add value within the greater plan and that cyber capabilities will require support from other arms is key. Equally important is the ability to communicate this to a non-technical audience. In order to ensure that the cyber component is optimized within a plan, the leader will need to be able to clearly articulate the effects that can be achieved and the support that will be required.[190] With an understanding that cyber weapons could be used in a strategic sense, the absence of a leader's ability to correctly communicate this could lead to sub-optimal employment of the assets or

---

[187] Ibid., 1.
[188] Conti and Raymond, *Leadership of Cyber Warriors: Enduring Principles and New Directions*, 1.

[189] Conti and Raymond, *Leadership of Cyber Warriors: Enduring Principles and New Directions*, 5-6.
[190] Conti and Raymond, *Leadership of Cyber Warriors: Enduring Principles and New Directions*, 6.

worse could have an unintended strategic effect. The ability of technical officers to communicate effects to operators is similar within supporting trades such as signals or logistics, however, with cyber the technical complexity can make it difficult to simplify and over-simplification could lead to mis-understanding. Further, the cyber capability can be considered closer to a weapon than a supporting function. This last topic will be explored further in chapter four.

Conclusion

We are currently in the midst of several demographic phenomena. The workforce is getting older, people are working longer and there is a wide range of technical expertise across the workforce. Clearly each of these factors plays a role in the development of a cyber-capability and specifically the generation of cyber soldiers, so a greater understanding will lead to a significant benefit in this development. It is easy for an organization like the CF to continue developing soldiers with methods that have worked for years, but in a changing population this may miss some important opportunities.

This range of expertise is not binary or based on generations and it is something that can be developed. But there is a range and failing to recognize this and mitigate will lead to a sub-optimized cyber capability. The mitigation strategy has to include training and familiarization across the organization. This is not a problem that can be resolved in the technical community in the military, ownership must be shared throughout. Development of cyber operators needs to consider the primary roles that they play and the strengths that should be sought and not necessarily develop these specialists in the same vein as every other soldier.

Understanding that the optimal employment of cyber forces hinges on the trust in cyber-warriors to complete tasks and achieve military effects based on a commander's intent. The cultivation of this trust will only happen through training and education that can produce soldiers that are expert in the tasks they are to achieve. It is also essential for leaders to have the ability understand a certain depth of technical information. With the responsibility of having strategic impacts, leaders will only be able to have the confidence to make these decisions if they have a technical appreciation for the problem. How to best employ cyber assets will be explored in the next chapter through a comparative analysis.

CHAPTER 4

This paper has established that the advent of the cyberwarfare has led to a Revolution in Military Affairs. It has showed that decentralization and the power of trust will optimize the employment of cyberwarfare. It has also linked the state of the workforce demographic to the development of cyber-warriors. The final chapter will look at where cyber fits within a combined arms conflict. Is it an airplane or a gun? Is it a tool that can be leveraged to strategic effect or is it a key enabling tool?

Retired Col and military analyst Fred Schreier believes "[c]yberpower is technically, tactically and operationally distinct from the other instruments of military power. But it is not beyond strategy."[191] He also notes that while the land, air, sea and space are able to generate effect in other domains, cyberpower is unique in the way it can simultaneously and unequivocally generate strategic effect across all of the other domains. Cyberpower has become an instrument that needs to be considered in each type of conflict and at each level of war.[192] What is the optimal way to achieve this?

The opinion on how cyberwarfare can be employed ranges from strategically dominant in the vein of nuclear weapons to a complimentary asset which can improve the chances of success when paired with other kinetic tools. Although there are limited examples of the employment of

---

[191]Fred Schreier, *On Cyberwarfare* (DCAF, 2012), 18.
[192] Ibid., 16.

cyber-attacks, even using the concrete examples to deduce where cyber sits does not yield clear answers due to the ambiguous nature of the actions and the unknown intent.

This chapter will show that the show that the while cyber capabilities are optimally employed as a supporting arm, it can also be a principle asset in a strategic military act. A comparative analysis with familiar capabilities, airpower, nuclear weapons and electronic warfare will help illustrate how best to categorize this unique capability.

Cyber vs Nuclear

The first is the comparison between cyberwarfare and nuclear war can be broken down to essentially having a single weapon that can have strategic effects with a single action. The nuclear weapon is the single most lethal weapon with a level of destruction that is unparalleled. Despite the awesome power of nuclear weapons there are numerous experts and high ranking politicians that have warned of a potential similar effect through cyberwarfare. Panetta spoke of an electronic " Cyber Pearl Harbor" and cyber-attacks being as destructive or worse than 9/11.[193] Mike McConnell, former Director of the National Security Agency and Director of National Intelligence says that cyber carries a similar weight as a nuclear attack due to the effect that it can have on the economy and the psychology of a nation.[194] Russian Deputy Chief of the General Staff Alexander Burutin said that wars are changing from using destructive measures to defeat the adversary to suppression of the adversary's state and military controls through the

[193]Panetta, *Defending the Nation from Cyber Attack*

[194] Mike McConnell, *The Road to Cyberpower: Seizing Opportunity while Managing Risk in the Digital Age* (Booz Allen Hamilton, 2011).

manipulation of information and communications systems. [195] Although each of the three men hold a prominent place in their country's respective national security apparatus, the analysis on the academic side makes it sound more like rhetoric than fact.

One of the major counter-arguments for cyber is that a cyber-attack is not capable of mass destruction or catastrophic effect. The effect of a nuclear weapon has been demonstrated, but the potential effect of a cyber-weapon is still very much an unknown. Theories that have been floated are often considered exaggerated.[196] There have been limited cyber-attacks that have been documented and even the most well publicized cyber operation, Stuxnet, achieved physical effects, but not destruction on parallel to a nuclear strike. No demonstrable effect means that there is no reason to have the same level of fear as with a nuclear weapon. As Libicki states, for cyber to be an effective strategic weapon: "it has to be frightening to the population at large, or at least to their leaders – so frightening that the aggressors can actually reap some of the gains from the reaction or concession of their targets." However, experts like Libicki believe that cyberwarfare can generate fear and cause deterrence, but it comes from uncertainty rather than understanding of the potential nuclear destruction from a nuclear weapon.[197]

Cyber vs EW

This brings up the second case, cyber strictly as a supporting weapon. Used correctly and it will be a force multiplier and increase the chances for success of a mission. Libicki believes

[195] Krepinevich, *Cyber Warfare: A "Nuclear Option"?*, 14.
[196] Schreier, *On Cyberwarfare*, 25.

[197] Libicki, *Cyberwar as a Confidence Game*, 132.

that in that vein it could have a very similar role to Electronic Warfare (EW).[198] It should be considered a force-multiplier when paired with other military assets to achieve joint effects. Like EW, the targets would be at the tactical and operational level of war, so direct strategic effects would not be achieved.[199] Libicki believes that dependence on technology within militaries can become a target for cyber-attacks. And understanding this, technological inferior adversaries are likely to lose confidence in many of those systems at critical times in the battle. So instead of attacking the fear of the adversary you are attacking the confidence in a specific system.[200] As Libicki says "A cyber-attack that disables some infrastructure says as much about its reliability—the liability of those who own, operate, or stand behind such infrastructures—as a physical attack." So, essentially, cyber deterrence could be achieved by proving to an adversary that they are vulnerable with certain infrastructure leading them to lose confidence in it. There are other variations of Libicki's perspective that are consistent with cyber being a supporting asset.

Others like Schreier believe that cyber will remain a "complimentary instrument" until it has proven to be a coercive capability.[201] He cites the cyber-attacks in Georgia, Estonia and Stuxnet as examples where cyber has been disruptive and has even caused physical damage, but has not incited a response from the adversary or caused an adversary to concede to the attacker's demands.[202] This may be a function of the lack of commitment on the part of the attacker; if they

[198] Ibid., 134.
[199] Ibid.
[200] Ibid., 139.

[201] Schreier, *On Cyberwarfare*, 16.
[202] Ibid.

have not identified themselves how do they communicate what exactly it is they desire?[203] Without this coercive capability, cyber objectives are more likely to be at the operational and tactical levels. In fact, Thomas Rid from King's College London, has distilled cyber tasks down to three activities: subversion, espionage and sabotage.[204] Rid reviews each of the reported cyber-attacks to date, shows how none of them should be considered acts of war, on their own and classifies each under one of the three supporting activities. His example of Op ORCHARD provides an excellent illustration of an enabling activity

Operation ORCHARD shows the power of integrating cyber capability into a combined arms strike and how it can be used in a sabotage role. Although much of the detail is based on speculation, as the Israelis have never published how they accomplished the mission, they were allegedly able to penetrate Syrian air space with bombers and destroy their strategic target, a nuclear reactor site, without being detected by Syrian air-defence, one of the most capable in the world.[205] The understanding is that an Israeli cyber unit was able to penetrate the Syrian computer network and plant a "kill switch" to the air-defence network. Prior to launching the air assets, the cyber unit hit the kill switch disabling the air-defence assets and allowing the Israeli jets to reach their target undetected.[206] This shows that having cyber as an integral part of the combined arms fight will allow a force to achieve objectives that would be unattainable or

[203] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? the Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012), 416.

[204] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012), 7.

[205] Ibid. 16-17.

[206] Ibid.

extremely difficult without it. It gives an additional level of access to targets throughout the other domains. But is this this limit of cyber capability? Can cyber play a lead role in operations?

Cyber vs Air

The third and probably the most popular comparison is with the birth of airpower. The comparison with airpower is certainly one that is appreciated in the cyber community. In fact, current director of the National Security Agency (NSA) and Commander of US Cyber Command General Keith Alexander says that the current challenges faced today are "strikingly similar" to what the US military faced from 1919-1938. He recalls the struggle that the military had with mechanization and adapting to an increasingly mobile military force. Alexander insists that like airpower, cyber is a capability that wasn't considered relevant to military plans until advances in technology made it a requirement.[207] In the early application of air assets, the primary role was information gathering and reconnaissance, similar to the initial uses of cyber technology. Following WWI, experts in air power theory asserted that air forces had the potential to achieve strategic effects independent of land and sea forces. With the newly acquired reach, airplanes would be able to strike the enemy in depth and cause catastrophic destruction.[208] Alexander highlights the "20 years of struggle" that the air force went through in order to make the advances required to contribute operationally and tactically in WWII and cautions that with the speed of change in the world today, we don't have 20 years to take the same action with cyber.[209]

---

[207] Krepinevich, *Cyber Warfare: A "Nuclear Option"?*, 20.
[208] Ibid., 21.
[209] Keith B. Alexander, "Warfighting in Cyberspace," *National Defense Univ, Washington DC Inst For National Strategic Studies* (2007), 4.

It is slightly misleading to make the comparison with the birth of air power, as the vision of many of the air enthusiasts has never come to fruition. Are we comparing to where air enthusiasts *believed* airpower would go or where it *actually* went. To this day, it is arguable if there has ever been a strategic catastrophic destruction that has been inflicted by air assets alone.[210] OP UNIFIED PROTECTOR in Libya 2011 is a great example of the capabilities of airpower as it was clearly the overwhelming component of the campaign which contained "limited boots on the ground".[211] However, there were significant commitments by the navy, which helped with the staging of air assets, developed the intelligence picture and enforced the sea embargo. [212] SOF also played a critical role in targeting for the air assets as well as being the liaison force with the Libyan Rebel forces which acted as a proxy ground force.[213] But the role of the Air Force is clearly more than a supporting role within a combined arms fight or a *complementary instrument*. Can cyber be considered at that level?

The example of Stuxnet does show that cyber can be a primary instrument in an attack, which is more similar to the airpower than it is to a supporting function such as EW. Stuxnet was more than a standalone cyber-attack. It was a combined attack from Israel and the US that required significant development of the target through both Human Intelligence sources and

---

[210] Krepinevich, *Cyber Warfare: A "Nuclear Option"?*, 21-23

[211] Timothy E. Book, *NATO's Air War in Libya: A Template for Future American Operations* (2012), 62-66.

[212] Ibid.

[213] Sean Rayment, "How the Special Forces Helped Bring Gaddafi to His Knees-," *The Telegraph* (28 Aug 2011).

cyber intelligence.[214] But the effect of sabotaging the systems at Natanz was ultimately achieved through cyber means.

Conclusion

As cyberwarfare is a unique capability it is challenging to compare with the warfare in the other domains. Parallels with air, land sea and space do not translate very easily as the cyber domain is not based on such concrete dimensions and visual results. The relatively small number of examples to draw on is also difficult to come to conclusions as it certainly does not tell the entire story of what cyber capability will some time become. This unknown has opened the door for people to judge the effects of cyber over a large scale of options; from the sensational comparison to nuclear weapons to a supporting function that will only enable other destructive weapons.

While cyberwarfare is likely to be employed in a supporting role it is clearly unique when compared to a traditional supporting function like EW. The reality of where cyberwarfare employment fits likely lies somewhere in between those two extremes. It has clearly proven that it can be a disruptive tool when employed during the Georgia and Estonia conflicts. It has been demonstrated that cyber can be a bridge to targets that were otherwise unattainable as it was in Op ORCHARD. Cyber-weapons have been used as a primary instrument in achieving a strategic effect as was the case in Stuxnet.

---

[214] Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power*, 195.

As was the case with Air Power during the inter-war period, the imagination of cyber-enthusiasts has shown few limits. However, we may never know what the true impact that cyberwarfare can have until it is demonstrated. To date, we have seen that cyber can be a valuable contributor in a number of different areas and with the attention that has been placed on the domain it has the potential to expand significantly.

CONCLUSION

The capabilities of cyberwarfare have revolutionized warfare for the future. The effects that cyber brings to the fore are unique and far reaching. The cyber domain has unprecedented ties to the other domains of warfare as cyber activities can have influence across land, sea, air and space domains. The traditional nature of state on state conflict is transforming and cyber is one factor that is influencing this change. The lines between state organization, private companies and even criminal organizations have become blurred which adds additional layers of complexity to the conduct of war.

With the increased complexity and ambiguity of cyber employment it is more critical than ever to have an understanding of the capabilities that cyberwarfare can offer, but also the potential risks that are being taken by using it. Moving forward, cyber will need to be a consideration for planners at tactical, operational and strategic levels of war. Platoon commanders will need to consider defense against cyber-attacks and operational commanders will need to figure out how best to integrate cyber effects into the overall campaign.

Commanders will also need to be innovative in the ways that cyber is employed. The cyber problem is unique and will therefore require a unique method to solve. Leaders need to understand the institution of the military in order to be able to shape it to have the greatest effect with cyberwarfare. Cyber is an unconventional capability, so the employment of cyber assets is also likely to be unconventional. Lessons from the private sector can be ported to military organizations. Private companies are continually looking for ways to maximize effect in the form of making more money. One of the ways that this is accomplished is through the development

and fostering of trust. However, there are a number of parallels that already exist within the military. Mission command is based on mutual trust and mutual understanding of commander's intent.

As with the institutional approach the same can be said at the individual level. Cyber leaders and soldiers will not necessarily possess the same traits as the prototypical infanteer. Intellect and technical expertise are crucial in developing successful cyber-warriors and much of the physical skills that are a standard part of basic soldier skills will be less important. The demographics combined with the gap of technical knowledge across the military will also be a challenge to be dealt with. Leaders will need to be somewhat versed in cyber technology in order to have the confidence to employ the asset correctly. Cyber-attacks can potentially have strategic impacts, so understand the potential risks when employing cyber-weapons is a responsibility that commanders must respect.

The capabilities that cyber brings to the table are significant for commanders. Cyber-attacks can be used as a primary instrument in targeting strategic objectives. Paired in a combined arms fashion, cyber assets can facilitate access to targets that would have previously been impossible to strike. It can also be a critical enabler in creating disruption in and shaping the environment for and other military options.

Cyber is a complex capability that needs to be understood in order to be employed correctly. It can provide revolutionary effects on the battlefield if leaders are able to take advantage of the tools that they have at their disposal. With a unique capability you need to

consider innovative options and cyber is an opportunity for militaries to take a hold of the changing global environment.

BIBLIOGRAPHY

"Canada's Cyber Security Strategy " , accessed 4/14/2013, 2013, http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx.

"Cyber Crime – A Growing Challenge for Governments | KPMG | GLOBAL " , accessed 4/8/2013, 2013, http://www.kpmg.com/global/en/issuesandinsights/articlespublications/pages/cyber-crime.aspx.

"Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually " , accessed 4/8/2013, 2013, http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

RSA 2012 Cybercrime Trends Report : EMC Corporation, 2012.

"The Times they are A-Changing: A Few Thoughts on American Military Discipline and Organization." *Small Wars Journal* (22 March 2013, .

"A Walk on the Dark Side : These Badhats may have Bought Your Bank Account." *The Economist* (Aug 30th 2007, 2007).

"Where is Lt Zuckerberg?" Small Wars Journal (2/10/2013) .

Adecco. "Managing today's Multigenerational Workforce." , accessed 02/13, , http://www.adecco.ca/en/knowledge-centre/employers/documents/whitepapers/managing-multigenerational-workforce.pdf.

Alberts, David S. *The Agility Advantage : A Survival Guide to Complex Enterprises and Endeavours* Department of Defence, CCRP, 2011.

———. "Agility, Focus and Convergence: The Future of Command and Control." *The International C2 Journal* 1, no. 1 (2007): 1-30.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare : Developing and Leveraging Information Superiority*. 2nd Edition ed. Department of Defence, CCRP, 1999.

Alberts, David S. and Richard E. Hayes. *Power to the Edge* Department of Defence, CCRP, 2003.

Alberts, David S., Reiner K. Huber, and James Moffat. "Achieving Agile C2 by Adopting Higher Levels of C2 Maturity." *International Command and Control Research & Technology Symposium* (2012): 24 Nov 2012.

Alberts, David S., Reiner K. Huber, and James Moffat. *NATO NEC C2 Maturity Model* Department of Defence, CCRP, 2010.

Alexander, Keith B. "Warfighting in Cyberspace" *National Defense Univ Washington Dc Inst for National Strategic Studies* (2007).

Armour, Stephanie. "Generation Y: They've Arrived at Work with a New Attitude." *USA Today* 6, (2005).

Barno, David W. "Loss Leader ." *Foreign Policy* no. March 29, 2013.

———. "Military Brain Drain." *Foreign Policy* no. February 13, 2013.

Bates, Marcia and Mary Niles Maack. *Complexity and Self-Organization* Free University of Brussels, 2008.

Bennett, Sue and Karl Maton. "Beyond the 'digital Natives' Debate: Towards a More Nuanced Understanding of Students' Technology Experiences." *Journal of Computer Assisted Learning* 26, no. 5 (2010): 321-331.

Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies* 35, no. 5 (2012): 689-711.

Bittman, Michael, Leonie Rutherford, Jude Brown, and Lens Unsworth. "Digital Natives? New and Old Media and Children's Outcomes." *Australian Journal of Education (ACER Press)* 55, no. 2 (11, 2011): 161-175.

Book, Timothy E. *NATO's Air War in Libya: A Template for Future American Operations* (2012).

Brickey, Jon, Jacob Cox, John Nelson, and Gregory and Conti. "The Case for Cyber." *Small Wars Journal* (September 13, 2012, .

Canada. *Leadership in the Canadian Forces: Conceptual Foundations*, edited by Canadian Forces Leadership Institute, edited by Department of National Defence. Ottawa, ON: Canadian Forces Leadership Institute, 2005.

Canada, Department of National Defence. *CF Integrated Capstone Concept*. Winnipeg, MB: Chief of Force Development, 2010.

Canada, Office of the Auditor General. "Chapter 2—National Defence—Military Recruiting and Retention ", accessed 4/18/2013, 2013, http://www.oag-bvg.gc.ca/internet/English/parl_oag_200605_02_e_14959.html.

Canadian Forces Leadership Institute. *Duty with Honor : The Profession of Arms in Canada 2009* Chief of Defence Staff by the Canadian Defence Academy - Canadian Forces Leadership Institute, 2009.

Collins, Jim. "Level 5 Leadership: The Triumph of Humility and Fierce Resolve." *Harvard Business Review* 83, no. 7 (2005): 136.

Conti, Gregory and David Raymond. "Leadership of Cyber Warriors: Enduring Principles and New Directions." *Small Wars Journal* (11 July 2011, .

Cook, Thomas, Howard Taylor, Gregory Conti, and James Caroland. "Self-Development for Cyber Warriors." *Small Wars Journal* (10 Nov 2011, 2011).

Corrin, Amber. "US Military's Basic Training Now Includes Cyber Education." *Defense Systems* (Nov 28, 2011).

Covey, Stephen R. and Rebecca R. Merrill. *The SPEED of Trust: The One Thing that Changes Everything* Free Press, (2006).

Creveld, Martin van. *Command in War* Harvard University Press,.

Day, D. Michael and Bernd Horn. "Canadian Special Operations Command: The Maturation of a National Capability." (2010).

Dempsey, Martin E. "Mission Command." *Army* 61, no. 1 (Jan 2011, 2011): 43-44.

Department of Defense, United States Air Force. *Air Force Doctrine Document 3-12* 2010.

du Plessis, A. and P. Webb. "Digital Immigrant Teacher Perceptions of an Extended Cyberhunt Strategy." *Australasian Journal of Educational Technology* 28, no. 2 (01/01, 2012): 341-363.

English, Allan D., Howard Coombs, and Richard H. Gimblett. *Networked Operations and Transformation: Context and Canadian Contributions* . Montreal: McGill-Queen's University Press, 2007.

Farwell, James P. and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4 (2012): 107-120.

Fishman, Charles. "Engines of Democracy." *Fast Company* 28, no. 174 (1999): 33.

Flynn, Michael T., James Sisco, and David C. Ellis. ""Left of Bang": The Value of Sociocultural Analysis in Today's Environment." *Prism : A Journal of the Center for Complex Operations* 3, no. 4 (Sep 2012, 2012): 13-21.

Forbes, Phillip P. "Son of SPECOPS: Rethinking the Nature and Operationalization of Cyberspace" Naval War College, 2012.

Franklin, David M. "US Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institutionalization of Cyber Coordinating Authority." *National Defense Univ Washington DC Inst for National Strategic Studies* (2010).

Freeman, Jo. "The Tyranny of Structurelessness." *Berkeley Journal of Sociology* (1972): 151-164.

Haddick, Robert. "This Week at War: Their Own Private Internet." *Small Wars Journal* (August 27, 2010, .

Hayden, Michael V. "The Future of Things "cyber"." *Strategic Studies Quarterly* 5, no. 1 (2011): 3-7.

Helsper, Ellen Johanna and Rebecca Eynon. "Digital Natives: Where is the Evidence?" *British Educational Research Journal* 36, no. 3 (2010).

Horn, Bernd. "A Rejection of the Need for Warrior Scholars?" (2011).

Hruska, Joel. "US Cyber Command Admits Offensive Cyberwarfare Capabilities, Fundamental Shift in US Doctrine - HotHardware " , accessed 4/8/2013, 2013, http://hothardware.com/News/US-Cyber-Command-Admits-Offensive-Cyberwarfare-Capabilities-Fundamental-Shift-In-US-Doctrine/.

Jeffery, Michael K. "Inside Canadian Forces Transformation." (2010).

Jonathan Kirshner. "Globalization, American Power, and International Security." *Political Science Quarterly* 123, no. 3 (Fall 2008, 2008): 363-389.

Jones, Chris and Shao, Binhui. "The Net Generation and Digital Natives: Implications for Highereducation."Higher Education Academy, York, 2011.

Jones, Cynthia M. "Utilizing the Technology Acceptance Model to Assess Employee Adoption of Information Systems Security Measures." D.B.A., Nova Southeastern University, 2009.

Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate." *Journal of Strategic Studies* no. ahead-of-print (2013): 1-9.

Keen, Andrew. "Solving 'the Google Problem' Key to Ensuring the Internet's Success - CNN.Com " , accessed 2/27/2013, 2013, http://www.cnn.com/2012/12/06/opinion/andrew-keen-google-antitrust/.

Kiras, James D. *Special Operations and Strategy: From World War II to the War on Terrorism (Cass Series: Strategy and History)*. New York, NY: Routledge, 2006.

Kluver, Randy. "Globalization, Informatization, and Intercultural Communication." *American Communication Journal* no. Vol. 3 Issue 3, p1 (June 2000, .

Kohlmann, Benjamin. "The Military Needs More Disruptive Thinkers." *Journal Article April* 5, no. 4 (2012): 36am.

Krepinevich, Andrew F. *Cyber Warfare: A "Nuclear Option"?* CSBA, 2012.

Lambeth, Benjamin S. "Airpower, Spacepower, and Cyberpower." *Joint Force Quarterly* 60, (2011): 46-53.

Lauder, Matthew. "Systemic Operational Design: Freeing Operational Planning from the Shackles of Linearity." (2009).

Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." *Isjlp* 8, (2012): 325-439.

———. "Cyberwar as a Confidence Game." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011, 2011): 132-146.

———. "The Nature of Strategic Instability in Cyberspace." *The Brown Journal of World Affairs* 18, no. 1 (Fall 2011, 2011): 71-79.

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

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? the Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (2012): 401-428.

Liles, S., M. Rogers, JE Dietz, and D. Larson. "Applying Traditional Military Principles to Cyber Warfare."IEEE, 2012.

Limer, Eric. "Meet Red October: The Global Cyber-Espionage Ring that Spent 5 Years in the Shadows " , accessed 4/8/2013, 2013, http://gizmodo.com/5975793/meet-red-october-the-global-cyber+espionage-ring-that-spent-5-years-in-the-shadows.

McConnell, Mike. "Mike McConnell on how to Win the Cyber-War we're Losing." *Washington Post* 28, (2010): B01.

———. . *The Road to Cyberpower: Seizing Opportunity while Managing Risk in the Digital Age*: Booz Allen Hamilton, 2011.

McCrindle, Mark. *New Generations at Work: Attracting, Recruiting, Retaining and Training Generation Y*. NSW, Australia: McCrindle Research, 2006.

McRaven, William H. and William H. McRaven. *Spec Ops: Case Studies in Special Operations Warfare : Theory & Practice*. Novato, CA: Presidio, 1995.

Miller, Matthew, Jon Brickey, and Gregory Conti. "Why Your Intuition about Cyber Warfare is Probably Wrong." *Small Wars Journal* no. Nov 29 2012 (.

Mitchell, Paul. "Media and the Military: Operational Weapon Or Tactical Schtick?"CFC, Canada, (2012).

Morozov, Evegeny. "Machines of Laughter and Forgetting " *New York Times* (31 March 2013).

———. "Why Social Movements should Ignore Social Media." *New Republic* (5 Feb 2013).

NATO. *AJP 01(D) Allied Joint Doctrine* 1 December 2010.

NSI, Allison Astorino-Courtois, Hriar Cabayan OSD, Bill Casebeer, Ms Abigail Chapman, Christopher Rice, Janice Adelman NSI, Mr Azad Amir-ghessemi, Gregory Berns, Belinda Bragg NSI, and David Browne. "National Security Challenges: Insights from Social, Neurobiological, and Complexity Sciences.".

Nugent, Rachel and Seligman, Barbara. "Demographics and Development in the 21st Century InitiativeTechnical Background Paper:How Demographic Change Affects Development.".

O'Connor, T. J. "The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare." The SANS Institute, (2011).

O'Harrow, Robert. "Understanding Cyberspace is Key to Defending Against Digital Attacks - Washington Post " , accessed 4/8/2013, 2013, http://articles.washingtonpost.com/2012-06-02/news/35461761_1_software-flaw-hackers-iphone.

Panetta, Leon. *Defending the Nation from Cyber Attack* (2012).

Parrish, Karen. "Special Operators Depend on Good Partners, Commander Says. " , accessed 4/8/2013, 2013, http://www.defense.gov/News/NewsArticle.aspx?ID=119137.

Pigeau, Ross and Carol McCann. "Re-Conceptualizing Command and Control." *Canadian Military Journal* 3, no. 1 (2002): 53-63.

Porche III, Isaac R. and Jerry M. Sollinger. "An Enemy without Boundaries." *Proceedings Magazine, U.S. Naval Institute* Vol. 138/10/1,316, (October 2012).

Prensky, Marc. " Digital Natives, Digital Immigrants." *On the Horizon (MCB University Press)* no. Vol. 9 No. 5 (October 2001).

———. "Digital Natives, Digital Immigrants, *Part II:*
do they really *Think* Differently?" *On the Horizon(NCB University Press)* no. Vol. 9 No. 6, (December 2001).

———. "H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom. " *Innovate 5 (3)* (2009).

Ransdell, Sarah, Brianna Kent, Sandrine Gaillard-Kenney, and John Long. "Digital Immigrants Fare Better than Digital Natives due to Social Reliance." *British Journal of Educational Technology* 42, no. 6 (11, 2011): 931-938.

Rayment, Sean. "How the Special Forces Helped Bring Gaddafi to His Knees-." *The Telegraph,* (28 Aug 2011).

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

Rid, Thomas and Peter McBurney. "Cyber-Weapons." *The RUSI Journal* 157, no. 1 (2012): 6-13.

RSA.*RSA 2012 CYBERCRIME TRENDS REPORT the Current State of Cybercrime and what to Expect in 2012*, (2012).

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising use of American Power* Broadway, 2012.

Sanger, David E. "Obama Ordered Wave of Cyberattacks Against Iran." *New York Times,* Publication (June 1, 2012).

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare* Cambridge University Press, 2013.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare* - , edited by Academic and Professional Books -. New York, NY: Cambridge University Press, 2013.

Schreier, Fred. *On Cyberwarfare*: DCAF, 2012.

Sheldon, John B. "Lessons Learned: Stuxnet and Cyberpowe in War." *World Politics Review* (19 April 2011)1 - 4.

Sheth, Jagdish N., Rajendra S. Sisodia, and Arun Sharma. "The Impact of Demographic Shifts and Facilitating Technology Trends on Future Customer Behavior." *Journal of the Academy of Marketing Science* (1999).

Smith, E. "The Digital Native Debate in Higher Education: A Comparative Analysis of Recent Literature / Le Débat Sur Les Natifs Du Numérique Dans l'Enseignement Supérieur: Une Analyse Comparative De La Littérature Récente." *Canadian Journal of Learning and Technology / La Revue Canadienne De l'apprentissage Et De La Technologie* 38, no. 3 (2012).

Stanton, Neville A., Daniel P. Jenkins, Paul M. Salmon, Guy H. Walker, Kirsten M. A. Revell, and Laura A. Rafferty. *Digitising Command and Control A Human Factors and Ergonomics Analysis of Mission Planning and Battlespace Management*. Burlington, VT: Ashgate Publishing Company, (2009).

US Airforce. *Air Force Doctrine Document 3-12* (2010) .

VanSlyke, Timothy. "Digital Natives, Digital Immigrants: Some Thoughts from the Generation Gap." *The Technology Source* 7, no. 3 (2003).

Weiner, Sarah. "Searching for Cyber Deterrence." , accessed 3/31, 2013, csis.org/blog/searching-cyber-deterrence.

Williams, Thomas M. "Understanding Innovation." *Military Review* Vol. 89, no. No. 4 (July - August 2009, .

Wingfield, Thomas C. "When is a Cyber Attack an "Armed Attack?": Legal Thresholds for Distinguishing Military Activities in Cyberspace." *Potomac Institute for Policy Studies* (2006).

Xu, Zhengchuan, Qing Hu, and Chenghong Zhang. "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56, no. 4 (2013): 64-74.