CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 36 / PCEMI 36

MASTER OF DEFENCE STUDIES RESEARCH PAPER

THE IMPACT OF NEW MEDIA ON MILITARY OPERATIONS

By/par: Major S. Mark Parsons

TABLE OF CONTENTS

ABSTRACT

This dissertation examines the effects of new media in a military environment and argues that new media and informationalism have a profound impact on the practice of planning, preparing, conducting, and sustaining major Canadian Forces operations. In evaluating new media and the operational art, a comprehensive overview of the theory of informationalism is outlined, including the identification of the human element of new media and the new media characteristics that are expected within today's society. In assessing the pervasive, instantaneous, social, and interactive characteristics of new media, a practical perspective is given on how these characteristics shape the present network society. Identification is made of a digital divide between the leadership and the younger generation within the CF. New media is challenging the operational art of the commander and staff officer and impacting the political, informational, and military elements of conflict. While commanders have benefitted from the improved common operating picture and situational appreciation for the battlespace, military forces however, have to deal with the abundant volume of information available making the modern planner more reliant on technology to complete operational art. The commander has succinct challenges in the complete implementation of new media within a theatre of operations. Information Protection activities and Influence activities of Information Operations are challenged by the openness of new media, the ease of information to be promulgated through social networking means, and the ability of the adversary to threaten the confidentiality, integrity and accuracy of information. Organizational efforts within the CF will have to be implemented in earnest to develop a better understanding of the strategic context and real-world conditions influencing the employment of new media in order to positively affect the desired endstates of military operations.

CHAPTER 1
INTRODUCTION

Tucked in the valley of the Hindu Kush mountain range, the political center of the Islamic Republic of Afghanistan: the city of Kabul lies on the banks of the Kabul River. Thousands of soldiers, sailors, and air personnel from 45 nations reside in a small compound literally minutes from the Presidential Palace of Hamid Karzai. Officers and non-commissioned members arrive from all corners of the globe, tasked by their nations to contribute to the North Atlantic Treaty Organization (NATO) headquarters for the International Security Assistance Force – Afghanistan. At first glance, all are different – their distinctive arid camouflage set them apart from every other participating nation. With closer scrutiny however, there are commonalities. The majority of personnel arriving in theatre are armed with personal cellphones, others bring their own laptops, personal gaming devices, mp3 players, and ebooks. From every culture and from every country, the present-day warrior wades into battle armed with digital technology.

Social network connectivity in theatres of war such as Afghanistan and Iraq is an expectation. Morale and welfare networks consisting of high speed Internet and file servers for games, music, and movies were available in each soldier's barracks. The three European-style cafés on base had wireless Internet hotspots for staff and a multitude of transient visitors on theatre assistance visits. For those without personal computers, national support elements had Internet cafés and voice over Internet (VoIP) telephones to stay connected with families and friends back home. It was impressive to think that in the

middle of a war zone, 10,443 kms[1] from home that any soldier could sit in front of any personal computer and videoconference via webcam over Skype in real-time.

The expectation of connectivity for the social welfare network was a priority and a constant consternation amongst the users.[2] This attitude carried throughout the entire area of responsibility. Every Regional Command had an established commercial communications network for their personnel, most based on local new upstart Internet service providers (ISP). Soldiers purchased local pay as you go SIM[3] cards for local personal texting and voice calls within the bases and also carried them on missions in local patrols or visits to ensure redundant communications with their units. Waging war in the 21st century has brought connectivity challenges to the forefront that were not present ten years ago. A social communications evolution has occurred within today's definition of the modern soldier.

Simultaneously, the reliance on mobile communication technology by the population in the countries to which we deploy has witnessed exponential growth. Since the fall of the Taliban regime in 2001, the communication revolution in Afghanistan has gone viral. From unreliable land line telephones where a handful would serve an entire region, Afghanistan boasted over 1.4 million cellular customers by 2007 and a growth of 150,000

---

[1] The straight line distance between Ottawa, Ontario and Kabul, Afghanistan.

[2] As the custodian for the ISAF HQ Morale and Welfare network from September 2007 to April 2008, I became acutely aware of the importance of the network to individuals, and became quickly thick-skinned to the complaints on outages and lack of bandwidth.

[3] SIM: Subscriber Identity Module.

new customers per month.[4] Where land line costs for long distance in 2001 was approximately $19USD per minute, Afghans now pay 10 cents per minute on pre-paid voice services.[5] GSM cellular coverage is now in 133 major cities and villages in all 34 provinces, enabled through a 2,500 kilometre microwave network that links the entire country. The Afghan population is now interconnected in ways that were literally inconceivable a decade ago.

The communication infrastructure in Afghanistan has created a quagmire for the Taliban insurgents who remain in Afghanistan to oust the infidels from their country. In 2001, its use was contrary to the Taliban's strict interpretation of Sharia Law that electronic communication – be it telephone, television, or radio – should be banned.[6] The necessity to control the population by hindering communications is grounded far back into their reign after the Soviet invasion forces left in 1989.[7] However, the al-Qaeda backed Taliban have proficiently used cellular telephones and Internet connections to coordinate their counter-insurgency efforts against ISAF. They have equally realized that ISAF also use the new communications infrastructure to their advantage: either to coordinate amongst themselves, or to contact with human intelligence (HUMINT) spotters and key

---

4 "Cell-Phone use Booming in Afghanistan," *Wireless- msnbc.com,* http://www.msnbc.msn.com/id/20479899/; Internet;accessed 9 February, 2010.

5 The price of $19USD for land line long distance rates was related to the author in a conversation with the founder of AWCC, Ehsan Bayat in November 2007.

6 Amy Waldman, "A Nation Challenged: The Law; No TV, No Chess, No Kites: Taliban's Code from A to Z," *New York Times Online*, http://www.nytimes.com/2001/11/22/world/a-nation-challenged-the-law-no-tv-no-chess-no-kites-taliban-s-code-from-a-to-z.html; Internet; accessed 18 March 2010.

7 "Timeline: Soviet War in Afghanistan," *BBC News – South Asia*, http://news.bbc.co.uk/2/hi/south_asia/7883532.stm; Internet; accessed 18 March 2010.

leaders inside of villages identifying Taliban locations. Faced with this critical problem, the Taliban demanded the Afghan Wireless Communication Company (AWCC), Roshan, Areeba, and Etisalat - the four leading cellular providers in Afghanistan - to turn off their services between 5 p.m. and 7 a.m. on the belief that ISAF was using the civilian carriers to track down insurgents using cell phone technology.[8] They made good on their threats and in the first five months of 2008, the Taliban successfully attacked the country's cellular communication infrastructure at 50 cellular towers in the southern and eastern regions of Afghanistan.[9] The Taliban was willing to forego their ability to communicate at night in order to regain tactical advantage over NATO forces when engaged in operations.

What they didn't expect was the pushback from local population. Residents of villages, towns, and communities threatened by the Taliban's promise to destroy cellular towers countered the insurgents by assisting ISAF in locating the Taliban threat, contacting the cellular companies to give them warning about impending attacks, and even forming vigilante security forces to protect their local community tower from attack. The local's reliance on cellular technology was now such an integral component of their society that they were determined to remain a part of the "network." The cellular companies and the locals were willing to stand up to the Taliban's threats in order to maintain connectivity.[10]

---

8 "T aliban: Nix Nighttime Cell Phone Service," *Military Tech - CNET News*, http://news.cnet.com/8301-13639_3-9881951-42.html; Internet; accessed 9 February 2010.

9 "Afghanistan Update: May 2008, " *Centre for Defense Information*, http://www.cdi.org/friendlyversion/-printversion.cfm?documentID=4320; Internet; accessed 9 February 2010.

10 One theory however, was that the cellular companies paid off the Taliban to cease their aggression. Both Roshan and AWCC were adamant throughout early 2008 that they did not negotiate with the Taliban to end the attacks.

These examples from Afghanistan demonstrate the considerable weight that new media have on societies – both developing and stable. On one hand, it shows the reliance of a war torn nation on a new communications infrastructure and on the other hand, an expectation of social network connectivity on the part of ISAF's soldiers. It demonstrates that the Taliban insurgents, even though vehemently against technology during their governance, appreciate the power of the new media in order to further their resistance against ISAF. This brings to the surface the complicated elements of new media and its effects on the battlespace. It begs to ask the questions: what significant role is new media playing in operations? How should forces react to the enemy's use of the same technologies? How will new media affect the operational art and decision making? field?

There are important questions on the employment and effects of new media in operations that are now coming to the forefront. However, our present reality is that with the dual pressures of a lack of up-to-date doctrine on employing new media on operations and in garrison and an exponential growth of both the capabilities and the frequency of personal communication devices in theatre, it behoves us to explore this aspect of communications in the battlespace and the affects it will have on operational art.

This paper argues that new media and informationalism have a profound impact on CF operations and that the effects of new media on the battlespace must be considered within operational planning in order to ensure strategic success. The focus in this research paper is on non-secure, unclassified communications within the Department of National Defence (DND) and the Canadian Forces (CF) and will concentrate on the passage of

open-source information. I anticipate that new media will directly impact CF operations. As the use of new media technology by soldiers, sailors, and air personnel during operations increases and the expectation of real-time ubiquitous connectivity becomes the norm, a younger, more "tied-in" generation will continue to challenge the older, more risk-adverse generation when applying change to the use and application of networking technologies. I also anticipate that the challenges of operational and information security will be the main obstacles to adopting new media technologies within the battlespace. Security concerns will also be paralleled with the unbridled proliferation of new media technologies by insurgents, non-state actors, and radicals.

Chapter 2 will start our discussion by investigating the technological paradigm of the information society and considering the technological determinist theory of Bell and the theory of informationalism of Castells. The value and importance of information and knowledge will be discussed as we look into the economics of information and its value within the new social structure of the network society. I will discuss the focus of connectivity, information, and the will of the network society. I will show that informationalism and the network society instil a requirement for organizations to understand the value within the characteristics of new media and the people that will be affected by their employ.

Chapter 3 will explore the characteristics of new media and provide an appreciation of how these characteristics will affect the CF. I will start with a formal definition of new media and will identify the main characteristics of new media: pervasiveness, instantaneity, social, and interactive and how they shape the present network society. I

will also define the characters at play within the network society: the digital natives and digital immigrants. I will establish in this chapter that there is a digital divide between the leadership and the younger generation within the CF.

My objective in Chapter 4 is to underscore the fact that innovations in global media technologies are challenging the operational art of the staff officer and impacting the political, military, and societal elements of conflict. I will discuss the impact that new media has on the diplomatic, informational, and military lines of operation. Chapter 4 will also investigate the proficiency that the enemy uses new media in their quest for information engagement and identify how their actions directly affect the operational art of military forces, the government, and members of society within nations who support the global war on terrorism.

To conclude this research paper, Chapter 5 will identify the challenges that new media places within the Information Operation (IO) campaigns of war. I will look at the Information Protection activities and Influence activities of IO and the challenges that new media pose on Operational Security and Information Security. I will also focus on the social element and explore the best way to achieve the attention of the target audience through the use of new media. By the end of the chapter, I will have identified the challenges that new media plays within the CF, and identify the areas of concern for the organization in order to integrate new media into the organization.

CHAPTER 2

NEW MEDIA AND SOCIETY – EXPLORING THE FOUNDATIONS OF SOCIAL CHANGE

New media and the Information Age has given spark to an inferno of new and revised social studies and theories on what influences society and how these influences change the political, economic, and social landscape. In order to comprehensively examine the effects of new media as it relates to CF operations, it is necessary to first have an understanding of the theories of information technology and its influence on society and institutions. To this end, informationalism, the economics of information, and the network society will be considered in this chapter before examining the military operational influences of new media.

I will start by discussing the technological paradigm of the information society and investigate the technological determinist theory of Bell and the theory of informationalism of Castells. I will also demonstrate the importance of information and knowledge; how it is of considerable value within the new social structure of the network society. By the end of the chapter, I will have established that the acceptance of new media is not being driven by pure technological advances, but by a societal desire to be ubiquitously connected within their organizations with a view to accessing and processing valuable information. A better understanding of the human factors of information and connectivity will give us better insight on how new media will affect CF operations.

INFORMATIONALISM – THE TECHNOLOGICAL PARADIGM

Technology is a fundamental dimension of social structure and social change.[11] It is usually defined as the use of scientific knowledge to set procedures for performance in a reproducible manner. It evolves in interaction with the other dimensions of society, but it has its own dynamics, linked to the conditions of scientific discovery, technological innovation, and application and diffusion in society at large.[12] This research pertains to information technology (IT) and information communications technology (ICT), and therefore, clarity on their definition is warranted.[13] The Information Technology Association of America (ITAA) defines IT as:

> …the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware. … [I]nformation technology is the capability to electronically input, process, store, output, transmit, and receive data and information, including text, graphics, sound, and video, as well as the ability to control machines of all kinds electronically.[14]

There are several schools of thought on Informationalism. In his 2001 work *Investigating*

---

11 Claude Fischer, "America calling: a social history of the telephone to 1940", (Berkeley: University of California Press) in Manuel Castells, *Informationalism, Networks, and the Network Society: A Theoretical Blueprint* (Northampton, MA: Edward Elgar, 2004), 9.

12 *Ibid*., 9-10.

13 The acronyms IT and ICT are interchangeable. In the CF, the abbreviation "ICT" is becoming the dominant term referring to technology as the CF community accepts the approved abbreviation "IT" to represent "individual training."

14 "Information Technology," http://en.wikipedia.org/wiki/Information_technology#cite_note-0; Internet; accessed 13 January 2010.

the Information Society, Hugh Mackay outlines the subject of the information society.[15] The dominant aspect that he posits is the consideration of the information society as the root of societal change.[16]

The differentiating positions on information as the source of change in society are twofold: (1) the idea of technological development – or technological determination - as the catalyst for social change versus (2) the focus of information social change driven by political, economic, social or cultural factors to which many refer not to the information society, "but to late modernity, post-industrialism, postmodernism or globalization to characterize the transformation of contemporary society."[17]

While the aforementioned distinctions of the information society are painted as a contrast of views amongst authoritative voices, the two best-known advocates are the American sociologist Daniel Bell and the urban theorist Manuel Castells.[18] Through their combined works, we see over a span of 35 years the evolution of the theories of the development of postmodern society from early "post-industrial" technological determinism of Bell to the network society of Castells' informationalism.

TECHNOLOGICAL DETERMINISM

Bell's hallmark writings in 1973 on a "post-industrial" society identified a coming

---

15 Hugh Mackay, *Investigating the Information Society* (New York: Routledge, 2001), 21.

16 *Ibid*.

17 *Ibid*.

18 *Ibid*.

revolution in which the computer played a central role in society.[19] Bell refers to pre-industrial society as raw muscle power against nature; the industrial age as characterized by machinery and post-industrial society based on services, when "what counts is not raw muscle power, or energy, but information."[20] For Bell, the post-industrial society is viewed by the centrality of scientific knowledge, and by scientific knowledge directing social change.[21] He saw technology as the basis of enhanced productivity, resulting in a transformed economy.[22] Bell's prediction on technology is the basis for the theory of technological determinism.

Various theorists,[23] including Bell, have adopted the stance of technological determinism. Technological determinism espouses the belief that technology shapes society and that technology, as an independent factor, is seen as the fundamental condition underlying the pattern of social organization.[24] As with Bell's post-industrial society in which the evolution of technology was responsible for the transformation of the economy, technological determinism asserts that technology is the main determinant of social

---

19 *Ibid*.

20 Dani el Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, London, Heinemann, 1973 in *Ibid*., 22

21 *Ibid*., 24.

22 *Ibid*., 29.

23 Daniel Chandler, "Technological Determinism: Technology-Led Theories," http://www.aber.ac.uk/media/Documents/tecdet/tdet02.html; Internet; accessed 26 February 2010. Chandler cites Sigfried Giedion, Leslie White, Lynn White Jr, Harold Innis and Marshall McLuhan as adopters of technical determinism.

24 *Ibid*.

change and the prime mover of history.[25]

This position argues that knowledge and information are the key factors in economic and social development. The central argument here is that productive and distributive processes within the economy are increasingly driven by knowledge-based inputs. In this way, the development of new media technology needs to be linked into the transformation of the economy and related changes within political and culture.[26]

Technological determinists see technology, in general, and ICTs, in particular, as the basis of society in the past, present and even the future. They say that technologies such as print, television, or the computer "changed society."[27] In its extreme, the entire form of society is seen as being determined by technology: new technologies transform society at every level, including institutions, social interaction and individuals. At the least a wide range of social and cultural phenomena are seen as shaped by technology. 'Human factors' and social arrangements are seen as secondary.[28] The direct contrast to technological determinism is Castells' theory of Informationalism.

DEFINING INFORMATIONALISM

The information revolution that has occurred over the past two decades concerns connectivity: the amount of information reach and the quality of interactions between

---

25 Mackay, *Investigating the Information Society*, 29.

26 Nick Stevenson, *Understanding Media Cultures*, 2nd ed. (London: Sage Publications, 2002), 184.

27 Chandler, *Technological Determinism: Technology-Led Theories*

28 Mackay, *Investigating the Information Society*, 30.

users resulting from advances in technology.[29]

Informationalism is a technological paradigm.[30] It refers to technology, not to social organization and not to institutions. Informationalism provides the basis for a certain type of social structure that Castells terms the "network society."[31] Informationalism is a catalyst for social evolution – a means to which a new social structure is formed. It does not however, directly produce social evolution. Informationalism has allowed organizations to achieve increased flexibility through more knowledge-dependent and less hierarchical structures. New technology has enabled large structures to co-ordinate their activities world wide, while building in reflexive inputs to both quickly respond to the current state of the market and benefit from economics of scale.[32] In order to appreciate how communications technology has been a catalyst, it is necessary to first look at the technological paradigms of the past seventy years and see how informationalism has aided society to evolve to our present state of network dependency.

A paradigm is defined as a conceptual pattern or example that formulates a framework, either theoretical or philosophical.[33] A technological paradigm is therefore the pattern of technological discoveries that can be grouped around a common occurrence or period of

---

29 David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, D.C.: CCRP Publications, 2003), 74.

30 Manuel Castells, "Epilogue: Informationalism and the Network Society," in *The Hacker Ethic and the Spirit of the Information Age*, ed. Pekka Himanen (New York: Random House, 2001), 158.

31 *Ibid*., 158

32 Stevenson, *Understanding Media Cultures*, 192.

33 "Paradigm," http://www.merriam-webster.com/dictionary/paradigm; Internet; accessed 11 March 2010.

time, and forms a system of relationships that enhance the performance of each specific technology.[34] By this definition, the transformation of ICT is characterized as a technological paradigm and arguably the root of the Industrial Age.

Informationalism is manifest through the pattern of change in ICT hardware. The revolution in computing technology began in the 1940s as computer hardware pioneers such as Atanasoff and Berry, (ABC Computer) Aitken and Hopper, (Harvard Mark I) and Eckert and Mauchly (ENIAC 1) invented the first models of freely programmable computers.[35] As demand for computing power grew, the invention of the integrated circuit by Kilby and Noyce in 1958 evolved to the Intel products of the first RAM computer memory and first microprocessor in 1970 and 1971 respectively.[36]

From this evolution of computer hardware developed the need for interconnectivity. In 1969, the technological paradigm branched to the network paradigm with the development of ARPAnet. The Defense Advanced Research Projects Agency[37] (DARPA) is a branch of the U.S. military that conducts advanced research and development on weapon systems and associated operational concepts.[38] While ARPAnet was designed to

---

34 Castells, *Informationalism, Networks, and the Network Society: A Theoretical Blueprint*, 10.

35 "The History of Computers - Computer History Timeline," http://inventors.about.com/library/blcoindex.htm; Internet; accessed 12 March 2010.

36 *Ibid*.

37 The organization DARPA was originally known as ARPA: Advanced Research Projects Agency and has interchanged between these two titles in 1972, 1993, and 1996. This document refers to it as DARPA as it is its present name. ARPAnet was the original name for the network and is similarly referred to as DARPAnet.

38 "ARPAnet - the First Internet," http://inventors.about.com/library/weekly/aa091598.htm; Internet; accessed 15 March 2010.

protect the flow of information between military installations by creating a network of geographically separated computers that could exchange information via a newly developed Network Control Protocol (NCP), DARPA's former director, Charles M. Herzfeld, claimed that ARPAnet was created, "out of our frustration that there were only a limited number of large powerful research computers in the country and that many research investigators who should have had access were geographically separated from them."[39] The connectivity of ARPAnet invigorated innovation in hardware and software to achieve the standards of connectivity in the present Internet.

To our modern era, advances in technology, be it hardware, software applications, or connectivity have converged to the development of the network and the network society. The transformation of ICT is proof of the power of this convergence. Land line telephones ceded to cellular phones whose primary use was for voice communications. Cell phones have given way to multi-functional communications devices. The 3G "smart phone" as they are coined, handles voice, text messaging, email, and web 2.0 supported Internet.[40] Certain models like Apple's iPhone or Google's Nexus One enable thousands of applications from GPS support, Friend Finder apps, RSS feeds, and many more. This does not take away from the device's ability to store and play audio and video files, capture photos like a camera and shoot home movies like a camcorder. From one device, users can be completely connected into their personal network of friends and interests.

---

39 *Ibid*.

[40] 3G technology is the common name commonly referring to the International Mobile Telecommunications – 2000 (IMT-2000) standards established by the International Telecommunications Union (ITU). 3G networks allow for simultaneous use of voice and data services at minimum established data transfer rates. See the link http://www.itu.int/osg/spu/ni/3G/technology/index.html#Cellular Standards for the Third Generation for more information.

Their ability to access, collect, and manipulate information assists them in their personal quest to achieve information dominance over their sphere of influence. The technological paradigm of informationalism has converged ICT based on the needs and demands of the user community. The human factors are the drivers of the technological change and through those influences, the technology has been readily adapted by society.

We have discussed the theories of technological determinism and informationalism. One constant throughout the discussion of both theories has been social change. While the argument for determinism puts its primary focus on the technology itself as the catalyst for change, its consideration that human factors and cultural arrangements have secondary influences on social change is a substantial flaw. The theory of informationalism gives focus to the human influences on the use of new media and how the societal value of information reach and the quality of interactions between users affect our use of converging ICT technology. Informationalism establishes that organizations such as the CF need to understand and appreciate the human factors – the value and economics of information and the need for social network connectivity – that will influence the need and methods of using new media within operations.

THE ECONOMICS OF INFORMATION

Throughout time, economics and power have been acutely connected. The Information Age is distinguishable from previous Ages twofold: (1) by the economics of information and (2) the nature of the power of information. What is new in our historical period is the technology of information processing and the impact it has had on the application of

knowledge.[41] A society's increased access to information provides an opportunity for its collective to rethink the ways that it organizes, manages, and controls.[42]

Sir Francis Bacon (1561-1626) emphasized the age old precept; *knowledge is power,*[43] conveying the notion that an individual's worth was related to their possession of information. The more exclusive the possession of knowledge, the more valuable the information. Hence, information is a commodity like any other commodity, whose value is related to scarcity.[44] Throughout history, knowledge and information, and their technological enablers, have been adroitly akin to political/military domination, economic prosperity, and cultural exclusiveness. So, in a sense, all economies are knowledge-based economies and all societies are, at their core, information societies.[45] In previous Ages, the commodity of knowledge was easily attained by royalty, governments, and corporations to leverage their rule on the masses due to their predisposed wealth, higher position in society, and higher levels of education. This advantage has diminished as the economics of information have changed. With the cost of information and its dissemination dropping dramatically, information has become a dominant factor in the value chain for almost every product of service[46] and within our individual social circles to attain personal authority, value, and a sense of belonging.

---

41 Castells, *Epilogue: Informationalism and the Network Society*, 159.

42 Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 71.

43 Francis Bacon. *Meditationes Sacrae. De Haeresibus.* "Famous Quotes of Sir Francis Bacon,." http://www.luminarium.org/sevenlit/bacon/quotes.php#txt12; Inernet; accessed 16 Mar 10.

44 *Ibid*., 72.

45 Castells, *Epilogue: Informationalism and the Network Society*, 159.

46 Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 73.

Informationalism enabled the widespread adoption of IP (Internet Protocols), browser technology, and the creation of Web pages and portals. Alberts and Hayes in *Power to the Edge* recognizes that such technological advances provide an increase in the economic value of information in richness, reach, and the quality of virtual interactions.[47]

Informationalism has narrowed the concept of space and time between users due to continual connectivity. It has created a real-time environment where delays between communications are no longer tolerated and the ability to coordinate and collectively submit ideas and inputs over once divisive organizational, cultural, or political boundaries. Informationalism unlocks the monopoly from the few to attain and retain exclusive knowledge. The ability of individuals to be collectively connected to leverage knowledge changes the economics of information and redefines the concept of information power.[48]

The economic theory of the Information Age identifies that, as society increases its access to information, all levels of society become more empowered. The once divisive organizational, cultural, and political boundaries of society have become porous as the ability to collaborate amongst peers and broadcast group interest to the world is currency in the new globalized civilization. As Castells submits, "the theoretical understanding of this culture and of its role as the source of innovation and creativity in informationalism is

47 *Ibid*., 73

48 *Ibid*., 72

the cornerstone in our understanding of the genesis of the network society."[49]

THE NETWORK SOCIETY – A NEW SOCIAL STRUCTURE

Castells identifies that information and knowledge are essential for the economy and in society at large. However, on the basis of informationalism, a new social structure has emerged - a structure, made of electronic communication technologies, powered by social networks.[50] The network society has surfaced as the dominant form of social organization in our time. It is a social structure made of information networks powered by information technologies characteristic of the informationalist paradigm.[51] The idea of a network society offers a different model of the capitalist economy, a rethinking of the link between communications and politics, and consideration of the changes taking place within our cultural life. The network society then is the attempt to provide a social theory of mass communication that takes both the rise of the new media and the shift to knowledge-based societies seriously. New information and communication technologies do not bring about a new society, but they provide the means that make it possible.[52]

There are three dimensions to informationalism as it pertains to the network society. The first essential dimension is connectivity and access to networks. These two traits are achieved through the continued evolution of information communications technologies. The second dimension is the information that resides on the networks. Easily accessible,

---

49 Castells, *Epilogue: Informationalism and the Network Society*, 177.

50 Castells, *Informationalism, Networks, and the Network Society: A Theoretical Blueprint*, 64.

51 Castells, *Epilogue: Informationalism and the Network Society*, 166.

52 Stevenson, *Understanding Media Cultures*, 184-185.

the information must also be of significant value to the user in order to provoke them to share it with other users. This information may either be already resident on the network (i.e. data, files, etc.) or generated by the user (i.e. user-to-user or user-to-network communications). The third dimension is the human capacity to utilize ICTs. There must be an intellectual capability to manipulate the technology, process the information it provides, and a will of the individuals within the society to communicate and socialize via this medium. There is also the barrier of cost. In a developing nation such as Afghanistan where the Gross Domestic Product per capita (PPP) is a mere $800,[53] the cost of living and annual wages do not support or justify the cost of owning ICT. Yet, over 8.5 million Afghans own a cell phone. The consumer must possess the will to own and have a belief in the importance of such technology. The proper combination of connectivity, information, and will of society becomes the key to ensure productivity, competitiveness, innovation, creativity, and, ultimately, power and power sharing.[54]

In his work, *Informationalism, Networks, and the Network Society*, Castells defines the importance of the network society to the present Information Age:

> The notion of the information or knowledge society is simply a technological extrapolation of the industrial society, usually assimilated, to the Western culture of modernization. The concept of the network society shifts the emphasis to *organizational transformation,* and to the emergence of a globally interdependent *social structure,* with its processes of domination and counter-domination. It also helps to define the terms of the fundamental dilemma of our world: the dominance of the programs of a global network of power without social control or, instead, the emergence of a *network of interacting cultures,* unified by

53 "CIA - the World Factbook – Afghanistan," https://www.cia.gov/library/publications/the-world-factbook/geos/af.html; Internet; accessed 2 February 2010. Afghanistan is 219th out of 227 nations for GDP per capita. It is 221st for the rate of inflation (30.5% in 2009).

54 Castells, *Informationalism, Networks, and the Network Society: A Theoretical Blueprint*, 65.

the common belief in the use value of sharing.[55] (*emphasis* added)

The three concepts that are of primary significance in Castells' previous passage to our study of new media and the CF are: the shift of the network society to emphasize the requirement for organizational change; the emergence of an interdependent social structure; and the emergence of a network of interacting cultures. These three concepts, when applied in the military environment, instil a requirement to focus on the network society if the organization wishes to adapt to its present – and future – demographic. The development of the network society has caused a cultural change within the CF to which we are slow to react.

CHAPTER SUMMARY

I believe that Castells' theory on informationalism as a catalyst for social evolution is the correct interpretation of what we as a society are witnessing today in the global adoption of new media. Informationalism has decisively shaped a new culture focused on information and knowledge. Informationalism has disposed the economic theory of the Information Age, empowering all levels of society through the increased access to information and providing a global voice to be heard. The currency of real-time collaboration and projection has assisted in the development of the network society.

The network society focuses on connectivity that virtually eliminates the barriers of time and space communications. The currency of information is predominant in the network society. The value of information is dictated by the society's inputs to ensure accuracy of

55 *Ibid*., 66.

the information, and the access that they have. The third aspect of the network society is the capacity and the will to use information and communications technologies. Technology has given even the poorest nations the opportunity to become a part of the network society, and new media is filling an enormous gap in the daily structure of their lives. It has led to organizational and social structure transformations, and enabled differing cultures to interact and network

Understanding informationalism and the network society has established the importance of our focus on the human factors on the use of new media. Without such an appreciation, the CF will not understand the importance that information and connectivity play within the present digital culture of younger CF members. The study of informationalism has established that we cannot ignore the human element of new media and the new media characteristics that are expected within today's society. Chapter 3 will consider these characters and characteristics of the new media paradigm.

CHAPTER 3
THE NEW MEDIA PARADIGM

"When a thing is current, it creates currency" H.M. McLuhan

INTRODUCTION

Organizations like the Canadian Forces are experiencing an evolution towards increasing connectivity both from the adoption of new information and communications technologies and from the recruitment of young personnel who are completely submerged in the digital world. This "culture of connectivity" that the network society inculcates into the workplace brings to light many challenges that senior managers must consider. But before we address the challenges that senior managers of the CF must consider as a result of informationalism, we have to get a full appreciation of what new media brings to the environment and how it directly affects the connectivity, information, and societal will of the network society.

Chapter 2 established that the CF needs to fully understand the present day network society in order realize the influences new media will have on the operational environment. The methodology to both of these challenges is to understand the new media sources and how they are used by today's network society. It is also imperative that we examine the main characters within the network society who are both influencing and influenced by new media.

The goal of this Chapter is to outline the characteristics of new media and to provide an appreciation of how these characteristics will affect the CF. I will start by formally

defining new media. From there, I will identify the main characteristics of new media: pervasiveness, instantaneity, social, and interactive and how they shape the present network society. I will also define the characters at play within the network society: the digital natives and digital immigrants.

By the conclusion of this chapter, I will have established that there is a digital divide between the leadership of the CF and the younger generation of soldiers, sailors, and air personnel that presently reside within the ranks. Without fully understanding the characteristics of new media by senior leadership, integration of new media into the CF society will continue to be a challenge. Attrition of the older generation is not a viable option. It bodes well for the CF to be more immediately engaged in the impact that new media will have on the organization and on the operational art.

DEFINING NEW MEDIA

First, what do we define as new media? New media is a generic term for the many different forms of electronic communication that are made possible through the use of computer technology. The term is in relation to "old" media forms, such as print newspapers and magazines that are static representations of text and graphics. In the work *The New Media Reader*,[56] Lev Manovich describes new media as, "a computer technology used as a distribution platform." The definition of new media is deduced from how the term is used in popular press:

> [N]ew media are the cultural objects which use digital computer technology for

56 Noah Wardrip-Furin and Nick Montfort, *The New Media Reader* (Cambridge, M.A.: The MIT Press, 2003).

> distribution and exhibition.[57] Thus, Internet, Web sites, computer multimedia, computer games, CD-ROMs and DVD, Virtual Reality, and computer-generated special effects all fall under new media. Other cultural objects which use computing for production and storage but not for final distribution -- television programs, feature films, magazines, books and other paper-based publications, etc. – are not new media.[58]

This definition is implicit that new media is categorized by the use of digital technology to distribute the message that is created within the digital environment.

The new media technological hardware of today is the result of convergence between computing properties of computers and convenience of consumer electronics. Computers and the Internet are becoming the music source to stereo systems as well as an alternate video source to TVs. The digital home experience now consists of medium to high-end TV sets, A/V receivers, home theatre gear, and gaming consoles that include Ethernet or Wi-Fi capability. Business and entertainment are also converging with the "smartphone," which wraps Internet access, music, video, camera, voice recorder, game machine and mini versions of nearly every software application imaginable into a do-it-all cellphone. The smartphone is the personal computer of the 21st century, because the cellphone is the single most "personal" machine people keep with them all the time.[59]

---

57 Lev Manovich, *The Language of New Media* (Cambridge, Mass.: The MIT Press, 2001) quoted in Noah Wardrip-Furin and Nick Montfort, *The New Media Reader* (Cambridge, M.A.: The MIT Press, 2003).

58 Lev Manovich, "Introduction: New Media from Borges to HTML," in *The New Media Reader*, eds. Noah Wardrip-Fruin and Nick Monfort (Cambridge, MA: MIT Press, 2003), http://www.manovich.net/DOCS/manovich_new_media.doc.

59 PC Magazine, "Definition of: Digital Convergence," http://www.pcmag.com/encyclopedia_term/0,2542,t=digital+convergence&i=41316,00.asp; Internet; accessed 31 Mach 2010.

New media goes beyond just the hardware. It also includes the concept that new methods of communicating in the digital world allow smaller groups of people to congregate online and share, sell and swap goods and information. It also allows more people to have a voice in their community and in the world in general.[60] This ability is afforded through the characteristics of new media: pervasiveness, instantaneous, social connectivity, and the ability to be interactive.

NEW MEDIA CHARACTERISTICS

The pervasiveness and ubiquity of New Media

Technology is so woven in to the fabric of modern life that it has become all but invisible.[61] It is hard to conceive modern society without technology. Our health, welfare, transport, communications, and social life are all inundated with technology to a point that it would be difficult to exhaustively describe all that influences our lives each day.

New media is certainly both pervasive and ubiquitous in our society. The two descriptors are very similar in their meaning and use when describing ICT. By definition, pervasive technology is one that has become diffused throughout every part of our environment.[62]

---

60 PC Magazine, "Definition of: New Media," http://www.pcmag.com/encyclopedia_term/0,2542,t=new+media&i=47936,00.asp; Internet; accessed 31 March 2010.

61 "Per vasiveness of Technology," http://www.nae.edu/nae/techlithome.nsf/weblinks/KGRG-55SPVK?OpenDocument; Internet; accessed 16 March 2010.

62 "Pervade - Definition and More from the Free Merriam-Webster Dictionary," http://www.merriam-webster.com/dictionary/pervade; Internet; accessed 16 March 2010.

A ubiquitous technology is one that exists or is everywhere at the same time.[63] The Internet is an excellent example of pervasive new media. The use of the Internet is in virtually every aspect of our society to communicate, research, download, and advertise. Institutions, businesses, and individuals all have websites and continually bombard us with their web addresses in print media, television, and online advertising. The Internet helps cities administer systems and sub-systems, run their transit systems, manage their hospitals, and control infrastructure. It is an enabler that is everywhere running in the background of society. Similarly, cellular networks are pervasive: we take it for granted that it is there, and have naïve expectations as to where connecting coverage should be. We expect connectivity in public places like cafés, airports, and libraries. Our reaction to the technology is when there is no coverage or there is an interruption to the services. The saturation of cellular phones, smartphones, laptop computers, and other new media devices into society demonstrate how ubiquitous technology is in today's world.

The ubiquity of ICT is not just a product of Western modernization. As of 30 September 2009, there were over 1.7 billion Internet users worldwide of which, North America, Europe, and Australia made up only 40 percent of global users. Asia alone accounted for 43 percent of Internet users with only 19.4 percent of total population penetration.[64] The International Telecommunication Union (ITU) reported that by the end of 2009, there were an estimated 4.6 billion mobile cellular subscription, corresponding to 67 percent of

63 "Ubiquitous - Definition and More from the Free Merriam-Webster Dictionary," http://www.merriam-webster.com/dictionary/ubiquitous; Internet; accessed 16 March 2010.

64 "World Internet Usage Statistics News and World Population Stats," http://www.internetworldstats.com/stats.htm; Internet; accessed 19 March 2010.

global inhabitants.[65] In today's network society, there is an inherent expectation of connectivity and reachability. ICT's pervasiveness permits this expectation in all facets our modern landscape.

Joseph Weizenbaum[66] refers to the pervasiveness of ICT as a 'condition'. He states:

> [N]o one planned it, and no one can say, "We're getting rid of it." The condition has grown, just like the use of automobiles today as a matter of course. But even with this example, you can ask yourself if it makes sense, given the traffic jams, exhaust, and the use of oil resources. Today, many people use a huge number of computers – many of them networked – with exactly the same lack of reflection. The condition has consequences: many of them a blessing, others the opposite.[67]

Dr. Weizenbaum's observations on the pervasiveness of communication technology bear to consider that the expectations of society to react very quickly in an environment where everyone can be reached at any time, has permeated continual evolution of technology to attain instantaneous connectivity.

The pervasiveness of new media has had a direct impact on the citizens within the network society. As I will discuss later, it has established the environment of the digital native.

Immediate Digital Awareness: Instantaneous Access to Information

New media has promoted individual's ability to connect with others to sublime

---

65 "Measuring the Information Society," http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_Summary_E.pdf; Internet; accessed 19 March 2010

66 Professor emeritus of the Department of Computer Science, Michigan Institute of Technology (MIT).

67 "The Pervasiveness of Technology Degrades Personal Responsibility," http://en.sap.info/the-pervasiveness-of-technology-degrades-personal-responsibility"/3525; Internet; accessed 17 March 2010.

proportions. Paired with connectivity is the expectation of real-time, instantaneous answers. For those who have owned a BlackBerry,® iPhone, or any other 3G smartphone device, difficulty to resist the ringtones of an incoming call, email, or SMS text is proof of the new habits as a result of instantaneous communications in the network society.

New media is also outpacing old media. With application add-ons such as Really Simple Syndication (RSS) feeds, users can now subscribe to interest feeds that allow them to monitor changes to web sites without the time consuming chore of monitoring manually personal favourite websites. Once the RSS feed is subscribed, it "pokes" the user to alert them of any changes that they themselves have deemed important. Users now have instant updates to the subjects to which they are interested, and the user is only one click away from accessing the information.[68] This RSS approach directly supports Alberts and Hayes' view of the characteristics of a networked environment. RSS allows users to act upon an automated *smart pull* of information rather than relying on the media networks or marketer's *push* of blanket coverage for information. Moving from a *push* to a *post and smart pull* approach shifts the problem from the owner of information having to identify a large number of interested parties of having the individual who needs information identifying potential sources of that information. The instantaneous access to *post and smart pull* applications makes it simpler for the user who has a requirement for information to determine its utility than for the producer to make this judgment.[69]

---

68 "What is RSS?" *PRESSfeed Co*., http://www.press-feed.com/howitworks/what-is-RSS.php; Internet; accessed 19 March 2010.

69 Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 82.

The phenomenon of mobile Internet is also fuelling the expectations of instantaneous access to information. The combination of the portability of small handheld devices and the mobility enabled by the coverage of the cellular networks is facilitating the phenomenon of "immediate digital awareness." Mobile Internet is just one of the many enablers of this real-time reality that the present generation is akin to.

Social and Interactive Connectivity

New media has leveraged social connections between people based on language, shared interests, family, and past shared social experiences.[70] The global media forecasting company Bloggerwave Inc. reports that people spend the most time overall on social networks and blogs. For the juggernaut Facebook, the statistics on the impact it has on daily social communications is staggering. This social networking site alone has over 400 million active users in 2010 of which half log in to the application each day. There are 5 billion pieces of content (web links, news stories, blog spots, notes, photo albums, etc.) shared each week. One quarter of all current active users access their accounts through a mobile device. Facebook reports that mobile users are twice more active on Facebook than non-mobile users.[71] As Internet usage worldwide increases, so too will the social functionality of application.

---

70 Deirdre Collings and Rafal Rohozinski, *Bullets and Blogs: New Media and the Warfighter* (Carlisle Barracks, Pennsylvania: Center for Strategic Leadership, US Army War College, 2008), http://www.carlisle.army.mil/dime/documents/Bullets_&_Blogs_new_Media_&_warfighter-Web(20%20Oct%2009%20w-%20link%20).pdf.

71 "Statistics," *Facebook.com*, http://www.facebook.com/press/info.php?statistics; Internet; accessed 19 March 2010.

The social characteristics of new media are one of the primary concerns of the present network society. Users are heavily reliant on the technological means to "stay in touch" in real-time and have invested heavily onto mobile media to achieve this connectivity. Organizations fear that social networking within the workplace will compromise operational security and negatively impact productivity.

The value of new media spans beyond the immediacy of access; it also allows for interactive communication on an unparalleled magnitude. It expands past the peer-to-peer communications of SMS,[72] email, and basic cellular calls. The functionality of applications that allow users to put content online so that it is accessible to all parties who have interest in reading it, and the functional flexibility of responding, commenting, or correcting the information that the initial user provided. While social networks like Facebook provide that instant gratification of comments of friends and associates, other applications like web log (blog) sites and micro-blogs like Twitter provide the peer-to-peer public interactive environment. The interactive nature of the Internet now allows any user in relative anonymity to comment on any entry. News outlets like the Canadian Broadcasting Corporation (CBC.ca) allow reader to comment on all posted articles and also support web application programming interfaces (API) that allow interaction or direct comments to threads on other predominant social networking sites. For example, when Prime Minister Stephen Harper's Conservative government sparked controversy in their Speech from the Throne on 3 March 2010 on the idea to change the words of the

72 SMS: Short Message Service

Canadian national anthem, bloggers, Twitterers,[73] and casual surfers flooded forums and on-line news outlets their outrage at the idea.[74] Within two days, the Prime Minister's Office, gauging the negative public outcry, quickly dropped the proposal.[75]

Interactive new media gives a voice to the public. As discussed in Chapter 2, the depreciating cost of accessing information has enabled virtually any member of society and not just the social elite, the ease of mass interaction. This allows anyone – including the fringe radicals – to get their message out in an inexpensive, instantaneous, and anonymous means.

New Media Characteristics: Summary

The characteristics of new media correspond to the expectations of the network society. Today's digital users demand extensive information reach and anticipate quality interactions within their network. New media provides the immediacy of accessing real-time information, the social connectivity, and interactive communications in a transparent and ubiquitous environment. There is a value of these new media characteristics to the CF. It allows for improved capabilities to plan, coordinate, and operate in a military environment. It allows for real-time collaborate intelligence gathering from all users that are tied in to the network. It also allows for two-way interactive communications between the leader and subordinates with limitless potential for training, improving

---

[73] Twitterers are also known as Tweeters. The online debate continues as to the proper term for "users who Twitter".

74 "Speec h from the Throne - Speech from the Throne," http://www.speech.gc.ca/eng/media.asp?id=1388; Internet; accessed 22 March 2010.

75 "CBC News - Canada - National Anthem Won't Change: PMO," http://www.cbc.ca/canada/story/2010/03/05/national-anthem.html; Internet; accessed 22 March 2010.

tactics and procedures, and feedback. The CF needs to consider the importance of these new media characteristics, as their pervasiveness will affect operations, and will influence the way people work and interact within the organization.

DIGITAL GENERATIONS: NATIVES VS. IMMIGRANTS

The CF is by its very nature, a hierarchical organization. Higher ranks and positions of authority are occupied by people who have experience in their environment and motivation to further their organization's agenda. Officers and senior non-commissioned members (the rank of sergeant to chief warrant-officer) comprise 40.2 percent of the personnel in the CF.[76] Within that demographic, Senior officers and chief warrant officers typically have 18 to 35 years of service. Therefore those officers and NCMs that are in highly influential positions all come from the same technical generation. They lead troops that have lived their entire lives in the Information Age. As baby boomers leave the workplace in droves and new recruits are being ushered in at a breakneck pace, on our present horizon lies a major challenge in the wide use of new media in the CF: the technical generation gap.

In 2001, Marc Prensky wrote an article on the effects that the arrival and rapid dissemination of digital technology has had on students in the 20th century and how their teachers had to adapt to the younger generation's thinking patterns. His findings identified that today's students "think and process information fundamentally differently

76 Statistics Canada. "A Profile of the Canadian Forces," *Perspectives.* http://www.statcan.gc.ca/pub/75-001-x/2008107/pdf/10657-eng.pdf; Internet; accessed 21 March 2010, 19, Table 2 – Characteristics of Military Personnel.

from their predecessors."[77] The largest separation of adaptation to technology was between the students and the teachers themselves. Prensky coined two designations that categorizes the technological generations: the *digital natives* and the *digital immigrants*.

Digital Natives

The generation born roughly between 1980 and 1994 has been characterized as the digital native[78] because of their "familiarity with and reliance on ICT."[79] This demographic is the "native speaker" of the digital language of computers, video games, and the Internet who are living their lives immersed in technology.[80] They learn differently than previous cohorts and are regarded by most social researchers as active experiential learners, proficient in multitasking, and dependent on ICT for access information and for social interaction.[81] Digital natives are, through their pervasive exposure to technology, able to piece information together from multiple sources. Oblinger and Oblinger summarize five observations from Prensky[82] about how the digital native processes information:

---

77 Marc Prensky, "Digital Natives, Digital Immigrants," *On the Horizon* 9, no. 5 (October, 2001), 1, http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf accessed 21 Mar 10.

78 *Ibid*., 1.

79 Sue Bennett, Karl Maton and Lisa Kervin, "The 'Digital Natives' Debate: A Critical Review of the Evidence," *British Journal of Educational Technology* 39, no. 5 (2008), 776, http://api.ning.com/files/AkclmKAQ9nT0vPJuCYL9261SknCvwP1UJ-RaVQ7kZumzWZVPq5iNlfGrqf0Jpc3wUnK8A07FuVmRXQ1WRqnre5q2z53PRnT0/Thedigitalnativesdebatecriticalreview.pdf ; accessed 21 March 2010.

80 Prensky, *Digital Natives, Digital Immigrants*, 2.

81 Bennett, Maton and Kervin, *The 'Digital Natives' Debate: A Critical Review of the Evidence*, 2.1, 2.5, 2.7, 2.11.

82 Marc Prensky, "Digital Natives, Digital Immigrants Part II: Do they really *Think* Differently?" *On the Horizon* 9, no. 6 (December, 2001), http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part2.pdf ; accessed 22 March 2010.

- *Ability to read visual images* – they are intuitive visual communicators;
- *Visual-spatial skills* – perhaps because of their expertise with games they can integrate the virtual with the physical;
- *Inductive Discovery* – they learn better through discovery than by being told;
- *Attentional deployment* – they are able to shift their attention rapidly from one task to the other, and may choose not to pay attention to things that do not interest them;
- *Fast response time* – they are able to respond quickly and expect rapid responses in return.[83]

The digital native is in synch with their technological environment. In fact, they do not realize their interaction with technology as ICT has always been a pervasive resource for them to use. Their abilities to multitask and to proficiently process information are prevalent in the culture of connectivity.

But how connected are the digital natives? As Prensky's student demographic moves from learning institutions to the workforce, industry has been keen in understanding the impact of the uprising of the digital native into the business world. In 2008, Nortel sponsored International Data Corporation (IDC) to conduct a survey to take "a global look at the exploding "Culture of Connectivity" and its impact on the Enterprise.[84] Their results further solidify the dependency of digital natives on ICT and categorizes our digital immigrants.

---

83 *Ibid*., 2.5. Oblinger and Oblinger's abridged review reflect Prensky's observations.

84 Romina Aducci and others, *The Hyperconnected: Here they Come!* (Framingham, MA: IDC,[2008]), http://www.nortel.com/promotions/idc_paper/collateral/hyperconnectivity_idc.pdf (accessed 22 Mar 10).

IDC fielded a global survey in March of 2008 where 2,367 participants across 17 countries in various industries, company size classes and age segments were questioned.[85] Survey questions ranged from device and application adoption of technology to location of use, attitudes about connectivity, and assessment of their companies' effectiveness deploying these new technologies. IDC used a data analysis technique called a cluster analysis, a procedure that determines natural groupings derived from the respondent's adoption and usage of technology.[86] As a result, four well-separated clusters with distinct demographics and technology adoption and usage were identified. The clusters were categorized as: *hyperconnected*; *increasingly connected*; *passive online*; and *barebones*.[87]

Our definition of digital natives includes the clusters of "*hyperconnected*" and "*increasingly connected*." Hyperconnected individuals, of which 60% are under the age of 35, have fully embraced the digital world and utilize more ICT devices and applications than the other clusters. IDC reported that the average hyperconnected person has reported using seven devices for work and home life and an average of nine applications.[88] Digital natives also would occupy the *increasingly connected* cluster as their main distinction from the *hyperconnected* is the use of fewer devices and applications, are half as likely to be involved with social networks, and a third as likely to use voice over IP (VoIP).[89] The migration from *increasingly connected* to

85 *Ibid*.

86 *Ibid*.

87 *Ibid*.

88 *Ibid*.

89 *Ibid*.

hyperconnected

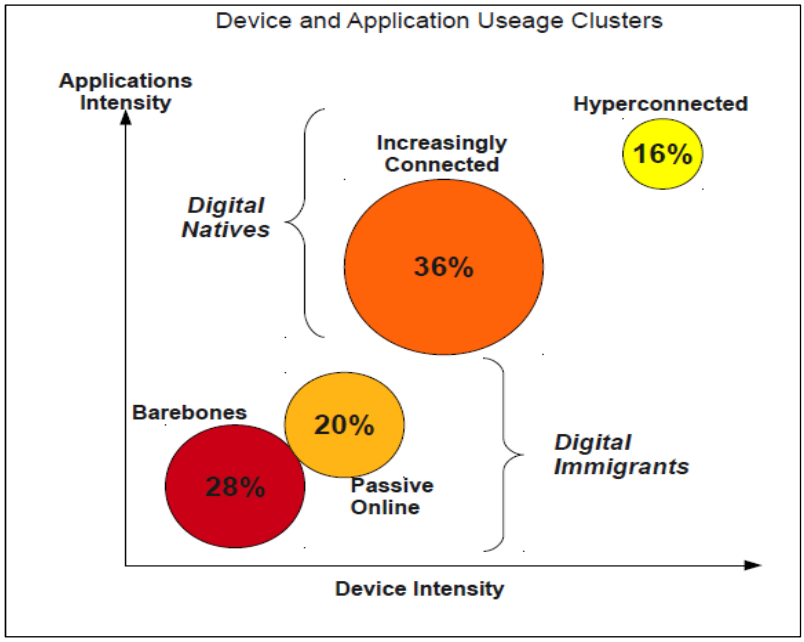

Figure 1: Device and Application Usage Clusters

Source: Aducci *et. al.*, *The Hyperconnected: Here They Come!*, 4.

will grow over time. In the next five years, as much as 40% of the total information workforce will fall into the category of *hyperconnected*.

Digital Immigrants

But what of the lower two clusters? They contribute to the category of digital immigrant. Prensky's definition of a digital immigrant are those in society that "were not born into the digital world but have, at some later point in their lives, become fascinated by and adopted many or most aspects of the new technology."[90] One of the major traits of the

90 Prensky, *Digital Natives, Digital Immigrants*, 1-2.

digital immigrant that Prensky proposes however is the fact that even though the digital immigrant learns to adapt to the new technological environment, they will always retain a tendency to rely on the more standard ways of doing things. This tendency is what he refers to as the digital immigrant's "accent". These accents are obvious in individuals who, for example, have a tendency to print our hard copies of computer generated text or presentations in order to edit them by hand – those who use the new technologies but still rely heavily on their traditional pre-digital habits.

Digital immigrants can be categorized into IDC's clusters as the "*passive online*" and "*barebones*" demographics. One-fifth of personnel that fall into the *passive online* cluster in the workplace are slow to accept ICT. They utilize a few devices, are beginning to experiment with some applications like SMS, but are not using the social-interactive applications like Facebook and Twitter. People in the *barebones* cluster tend to be ICT minimalists in the workplace, using email to communicate, relying on desktop access only to use the Internet, and using cell phones uniquely for voice calls.[91] At 28 percent of the population, this is a large demographic that have no buy-in to the culture of connectivity.

Overlapping the CF's demographics with the clusters identified by IDC, the CF faces a considerable technical divide between digital natives and digital immigrants.

CHAPTER SUMMARY

---

91 Aducci and others, *The Hyperconnected: Here they Come!*, 3.

The characteristics of new media are the framework for future communications in the CF. Characteristics like instantaneous connection and interactivity are important, not only to a soldier's personal communication's needs, but also to the structured, classified command and control networks of the army, navy, air force, and special forces. As the digital divide narrows, the expectation of what is achievable on commercial networks – both from a technological and informational perspective - will be transferred over to the expectations of the military's private networks. The CF will benefit from the present capabilities of the pervasive and social new media in the public domain.

The digital divide between the digital immigrants and digital natives will be with us for another fifteen years. Until such time that all of the digital immigrants have retired from the Forces, senior leadership will be responsible for identifying and mitigating the perceived risks that they identify as the roadblocks to complete integration of new media. I will address those risks and mitigations in Chapter 5. Failure to engage the impact that new media will have on the organization and on the operational art will ultimately disadvantage the command and control of the organization both in garrison and on operations.

CHAPTER 4

NEW MEDIA EFFECTS: WAR AND THE OPERATIONAL ART

> *I say to you that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle, a race for the hearts and mind of our Umma ["Community of Believers"].*[92]
>
> *al-Qaeda leader, al-Zawahri, 9 July 2005*

Advocates of the "Revolution in Military Affairs" champion the belief that advances in information and communication technologies have altered the nature and practice of warfare. Gathering, processing and distributing information using the technology of the Information Age enables clear operating picture of the battlefield while other technologies deny the same degree of knowledge to the enemy.[93] The fusion of advances in IT and the operational art has altered the nature and practice of warfare. Informationalism has contributed to information overflow as commanders and command staff have to sift through large amounts of collected information from a multitude of sources before they are able to apply their planning craft. The CF doctrine on *Command in Land Operations* identifies the pressures that information technology places on commander and cautions of its challenges:

> Technological improvement in range, lethality and information gathering continue to compress time and space, and create even greater demand for information. There is no denying the increasing importance

---

92 "Letter from Al-Zawahri to Al-Zarqawi July 9, 2005," Released by *the Office of the Director of National Intelligence*, http://www.dni.gov/press_releases/letter_in_english.pdf ; Internet; accessed 24 March 2010.

93 John Lynn, "The Evolution of Army Style in the Modern West, 800 - 2000," *The International History Review* xviii, no. 3 (August, 1996), 506.

> of technology to command, and to command and control systems. Advances in technology provide capabilities not envisioned even a few years ago. However this trend presents inherent dangers....[U]sed unwisely, technology can become part of the problem, contributing to information overload and feeding the dangerous illusion that certainty and precision in war are not only desirable, but also attainable. Commanders must resist the desire to become over-reliant on technology.[94]

New media enables not only the collection of information, but its modification. It is all about taking information developed for one purpose and using it in a different manner. An intelligence officer in theatre who combines the content of a blog commentary with photographs taken by troops on patrol and embeds these sources into a networked collaboration platform like Microsoft SharePoint is best leveraging the resourcefulness of new media. In order to bring success to the operational plan, the staff officer must be able to use this ability to modify and collaborate to their advantage.

Without the appropriate leverage, ICT innovations will produce unexpected consequences for military strategists. A largely unexpected consequence was noticed during Operation ENDURING FREEDOM involving U.S. and allied troops in Aghanistan. Global access to the Internet made the battle for the "hearts and minds", as the U.S. DoD put it, "all the more difficult."[95] The ease of insurgent propaganda involving valid information or a valid incident is laced with dis-information, mis-information or excessive information causing the intended message to be bastardized from its original intent and refocused towards the insurgent's benefit. New media provides greater opportunities for alienated

---

94 Department of National Defence, B-GL-300-003/FP-001 *Command in Land Operations* (Kingston: DND Canada, 2007), 1-17.

95 Hall Gardner, "War and the Media Paradox," in *Cyber Conflict and Global Politics*, ed. Athina Karatzogianni (New York, NY: Routledge, 2009), 13.

activists to intercommunicate, interact, and intervene together.[96] In both examples, unwarranted effects impact military operations when new media is not leveraged to the military's advantage.

We have concluded in Chapter 2 that both information and knowledge are sources of power. As technology improves and the demographics of hyperconnected digital natives increase, organizations such as the Canadian Forces need to leverage the changes in the networked society and their effects on the military, social, and political elements of war.

The goal of this chapter is to consider how new media is challenging the operational art of the staff officer and impacting the political, informational, and military elements of conflict. I will discuss the impact that new media has on each of the three elements, and identify how they effect the operational art of the military planner.

NEW MEDIA AND THE OPERATIONAL ART

Commanders and their staffs need to fully comprehend, not only military, but also nonmilitary (diplomatic, political, economic, financial, social, religious, etc.) aspects of the situation in a given theater when they plan, prepare, and execute major campaigns or operations. By better utilizing the tools of operational art, they can make decisions that will greatly contribute to the accomplishment of the overall operational or strategic objective.[97] The skillful application of operational art within the military environment

---

96 *Ibid*., 14

97 Milan Vego, *Joint Operational Warfare* (Newport, RI: U.S. Naval War College, 2007), I-7.

ensures obtaining and then maintaining the initiative of war.[98] In generic terms, operational art can be defined as:

> a component of military art concerned with the theory and practice of planning, preparing, conducting, and sustaining campaigns and major operations aimed at accomplishing strategic or operational objectives in a given theater.[99]

Operational art involves the employment of one's military forces to accomplish strategic objectives in a theater of war or theater of operations through the design, organization, and conduct of campaigns and major operations. It involves fundamental decisions about when and where to fight and whether to accept or decline combat.[100] The core of operational art is to win decisively in the shortest time possible and with the least loss of human lives and materiel. This is especially important in the present era of smaller forces, limited resources, and low tolerance of casualties by the political leadership and the public.[101]

To compliment this, The Canadian Forces Joint Publication, *Canadian Military Doctrine* outlines **diplomacy**, **information**, **military**, and **economics** (DIME) - the four principle instruments of national power[102] - as the primary lines of operation that require consideration within a conflict. Focus of this research will be on the diplomatic,

---

98 *Ibid*, I-6.

99 *Ibid*. I-7.

100 Scott A. Marcy, "Operational Art: Getting Started," *Military Review* 9 (September 1990), p. 107.

101 Vego, *Joint Operational Warfare*, I-6.

102 Department of National Defence, CFJP 01 *Canadian Military Doctrine* (Ottawa: DND Canada, 2009), 2-22.

informational, and military lines of operation,[103] and on the consequences new media has on operational art.

DIPLOMACY AND NEW MEDIA

Diplomacy is "the management of international relations by negotiation,"[104] and is dependent on the power of persuasion. Principally through their role in deterrence and coercion, armed forces play a major part in diplomacy, and provide resources to counter hostility, build and maintain trust, and assist in international development.[105] The operational planner then, has to be cognizant of how new media will impact the consideration of diplomacy within a campaign.

The rise and spread of non- governmental organizations and other civil society actors is attributable to achieving diplomatic solutions in conflict. Echevarria states that globalization—the spread of information and information technologies coupled with greater public participation in the world's economic and political processes—is transforming every aspect of human affairs.[106] Indeed, globalization has enhanced the real

---

103 Economics was not considered within this portion of the research. Defined in *Canadian Military Doctrine* as: "liberal or restrictive trade policies [that] can open up or deny markets, [and] the provision of foreign aid can be used to entice nations to behave in certain ways. Specific economic activities in support of national objectives may include disruption of trade, withdrawal of aid, or direct economic sanctions. The instrument of economics may require the application of military force to give it effect, as in the case of sanction enforcement operations." Although important at the strategic and operational levels of campaign planning, has no tie-in to new media, and therefore disregarded.

104 *Canadian Oxford Dictionary*, 2nd ed., p. 424.

105 DND, *Canadian Military Doctrine*, 2-24.

106 Antulio J. Echevarria II, "Globalization and the Clausewitzian Nature of War," *European Legacy* 8, no. 3, (2003), 317

and virtual mobility of people, things, and ideas as well as increased social, political, and economic interconnectedness worldwide.[107] These factors directly affect the consideration of diplomacy within operational planning.

The social network capabilities of new media make it easy to form virtual communities, mobilize support, and effect political change. Causes of all dimensions seek and find support on a global basis and consequently, local politics now plays itself out on a global scale. But as Deibert and Rohozinski identify, "the technological explosion of global civil society has not emerged without unintended and even negative consequences, particularly for non-democratic and authoritarian states."[108] The Internet has enabled new, nimble and distributed challenges to these regimes, apparent in enthusiastic opposition movements, protests, and even revolutionary changes to long-established political authority. Even among democratic states, the explosion of global civil society has presented serious challenges: as social justice groups have made use of new media to advance their position, so too have the militant groups, extremists, criminal organizations, and terrorists.[109]

In Rheingold's *Smart Mobs: The Next Social Revolution*, he illustrates the use of mobile phones as a social instrument in the 2001 "People Power II" demonstrations in the Philippines. Over 1 million people used text messaging to coordinate and mobilize

---

107 *Ibid.*

108 Ronald J. Deibert, and Rafal Rohozinski. "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet." Deibert, Palfrey, Rohozinski, Zittrain, (eds.), *Access Denied* (MIT Press: 2007).

109 *Ibid.*

peaceful demonstrations to protest the sudden halt to the impeachment trial of President Joseph Estrada. Political instability in a country that had seen significant increase in the availability and use of ICT capabilities – a population where 40 percent make less than one dollar a day, 5 million people own cell phones – led to the masses of protesters.[110] The military withdrew support from the regime and Estrada was overthrown. The proliferation of new media to the masses is empowering social groups who previously did not have a voice or the medium to connect with like-minded members of their culture.

Diplomacy is meant to influence the members of a targeted society. The increasing ability of people in most parts of the globe to access international sources makes targeting particular audiences more difficult. Information intended for foreign audiences, including public diplomacy, increasingly is consumed by domestic audiences and vice-versa. Messages disseminated to any audience except individual decision-makers (and perhaps even then) will often be replayed by the news media for much larger audiences, including the Canadian public. This difficulty in distributing the diplomatic message can be alleviated by using new media to our advantage and getting accurate and relevant information out to the masses first, and in a format that is easy to understand.

The effect of new media on diplomacy will affect the planner's considerations of the employment of forces within the battlespace. Different operational courses of action are dependent on the stability of governments, the number of NGOs and aid agencies that are employed within the area of operations, and the diplomatic effect we have had with both

110 Harold Rheingold, *Smart Mobs: The Next Social Revolution* (Cambridge, MA: Basic Books, 2002), 158-160.

domestic and foreign audiences. New media can play a role in assisting in our diplomatic endstates by getting the informing and influencing messages of Public Affairs (PA) and Information Operations (IO) to a target audience. It can also hinder diplomacy by acting as a social instrument to empower social groups to counter the diplomacy that is ongoing between governments and regimes. Therefore, the planner has to consider how the diplomatic message – or lack of one – will affect courses of action in the operational plan.

THE INFORMATIONAL LINE OF OPERATION

Information itself is a strategic resource vital to influencing national interests. Military operations, in particular, are dependent on many simultaneous activities, relying on timely flow and dissemination of information to aid real-time effective decision making.[111] Information influences domestic and foreign audiences including citizens, adversaries, and governments.

Mattox affirms that the free flow of information from the battlefield and from the deliberative chambers of government enabled by new media technologies such as smart phones, television, and the Internet has more acutely exposed the issues and results of war, and has rekindled the unwillingness of average citizens to accept critically moral valuations about war. While, in earlier eras, the lack of information from the battlefield may have afforded strategists and policymakers the leeway to conduct war without regard to public reaction over issues with obvious moral implications, those days are forever

111 DND, *Canadian Military Doctrine*.

gone.[112]

The endstate of balancing government and society within the elements of war is difficult to achieve in perpetuity. Now that societal issues such as the plight of women and girls in Aghanistan, and child labour issues in Africa and Asian-Pacific regions, for example, are brought to the forefront because of the reach of new media to influence the operational and strategic goals of governments and militaries. This is not to say, of course, that the network society is necessarily more morally judicious, or even more morally sensitive, simply because it now has almost immediate access to vast amounts of data with moral implications.[113] Knowledge does not guarantee virtuous conduct. Rather, it simply means that the access to information afforded by the Information Age now enables the public to form, to an unprecedented extent, moral judgments (accurate or not) concerning the political and military decisions directing the conduct of war.[114]

The view of society on the social issues related to the theatre of war direct impacts operations. Afghanistan's President Harmid Karzai's proposition in April of 2009 to introduce law that includes a provision making it illegal for a Shia Muslim woman to refuse to have sex with her husband and also make it illegal for a woman to leave the house without her husband's permission, or have custody of children.[115] As new media

112 John Mark Mattox, "The Clausewitzian Trinity in the Information Age: A Just War Approach," *Journal of Military Ethics* 7, no. 3 (November 2008), 203.

113 *Ibid.*

114 *Ibid*.

115 CBC News, "Rape Law Hurting Efforts to Sell NATO Role in Afghanistan: NATO Chief,"

promulgated this story to the forefront of the news cycle and the blogs of the Internet, it created enormous pressure on NATO member governments to influence such a law. Jaap de Hoop Scheffer, NATO Secretary General realized that public outcry over such a law could negatively affect commitments to ISAF. "How can I defend — or how can the …Canadian government… — that our boys and girls are dying there in the defence of universal values, and you see a law almost coming into effect… that fundamentally violates women's rights and general human rights, then I have a problem." [116] Karzai immediately acquiesced to international pressures and called for a review of the law through parliament. Although the end result was a "softening" of the wording of the law[117] and eventually becoming law in July 2009[118]

This example demonstrates how information plays a role in the effect on operations. New media enabled the relevant social issues of a war to be disseminated worldwide. It stirred the emotions of the public and also provided the interactive venue to state their opinions on the matter. This voice applied pressure on the Canadian government to address the issue to the Afghan government and to NATO. The ramifications of this particular example on the operational art, had the potential to effect government foreign policy and

---

http://www.cbc.ca/world/story/2009/04/04/law-nato.html; Internet; accessed 17 April 2010.

116 *Ibid.*

117 The wording of the law defining a woman's role as "readiness for sex and not leaving the house without the husband's permission," was changed to requiring Shiite women to give their husband "their sharia rights" when it comes to sex, a reference to Islamic law., and allowing women to leave their own homes "according to local customs."

118 Jim Sciutto, Bruno Roeber, and Nick Schifrin. "Afghanistan President Hamid Karzai Passes Controversial Law Limiting Women's Rights," *ABC News International.* http://abcnews.go.com/International/story?id=8327666&page=1; Internet; accessed 17 April 2010.

military troop deployment (should a topic like this been a deciding factor of renewing commitments to NATO). These are all components that will affect the decision-making process of the commander and the staff and how the political and informational lines of operation are developed.

MILITARY EFFECTS AND NEW MEDIA

Military power is applied as appropriate to achieve national objectives. Military power is normally used only as a means of last resort when other instruments of national power have failed, or are at risk of failing, to protect national interests.[119]

The dominant tendencies of war's "uncertainty and chance" are counterbalanced by the command and control (C^2) the commander employs on the battlefield. ICT is the backbone of C^2 and provides a direct bridge between the political-strategic and the tactical levels. Modern information technology has greatly improved the operational commander's knowledge about the locations and movements of friendly and enemy forces. The beginnings of what is called the *common operating picture* for commanders at all levels of command are becoming a reality. Wide-area communications are greatly improved; garbled or incomplete information is being replaced by standardized messages in easy to access formats that offer less chance for confusion or ambiguity.

This however, is a double edged sword as strategic players have direct ability to influence the tactical battle. ICT is an unfortunate enabler that erodes mission command and staff planning. The "5,000 mile screwdriver" effect that modern communication allows

119 DND, *Canadian Military Doctrine*.

undermines the purpose and functionality of the operational staff. Add on the social layer of new media, and the complexity of situational awareness greatly expands.

Much is also unclear about current technical developments in military networks. While considerable faith is placed on network-enabled operations or network-centric warfare (NCW), academics such as Mitchell state that concepts like NCW are still in their infancy and therefore difficult to determine if they are of decisive advantage at the operational level. Mitchell states, "[a]s in the case of nuclear weapons, it may ultimately prove impossible to implement information technologies militarily in the matter predicted by NCW's early proponents."[120]

What is irrefutable is that the importance of information is growing rapidly and has a critical impact on the application of operational art. Information must be accurate, timely, and relevant.[121] With new media technology, almost any information can be transmitted instantaneously and at very little cost. Yet the sheer volume of information available makes it extremely hard to distinguish what is accurate from what is false. The volume of information can also fluctuate greatly. Information is received, evaluated, and transmitted to users. However, the enemy can also take it away without the commander's knowledge. It is extremely difficult to know what the enemy knows and when he obtained that knowledge. An almost unlimited amount of information often impairs the ability to understand it. Then the important information cannot be distinguished from the

120 Paul T. Mitchell, *Network Centric Warfare and Coalition Operations: The New Military Operating System* (New York, NY: Routledge, 2009), 31.

121 Vego, *Joint Operational Warfare*. III-66.

unimportant, and too-large amounts of information simply cannot be absorbed.[122]

Information overload also fuels the "uncertainty and chance" of war. The ubiquitous accessibility of new media puts the tools required to collaborate, create value, and cooperate at everyone's fingertips.[123] Similarly, although there is recognition that quality, not just quantity, of information is an important consideration, capitalizing on the accuracy, relevancy, and timeliness of information is critical. A planner who is to coordinate a resupply convoy to a forward observation base (FOB) has to ensure that the information he has on the enemy threat, the conditions of the route, the volume of traffic on the road, and other missions deploying to the area is accurate. If information that is populating the network is outdated, inaccurate in its observations or there is a conflict in the content of two differing sources, the planner will have to assume risk on taking more time to evaluate the information or collect collaborating information from other sources or accepting the accuracy of the information in the judgement of his plan. Collaboration at all levels of planning within a net-centric environment does not eliminate the risk that information is not easily verified or validated for use; it potentially increases the "fog" of war for commander and staff as to what information is accurate or even useful.

It can be argued that network-centric information sharing is far from reaching maturity.

---

[122] Myriam Dunn, "Part II—Theory: Concepts to Explain a Changing International System," in Kurt R. Spillman and Andreas Wenger, editors, *Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment,* Zuercher Beitraege zur Sicherheitspolitik und Konfliktforschung No. 64 (Zurich: Forschungsstelle fuer Sicherheitspolitik und Konfliktanalyse der ETH Zuerich), p. 72, quoted in Milan Vego, *Joint Operational Warfare*.

123 Don Tapscott and Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (New York: Penguin Group, 2006), 1, quoted in Mitchell, *Network Centric Warfare…*, 9.

As the present day staff officer has become more reliant on technology to complete operational art, they also have to deal with the potential of information overload and will have to develop the skill of being able to quickly assess the accuracy and relevancy of information and collaborate that information with the right person within the battlespace at the right time.

THE ENEMY AND NEW MEDIA

Informationalism and new media technology knows no geographic or geopolitical boundaries. As I have alluded to throughout this paper, insurgent and terrorist organizations are leveraging new media to advance their cause, recruit and fundraise, and communicate covertly. Their actions directly affect all three of the diplomatic, informational, and military lines of operation.

In *The Mind of the Terrorist*, Post, after ample description of the history, motivations, and threats of nationalist-separatist, social-revolutionary, and religious extremist terrorists, identified that the U.S. and other nations that are combating terrorism have not fully entered "the arena of strategic communications, let alone developed a strategy for countering the highly effective media strategy developed and refined by … terrorist adversaries."[124] He posits:

> The major terrorism organizations have media committees whose main tasks is to get their message out quickly and effectively, putting their own spin on events, playing optimally both to their external and internal audiences. They are adroit at portraying themselves as victims whose actions were defensive and were

124 Post, *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to Al-Qaeda*, 245.

required by their enemy's actions.[125]

Post confirms that terrorist organizations have effectively employed new media in their efforts to incite activism, to share tactical and operational information, and to conduct their terrorist act. For example, Hezbollah has proven highly effective at mobilizing modern-day technologies to suit their terrorist agenda. Hezbollah employs computer and information technology experts to disseminate their agenda using Internet websites, computer games, and their own satellite broadcast Al-Manar TV (the beacon).[126]

Another group that has proven particularly effective at mobilizing new media is Hamas – the Islamic Resistance Movement and Palestinian military wing. The Internet site for the al-Qassam Brigades[127] maintains websites that allow communications between Hamas members and other sympathizers who may wish to engage in acts of violence.[128] They also use these sites to entice non-members who are sympathetic to the cause along the path of violence. Their use of new media has allowed them to provide instructions for the production and exploitation of terrorist weapons. Al-Qassam has also instituted an online "military academy" which provides courseware for bomb-making, manufacturing plastic explosives, and the selection of terrorist targets.[129]

---

125 *Ibid*., 245-246.

126 *Ibid*., 169.

127 The *Izz ad-Din al-Qassam Brigades* are named as the military wing of Hamas.

128 *Ibid*., 188.

129 *Ibid*., 188.

The enemy has understood the power of the Internet and has used digital media to incite the "violence and passion" of the global audience. Moreover, the public statements by enemy leaders such as bin Laden in periodic releases of video messages through mainstream media sources like Al Jazeera, or through videos and voice messages on the Internet, demonstrate that insurgent leadership can address support bases to give guidance, motivate, or to garner further support, while at the same time challenging or vexing the opponents of al Qaeda.[130] The advances in ICT and the ability to mass distribute their message gives power to the enemy as Western governments and militaries struggle to disrupt their psychological operation's OODA loop.

CHAPTER SUMMARY

In this chapter, I set out to demonstrate how new media is challenging the operational art of the staff officer and impacting the political, informational, and military elements of conflict. Commanders and their staffs need to fully comprehend, not only military, but the diplomatic, political, economic, financial, and social aspects of the situation in a given theater when they plan, prepare, and execute major campaigns or operations. New media does challenge the diplomatic, informational, and military lines of an operation or campaign.

The influence of diplomacy on a targeted society is more difficult because of new media's ability to enable people to access international informational sources. Likewise, the

130 Echevarria, "Globalization and the Clausewitzian Nature of War," 324.

information from the military or government intended for foreign audiences, including public diplomacy, increasingly is consumed by domestic audiences and vice-versa. This difficulty in distributing the diplomatic message can be alleviated by using new media to our advantage and getting accurate and relevant information out to the masses first, and in a format that is easy to understand. The military planner then, has to leverage new media in order to get the diplomatic message out to influence the population.

The view of society on the social issues related to the theatre of war direct also impacts operations. New media enabled the relevant social issues of a war to be disseminated worldwide and has stirred the emotions of the domestic and foreign public and also provided the interactive venue to state their opinions on the matter. This voice applies pressure on the government to address these issues and directly influence foreign policy. As foreign policy shifts, so too does the focus of operations in theatre.

New media has greatly improved the operational commander's common operating picture and situational appreciation for the battlespace. There is considerable potential for further application of new media technologies into the battlespace in order to assist commanders to make timely and accurate decisions. Military forces however, have to deal with the abundant volume of information available making the modern day planner more reliant on technology to complete operational art. They have to contend with the potential of information overload and will have to develop the skill of being able to quickly assess the accuracy and relevancy of information and collaborate that information with the right person within the battlespace at the right time.

The influences of new media on the operational art require focus by the Canadian Forces

at the operational and strategic levels. Chapter 5 will address the problem space and explore why new media is of concern within the CF.

CHAPTER 5

THE CHALLENGES OF NEW MEDIA IN INFORMATION OPERATIONS

> *The proactive approach in the implementation of new media is not without risk, and there have been less than perfect results, but the benefits far outweigh the concerns.*[131]

INTRODUCTION

It is an understatement to say that information technology has fuelled significant changes, enormous improvement and advances in society. Our dependence on new media has simultaneously created a myriad of liabilities that threaten these same advancements. McNamara observes that the search for solutions must incorporate an increased awareness of the human behavioural dimension of this complex problem. While new media has introduced a new set of problems, the issue is not with the technology but the human use and misuse of that technology. Apprehension towards the use of new media in the battlespace must be founded upon such an understanding, since people are both the source and the solution to the problem.[132]

This chapter focuses on information operations and new media. Two core activities of Information Protection and Influence will be discussed. New media will introduce

---

131 "Public Relations: Exploring New Media ... Shaping the Battle Space," *Naval Forces* 31 (2010, 2010), 53, http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=48181360&site=ehost-live.

132 Michael R. McNamara. "Dysfunction in Cyberspace: The Insider Threat." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000.

challenges and risk to information protection in both operational security and information security domains. Influence activities, as defined by perception management, will also have to consider the impact of new media on the message that the operational commanders want to portray to target audiences. The future application of new media technology in the battlespace will also be discussed as to how new technologies will enhance intelligence and information within an operational theatre.

INFORMATION OPERATIONS AND NEW MEDIA

The use of new media within the battlespace is subject to the functions of Information Operations (IO). CF doctrine *Land Operations* defines IO as:

> Coordinated actions to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other approved parties in support of overall objectives by affecting their information, information-based processes and systems while exploiting and protecting one's own.[133]

Land Operations affirms that IO is not an operation unto itself. Instead, it is a coordinated collection of capabilities related to maximizing the use of information while at the same time denying it to the adversary.[134] Dearth identifies a synergy within IO between information assurance, critical infrastructure protection, information dominance, and operational effectiveness.[135] A critical aspect to IO however, is Perception Management (PM).

---

[133] Department of National Defence, B-GL-300-001/FP-001 *Land Operations* (Kingston: DND Canada, 2008), 5-44, http://armyapp.forces.gc.ca/ael/pubs/B-GL-300-001-FP-001.pdf.

[134] *Ibid.*

[135] Douglas H. Dearth. "Operationalizing Information Operations: C2W…RIP." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000. Information assurance combines the confidentiality, integrity, and availability of information. New media demonstrates that it is no longer adequate to secure information by physical means. Information dominance requires timely and accurate all-source intelligence on the adversary and the operational environment, as well as the timely and accurate information on the location and capabilities of one's own forces. (Col John Boyd's OODA Loop).

Seigel defines PM as the ability to shape worldwide perceptions in one's favor to foster compliance and facilitate mission accomplishment.[136] Public Affairs, public diplomacy, psychological operations (PSYOPS), and deception all play significant roles with PM. According to Seigel, PM seeks to:

- build and preserve public opinion support (at home and abroad) to gain an maintain legitimacy;
- communicate intent and objectives to hostile and/or third parties to establish a high degree of credibility so they fully understand the consequences of their actions; and
- influence the attitudes and behaviors of the local populations so they act in accordance with US objectives.[137]

PM will target many audiences. Domestic audiences require information about operation's rationale, risks, and benefits, as without public support, democracies cannot sustain military engagement. Meanwhile, adversaries' and third-party perceptions have to be managed so that they reorder their priorities and strategies in accordance with the military's goals and objectives.

Garfield suggests that PM presents itself as the element of greatest gains and risks within IO. The goal of the adversary is to undermine the public support for military action of the Allies. The campaign waged by General Aideed in Somalia which resulted in the

---

[136] Pascale Combelles Siegel. "Perception Management: IO's Stepchild." *Information Warfare: Separating Hype from Reality*, ed. E. Leigh Armistead (Washington, DC: Potomac Books, 2007), 27.

[137] *Ibid.*

withdrawal of US forces, largely undermined domestic support because of the images seen on TV and in the print media. During the Kosovo war, Milosovich's regime presented images designed to sow doubts in the minds of wider Alliance publics, in the hope that it would result in declining support for military action.[138] The "first to post" adage carries significant weight within the conduct of and IO campaign. The important element to grasp in Derth's focus on IO is the shift from the concept of purely kinetic attacks intended to destroy, to the concept of influence designed to manipulate the opponent into a disadvantageous situation – the idea of imposing one's will on the enemy.[139]

Canadian doctrine identifies several core activities inside of IO[140]: information protection activities, which safeguards friendly information, thereby inhibiting an adversary's understanding; and influence activities, which is the primary means of influencing will. New media within each of these two core activities will offer as challenges to which commanders within the CF need to overcome.

INFORMATION PROTECTION ACTIVITIES

Operational Security

One of the ten "principles of war" that govern the application of military power is security. The effective application of security forms the fundamentals of military

---

[138] Andrew Garfield. "Information Operations as an Integrating Strategy: The Ongoing Debate." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000.

[139] Dearth, "Operationalizing Information Operations…".

[140] DND, *Land Operations*, 5-45.

operations and must be understood by commanders and staff at all levels.

Security protects the cohesion of a force and other elements of its combat power. During operations it serves to guard vulnerabilities and protect vital interests. In the case of operations security (OPSEC), the protection of information must be assured at all times, not just during the conduct of operations. Security further provides the freedom of action to achieve objectives as well as preventing the enemy from gaining an unexpected advantage. Security does not, however, imply undue caution and avoidance of risks, as bold action is essential to success in war.

The publication *CF Information Operations* identifies OPSEC as a "methodology that can be applied to any operation or activity for the purpose of denying critical information to the enemy. OPSEC is applied to all military activities at all levels of command."[141] A sound OPSEC plan by the commander outlines the critical incidents and actions that can be observed by adversary intelligence systems that can be pieced together or interpreted to derive critical information that will jeopardize the secrecy, timing, or execution of operations.[142]

The challenges to OPSEC are many. The commander has the internal challenges of commanding digital natives; most of whom embody a culture of communicative openness, with few qualms about sharing private information and thoughts on "personal"

---

[141] Department of National Defence, B-GG-005-004/AF-010 *CF Information Operations* (Kingston: DND Canada, 1998), 2-2.

[142] *Ibid.*

communication media.[143] Some members of younger generations may not have a sound understanding of the potential for the enemy to view personal postings or listen in on cell phone conversations. Douglis observes that they display naïvety towards the domains of social networking.[144] They consider their private space on social networking is exclusive to them and to those who they choose to share it with. Many do not seem to share the healthy paranoia related to new media that digital immigrants had with traditional communications – letters and phone calls – in earlier operations.[145]

The reluctance of using new media within the military environment is due to the openness of access that new media applications have within cyberspace and the effect this openness will have on OPSEC. A singular occurrence of critical information that is inadvertently – or carelessly – broadcast on a Facebook account, blog, YouTube, or email can be compiled by search engines and correlated with other open-source information to provide an adversary accurate intelligence.

Some OPSEC occurrences are more blatant than others. YouTube for example, houses hundreds of home made movies from troops in combat situations, or comedic videos of troops relieving the pressures of battle. However, the information that resides behind or in the clip provides considerable information that endangers OPSEC. For example, a

---

[143] Collings and Rohozinski, *Bullets and Blogs: New Media and the Warfighter*, 54.

[144] Fred Douglis, "On Social Networking and Communication Paradigms," *IEEE Internet Computing*, 12, no. 1, pp. 4-6, Jan./Feb. 2008, http://doi.ieeecomputersociety.org/10.1109/MIC.2008.17; Internet; accessed 18 April 2010.

[145] *Ibid*.

YouTube video[146] released in 2004 demonstrated how military videos impacted OPSEC in theatre. Soldiers have been posting videos of improvised explosive devices (IED) for years from operations in Iraq and Afghanistan. While the intent of each author who posted the video can only be speculated, its effect demonstrated the power and damage created by on convoys the blasts. One unintended result however, was a change in training, tactics and procedures (TTPs) by the insurgents employing IEDs. An analysis of these IED videos (and notably, some of their own video that their personnel captured during roadside attacks), saw what he reactions of the soldiers on site of the blast: what offensive and defensive postures they took, where they parked their vehicles, how many people showed up on site, and how long it took follow on forces to arrive on scene. The 2004 video in question shows a second IED blast at the same location, striking the exposed military personnel assisting the victims of the first blast, and protecting the blast site. The videos of US and allied forces exposed the security gaps of vehicle convoys, not by the intended content of the footage, but what was analyzed in the background.

Information Security

Another associated risk to new media technology is the compromise of confidentiality, integrity, and accuracy of information. The enemy will purposefully publish and promulgate inaccurate information on actual incidents in order to compromise the integrity of available information. A military blogger may make comments or state facts that may misrepresent the mission and undermine the operation. Military forces must react to the accuracy and confidentiality of information that is posted online. Inaction or

[146] "IED In Afghanistan," http://www.youtube.com/watch?v=PKeNvIHC6hs; Internet; accessed 21 March 2010.

a slow response by military officials to set the record straight will only support the enemy's lies. For example, a bomb dropped by ISAF forces strikes a military target and produces the desired effect. Collateral damage reports two locals injured in the blast. Al Jazeera however, picks up the Taliban correspondence through their website that ISAF had purposefully targeting a local market and killed 23 civilians, including children. This message is first to post, and therefore has a certain "stickiness" to the audience. ISAF publishes a statement after the fact; however the sensationalism of the Taliban's message over washes the truth.

To protect the integrity of military designated[147] networks such as the CF DWAN[148], new media sites are inaccessible from the DWAN, and new media technologies cannot integrate with the network. Other devices like smartphones, have their integrated online capabilities restricted or removed. Denying access on military unclassified systems –- will only drive digital natives to connect to the social network through their personal means.

Adopting new media into the main stream of DND is inevitable. There remains little choice but to engage new media as a part of the larger media explosion. Failure to accept new media would leave an undesirable vacuum in which the adversary's version of reality

---

[147] Designated information is not classified. Designated information pertains to any sensitive information which does not relate to national security and cannot be disclosed under the access and privacy legislation because of the possible injury to particular public or private interests. Designated information (PROTECTED A and PROTECTED B only) can be processed on computers residing on the Defence Wide Area Network. Classified information can be designated *Top Secret*, *Secret* or *Confidential*. These classifications are only used on matters of national interest. Classified information is processed on dedicated private secure networks.

[148] DWAN: Defence Wide Area Network.

would become the dominant perception.[149] U.S. Department of Defense has realized this inevitability and has published new policy in February 2010 that will allow U.S. military personnel access to social networking sites from the military's non-classified computer network, NIPRNET.[150]

An article in *The New York Times* comments that this development is considered a step forward by advocates of social networking in the military.[151] Advocates have criticized that local commanders, sometimes for vague or arbitrary reasons, have shut down personal blogs or restricted access to social networking. Now with the new directive in hand, all DoD components will reconfigure NIPRNET to provide access to Internet-based capabilities including collaborative tools, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g. YouTube, Facebook, MySpace, Twitter, Google Apps).[152] The American directive is sound: it equally restates the rules and regulations on official use, OPSEC, representation of policies and official positions of DoD, and records management. The office of the Deputy Secretary of Defense is assuming risk on the employment of external new media to the outside world. When the CF follows in their footsteps, they too will have to assume risks.

Dealing with the Risks of Information Protection Activities

---

[149] Caldwell, Murphy and Menning, *Learning to Leverage New Media*, 3.

[150] NIPRNET: Non-classified Internet Protocol Router Network.

[151] James Dao, "Military Announces New Social Media Policy," *NYTimes.com*, http://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy/; Internet; accessed 31 March 2010.

[152] U.S. Department of Defense, "Responsible and Effective use of Internet-Based Capabilities," *Deputy Secretary of Defense, Pentagon*, http://www.defense.gov/NEWS/DTM%2009-026.pdf; Internet; accessed 31 March 2010.

Education and training in the use of new media are essential to mitigating the risks of Information Protection. Our time invested in workups prior to deployment for tactics and drills, weapon and communication systems, and knowledge and understanding of the environment to which they are to be deployed is considerable.[153] Education and training on the use of new media is critical for operational success and must be continually in the forefront of training and simulation. National assets such as the Canadian Forces Network Operations Centre (CFNOC), CF Electronic Warfare Centre (CFEWC), and 21 Electronic Warfare Regiment need to red-team interception, collection, and analysis of personnel during workups to deployment in order for soldiers to understand how easy it is to collect and analyze personal information in the hopes that, confronted with real-time examples and data of open-source intelligence (OSINT), soldiers will become more sensitive and cautious with open-source social networking. OSINT needs to expand efforts in using social networking against the enemy as well. The tools that we use to train our forces also need to be put into play to collect our own intelligence on the enemy's actions through the global network of open-source.

A renewed effort in education and training in regard to new media is important; however one cannot overlook the necessity for the chain of command to trust the digital native. Trust is the linchpin in most secure environments. Rules and regulations can be enforced for the physical security of information, but retained knowledge – the information in the minds of the soldier - is a consideration of trust in the individual. When an officer or NCM receives a security classification, the military has deemed that his or her

[153] This is certainly the case for Canadian and other Western forces. Levels of pre-deployment training for other nations will very significantly based on their national contributions and training philosophy.

background is suitable – there are no overt indications of criminal activity or conditions that would make the individual an easy target for coercion - to trust the individual to collect, process, and safeguard sensitive information. Yet we treat information different than we do weaponry. A soldier is issued a whole battery of weapons and is authorized to use them in theatre; and we trust the individual that they will not shoot their comrades. We have trained that soldier to use those weapons properly. We have to do the same for new media.

All members of the CF need to be properly trained on how to engage audiences, sanitize the information they post, and protect the critical information they have on operations from being place in the open-source realm.[154] The creation of new media "rules of engagement" have to be established and applied.

INFLUENCE ACTIVITIES

The Message

Similarly, the soldier can be a vital participant in the influence activities of the CF. Allowing the CF member to be an active participant in the global social network will enable a broader swath of information and exposure to many different sources and interest groups. A soldier who has been educated and trained as to what the focus of the message should be is able to be influential within his or her social group. Enabling the soldier to get the story out in a manner that gives credit to the operation and the organization is an effective tool in winning the IO campaign. As we discussed Mattox's views in Chapter 4, the access to information that new media has afforded to the public the ability to form

[154] *Ibid*.

moral judgments concerning political actions and military conduct. This requires adaptability by both the government and the military to society's new medium of communication – one that is able to harness the "violence and passion" of the global audience and influence their perceptions.

The CF's first challenge in the operating environment is achieving meaning with key audiences. This will be achieved by getting the message out on the media that they frequent, in a vernacular that they understand, and through speakers that they trust.[155] Their second challenge is the speed of the message. As we discussed with perception management, shaping the conditions of acceptance and perceptions of society in the Information Age requires the message to be first to the post, accurate, and influential. Finally, the CF's challenge with new media within the social element is the ability to be proactively interconnected with the network society so that influence can be attributed to the "citizen journalist" or blogger. All three of these challenges will require change in process and a shift in organizational responsibilities.

"The medium is the message."[156] The infamous quote that the great Canadian Marshall McLuhan wrote in *Understanding Media: The Extension of Man* in 1964 enlightened generations that a medium affects the society in which it plays a role not by the content delivered over the medium, but by the characteristics of the medium itself.[157] Distinctly

---

[155] Collings and Rohozinski, *Bullets and Blogs: New Media and the Warfighter*, 65.

[156] "The Estate of Marshall McLuhan," http://www.marshallmcluhan.com/main.html; Internet; accessed 31 March 2010.

[157] Herbert Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGraw-Hill, 1964), 9.

enough, McLuhan also wrote that the "content" the medium broadcasts becomes itself, a medium. To achieve meaning with key audiences, the CF has to be effective in its use of the "new medium" and influential in the message.

The CF needs to play both an offensive and defensive role in the conduct of IO. Our focus is on the societal elements of war; therefore both offensive and defensive roles play equally amongst our adversaries and our home audience. Offensive IO is adopted against audiences (adversarial or friendly) who do not support the campaign while defensive IO is used on audiences that demonstrate interest and support to operations. Both types of IO are achievable through the use of media operations (Public Affairs - PA) and psychological operations (PSYOPS).

The purpose of media operations is to protect the legitimacy and credibility of operations and promote widespread understanding of the operations.[158] It communicates through PA who facilitates information to audiences through all media sources. PSYOPS however, influences the perceptions, attitudes, and behavior of selected individuals or groups. Unlike PA who manages the information communicated by third party sources, PSYOPS retains direct control over content and dissemination.[159] While the idea of using PSYOPS against our own citizens may not sound palatable to some, the fact is, the CF needs to invest in the production and dissemination of an influential message in a manner to target the audience without damaging the reputation and credibility of the role of PA. This is

---

[158] *Ibid*., 5-48

[159] *Ibid*., 5-47.

achievable through new media.

We have already commented on the pervasiveness and interaction of new media. Canadian trends in social media sites have been gaining momentum. In 2008, the CRTC identified that conversational media and social networking sites had over 20 million unique visitors accounting for over 85 per-cent reach of the Internet audience. 15 million unique visitors visited blogs for 63 per-cent reach of the audience.[160] This is a growing demographic that needs to be influenced by the CF.

The CF needs to seize this opportunity by directly influencing the "message." This can be accomplished in different manners. First, is by direct administration of social networking sites and blogs. Present exposure of the CF within new media is sparse at best. There is no official CF site on Facebook, for the Chief of Defence Staff or other major figures within the organization.[161] The official media publication "The Maple Leaf" does not have a blog application; "share" API or other commentary function besides a "comments" tab.[162] There is also an absence of official CF coverage on military blogging websites like www.milblogging.com that hosts over 2,600 military blogs in 43 countries. This site, an internet database for organizing military blogs, has only 25 milblogs from Canadian participants.[163] The forum for choice to suppress the appetites of

---

[160] Industry Canada and others, *Regulating Content on the Internet: A New Technological Perspective*

[161] There are Facebook sites that are titled "Canadian Forces" or "Canadian Army", however they are not listed as official pages and lack considerable amount of detail. These are private pages.

[162] Department of National Defence. *The Maple Leaf*, http://www.forces.gc.ca/site/commun/ml-fe/index-eng.asp; Internet; accessed 31 March 2010.

[163] "The Story of Milblogging.com," http://www.milblogging.com/about.php; Internet; accessed 31 March

Canadian military conversationalists is *Army.ca*.[164] This is an unofficial site that has an array of military forums and boasts over 850,000 posts, 51,000 topics by 25,650 members. The site also contains a "wiki"[165] of CF and DND information. The CF needs direct input into the creation of blogs for comment by the people and by CF members. The engagement of third party bloggers that would provide highly indexed content with chosen keywords for maximum exposure are options if manning and skills are lacking within the present cadre of military personnel. This would accomplish two effects: proactive interconnection with society; and connection in a media frequented by the target audience. The use of video sites like YouTube need to have CF channels that adhere to the challenges of OPSEC and still portray troops in action, soldiers lives in austere conditions, and evidence of the effects that Canadians are having in theatres such as Afghanistan and Haiti. The CF needs to be "first to post" to get the message out on what is being accomplished in the tone and framing that influences the audience. Should these productions by PA led or PSYOPS led? I would say both. It would accomplish both offensive and defensive IO in influencing key audiences.

The Technology

The CF has an opportunity to commence an information engagement through the use of new media on the battlefield. Military Research and Development in the use of new media tools has the potential to increase protection of soldiers on the ground and the

---

2010.

[164] "Army.ca Forums - Index," http://forums.army.ca/; Internet; accessed 31 March 2010.

[165] A "Wiki," meaning "fast" in Hawaiian, is a website that allows easy creation and editing of interlinked web pages via a web browser.

collection of information for intelligence sources. New technologies that permit augmented reality (AR) will assist the soldier in operations. AR adds graphics, sounds, haptic[166] feedback and smell to the natural world as it exists. Both video games and cell phones are driving the development of augmented reality. AR will enable the user to benefit from the ability to place computer-generated graphics in their field of vision.[167]

AR developers like *Layar*[168] have applied the technology to browsers that show what is in your environment by displaying real-time digital information on top of the real world as seen through the camera of your mobile phone. Layar works by using a combination of the mobile phone's camera, compass and GPS data to identify the user's location and field of view, retrieve data based on those geographical coordinates, and overlay that data over the camera view.[169] Data can be stored as wiki notes on the screen that, when activated on a mobile touch screen, opens to provide a multitude of information and intelligence. AR applications like this would be useful for military personnel in operations. As they walk or drive the ground, AR can give the user constant overlapped data on route directions, historical IED strike locations, and names of important features. Future new media capabilities like this can be projected on windshields or even inside protective eyewear.

---

[166] Haptics: a tactile feedback technology that takes advantage of a user's sense of touch by applying forces, vibrations, and/or motions to the user.

[167] "How Stuff Works: How Augmented Reality Will Work" http://www.howstuffworks.com/augmented-reality.htm; Internet; accessed 3 April 2010.

[168] http://layar.com

[169] "What is Layar – Augmented Reality Browser: Layar" http://layar.com/download/layar/; Internet; accessed 3 April 2010.

The soldier can also use new media as a human intelligence (HUMINT) source on the ground. Snapping photos and sending them back to the All-sources Intelligence Centre (ASIC), or scanning a local's fingerprints or other biometrics to be compared with a centralized database would provide information to the soldier on the ground whether to release or detain locals. The real-time collection of video, photos, or reports from within the battlespace will assist the commander to make better sound and timely decisions and shorten the speed of media releases with accurate and credible information.

There are many facets of new media that can be developed into better, more flexible technological tools that will provide more succinct information to the soldier and enable the intelligence and PA branches of the military to better influence the message. The application of new media technology in operations will assist the commander and their staff to achieve information dominance in the battlespace, and information engagement with target audiences.

CHAPTER SUMMARY

IO and new media do not diminish the role of the commander. However, they do necessitate significant changes in the nature of command to ensure the potential of IO and the digitization of the battlespace are fully exploited. At the same time, commanders must adapt to the significant changes that have occurred and that are still taking place in the strategic environment.[170]

[170] Garfield. "Information Operations as an Integrating Strategy…".

The commander has succinct challenges in the complete implementation of new media within a theatre of operations. Information Protection activities such as OPSEC and INFOSEC are challenged by the openness of new media and the ease of information to be promulgated through social networking means that can be collated and analyzed by the adversary to gather intelligence on operations, key leaders, and TTPs. New media also enables the adversary to threaten the confidentiality, integrity and accuracy of information and allows our own users to do the same.

New media is also pivotal in the Influence activities of IO. The media is the outlet for the message; the challenge for the CF is to deliver that message to the target audiences with timely, accurate, and relevant information. Enabling the soldiers in theatre to provide that message will close the timelines in getting the message out in the domain that the audience uses, and in a language that they understand. Shaping the conditions of acceptance and perceptions of society in the Information Age requires the message to be first to the post, accurate, and influential. Adopting new technologies like AR that evolve new media capabilities will also be a challenge but also a considerable benefit to the soldier in the provision of real-time information in the battlespace.

The reality is that IO is still far from a mature concept, and it comes at a cost as well as benefits. It is an integrating strategy that creates new vulnerabilities, as well as significant opportunities. The challenge to the CF is twofold: first, to develop a better understanding of the strategic context and real-world conditions influencing the employment of new media within the military environment; and second, to identify and

highlight the changes that our political, military and intelligence communities need to introduce in order to fully exploit the benefits of the new media environment of IO.

CHAPTER 6
CONCLUSION

This paper argues that new media and informationalism have a profound impact on CF operations and that the effects of new media on the battlespace must be considered within operational planning in order to ensure strategic success. It described the technological paradigm of the information society and supported the theory of informationalism as a catalyst for social evolution in the global adoption of new media. Informationalism has disposed the economic theory of the Information Age, empowering all levels of society through the increased access to information and providing a global voice to be heard. Understanding informationalism and the network society has established that we cannot ignore the human element of new media and the new media characteristics that are expected within today's society.

This research identified that the characteristics of new media are the framework for future communications in the CF. Characteristics like instantaneous connection and interactivity are important, not only to a soldier's personal communication's needs, but also to the structured, command and control networks of the army, navy, air force, and special forces. As the divide between our digital immigrants and digital natives narrows, the expectation of what is achievable on commercial networks – both from a technological and informational perspective - will be transferred over to the expectations of the military's private networks. The CF will benefit from the present capabilities of the pervasive and social new media in the public domain.

Chapter 4 demonstrated how new media is challenging the operational art of the staff officer and impacting the political, informational, and military elements of conflict. Commanders and their staffs need to fully comprehend, not only military, but the diplomatic, political, economic, financial, and social aspects of the situation in a given theater when they plan, prepare, and execute major campaigns or operations. New media does challenge the diplomatic, informational, and military lines of an operation or campaign.

The influence of diplomacy on a targeted society is more difficult because of new media's ability to enable people to access international informational sources. The military planner then, has to leverage new media in order to get the diplomatic message out to influence the population. The view of society on the social issues related to the theatre of war direct also impacts operations. This paper identified that new media has enabled the relevant social issues of a war to be disseminated worldwide and has stirred the emotions of the public and directly influencing the government's foreign policy.

On the military line of operation, new media has greatly improved the operational commander's common operating picture and situational appreciation for the battlespace. Military forces however, have to deal with the abundant volume of information available making the modern day planner more reliant on technology to complete operational art. They have to contend with the potential of information overload and will have to develop the skill of assessing the accuracy and relevancy of information.

The commander has succinct challenges in the complete implementation of new media

within a theatre of operations. This paper established that Information Protection activities and Influence activities of Information Operations are challenged by the openness of new media, the ease of information to be promulgated through social networking means, and the ability of the adversary to threaten the confidentiality, integrity and accuracy of information.

New media is the outlet for the message; the challenge for the CF is to deliver that message to the target audiences with timely, accurate, and relevant information. Adopting new media technologies that will evolve new media capabilities will also be a challenge but also a considerable benefit to the soldier in the provision of real-time information in the battlespace.

The "uncertainty and chance" of war is never fully avoided. Commanders and staff officers apply their operational art to the best of their abilities and training in hopes that their operational courses of action contain enough actionable knowledge so as to mitigate the risks of the plan to achieve success. New media is, and will be, a discernable source of information and knowledge for military operations. It has the potential to turn every soldier into a real-time digital sensor within the battlespace, empower social sub-groups that exist within the military to work collaboratively, and instantaneously influence perceptions both at home and in theatre. The CF has to develop an implementation plan to adopt new media and foster its development. This plan however, will result in the assumption of risks in its employ. Mitigating those risks will occur through more resilient education and training on the employment of new media, better discipline on the use of new media throughout the chain of command, and a higher sense of trust between the

digital immigrants and digital natives of the CF.

The CF is not seizing the full potential that new media and the digital natives have to offer. New media is a "centre of gravity" for the success in influencing the "hearts and minds" of Canadians and other audiences within operations. Organizational efforts have to be implemented in earnest to develop a better understanding of the strategic context and real-world conditions influencing the employment of new media in order to positively affect the desired endstates of military operations.

BIBLIOGRAPHY

ELECTRONIC SOURCES

"Army.ca Forums - Index." http://forums.army.ca/ ; Internet accessed 31 March 2010.

"ARPAnet - the First Internet." http://inventors.about.com/library/weekly/aa091598.htm; Internet; accessed 15 March 2010.

"Battfield of the Future." http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html; Internet; accessed 29 January 2010.

"Cyber Command Chief Outlines Future of Cyber Warfare." http://www.sheppard.af.mil/news/story_print.asp?id=123089373; Internet; accessed 25 January 2010.

"Cyber Warfare and Telecommunications Espionage." http://www.globalsecurity.org/wmd/library/news/cuba/oagmc029.htm; Internet; accessed 25 January 2010.

"Cyber Warfare Oracle Reveals Stark Vision." http://integrator.hanscom.af.mil/2007/October/10112007/10112007-19.htm; Internet; accessed 25 January 2010.

"Defining the Ages of Social Networking Users." http://www.impactlab.com/2010/02/27/defining-the-ages-of-social-networking-users/; Internet; accessed 12 March 2010.

"The Estate of Marshall McLuhan." http://www.marshallmcluhan.com/main.html; Internet; accessed 31 March 2010.

"The Evolution of Cyber Warfare." http://integrator.hanscom.af.mil/2008/February/02282008/02282008-19.htm; Internet; accessed 25 January 2010.

"Famous Quotes of Sir Francis Bacon." http://www.luminarium.org/sevenlit/bacon/quotes.php#txt12; Internet; accessed 16 March 2010.

"The History of Computers - Computer History Timeline." http://inventors.about.com/library/blcoindex.htm; Internet; accessed 12 March 2010.

"How Augmented Reality Will Work." http://www.howstuffworks.com/augmented-reality.htm; Internet; accessed 3 April 2010.

"Instantaneous - Definition and More from the Free Merriam-Webster Dictionary." http://www.merriam-webster.com/dictionary/instantaneous; Internet; accessed 16 March 2010.

"Pervade - Definition and More from the Free Merriam-Webster Dictionary." http://www.merriam-webster.com/dictionary/pervade; Internet; accessed 16 March 2010.

"Pervasiveness of Technology." http://www.nae.edu/nae/techlithome.nsf/weblinks/KGRG-55SPVK?OpenDocument; Internet; accessed 16 March 2010.

"Public Relations: Exploring New Media ... Shaping the Battle Space." *Naval Forces* 31, (2010, 2010): 52-53.

"The Story of Milblogging.com." http://www.milblogging.com/about.php; Internet; accessed 31 March 2010.

"STSC CrossTalk - Cyber Warfare: A New Doctrine and Taxonomy - Apr 2001." http://www.stsc.hill.af.mil/CrossTalk/2001/04/alford.html; Internet; accessed 25 January 2010.

"Taliban Threaten Afghan Mobile Phone Network." http://www.cellular-news.com/story/23665.php; Internet; accessed 9 February 2010.

"Ubiquitous - Definition and More from the Free Merriam-Webster Dictionary." http://www.merriam-webster.com/dictionary/ubiquitous; Internet; accessed 16 March 2010.

"What is RSS?" http://www.press-feed.com/howitworks/what-is-RSS.php; Internet; accessed 19 March 2010.

"World Internet Usage Statistics News and World Population Stats." http://www.internetworldstats.com/stats.htm; Internet; accessed 19 March 2010.

BBC News "Timeline: Soviet War in Afghanistan." http://news.bbc.co.uk/2/hi/south_asia/7883532.stm; Internet: accessed 18 March 2010.

CBC News. "National Anthem Won't Change: PMO." http://www.cbc.ca/canada/story/2010/03/05/national-anthem.html; Internet; accessed 22 March 2010.

———. "Third Attack on Cellphone Tower in Afghanistan." http://www.cbc.ca/world/story/2008/03/03/afghanistan-mobilephones.html; Internet; accessed 9 March 2010.

———. "Rape Law Hurting Efforts to Sell NATO Role in Afghanistan: NATO Chief." http://www.cbc.ca/world/story/2009/04/04/law-nato.html; Internet; accessed 17 April 2010.

Centre for Defense Information. "Afghanistan Update: May 2008." http://www.cdi.org/friendlyversion/printversion.cfm?documentID=4320; Internet; accessed 9 February 2010.

Chandler, Daniel. "Technological Determinism: Technology-Led Theories." http://www.aber.ac.uk/media/Documents/tecdet/tdet02.html; Internet; accessed 26 February 2010.

CNET News. "Taliban: Nix Nighttime Cell Phone Service." http://news.cnet.com/8301-13639_3-9881951-42.html; Internet; accessed 9 February 2010.

CNNMoney.com "Social Media use Increases 82% Worldwide." http://money.cnn.com/news/newsfeeds/articles/marketwire/0589146.htm; Internet; accessed 19 March 2010.

CNNMoney.com "Social Media use Increases 82% Worldwide: Nielsen Report Confirms Growing Power of Bloggerwave's Business Strategy." http://money.cnn.com/news/newsfeeds/articles/marketwire/0589146.htm; Internet; accessed 19 March 2010.

Dao, James. "Military Announces New Social Media Policy." NYTimes.com. http://atwar.blogs.nytimes.com/2010/02/26/military-announces-new-social-media-policy/; Internet; accessed 31 March 2010.

Facebook.com "Statistics."http://www.facebook.com/press/info.php?statistics; Internet; accessed 19 March 2010.

Gertz, Bill. "Cyber Command Delayed." *Washington Times,* sec. Inside the Ring.

International Telecommunications Union. "3G: All about the Technology." http://www.itu.int/osg/spu/ni/3G/technology/index.html#Cellular Standards for the Third Generation; Internet; accessed 13 April 2010.

Layar.com "What is Layar – Augmented Reality Browser: Layar." http://layar.com/download/layar/; Internet; accessed 3 April 2010.

M2 Press Wire. "Army Embraces Social Media at Conference." *Newspaper Source Plus*. http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=16PU1067486156&site=ehost-live; Internet; accessed 11 March 2010.

MSNBC.com "Cell-Phone use Booming in Afghanistan" http://www.msnbc.msn.com/id/20479899/ ; Internet; accessed 9 February 2010.

MSN.ca. "Cybercrooks and Hackers Prowling Vancouver Games; Experts Say to be on Guard." http://tech.ca.msn.com/canadianpress-article.aspx?cp-documentid=23507765; Internet; accessed 24 February 2010.

SAP. "The Pervasiveness of Technology Degrades Personal Responsibility." http://en.sap.info/the-pervasiveness-of-technology-degrades-personal-responsibility"/3525; Inernet; accessed 17 March 2010.

Sciutto, Jim, Bruno Roeber, and Nick Schifrin. "Afghanistan President Hamid Karzai Passes Controversial Law Limiting Women's Rights," *ABC News International.* http://abcnews.go.com/International/story?id=8327666&page=1; Internet; accessed 17 April 2010.

Shachtman, Noah. "Army Orders Bases to Stop Blocking Twitter, Facebook, Flickr." http://www.wired.com/dangerroom/2009/06/army-orders-bases-stop-blocking-twitter-facebook-flickr/ (accessed 3/11/2010, 2010).

Waldman, Amy. "A Nation Challenged: The Law; No TV, No Chess, No Kites: Taliban's Code, From A to Z." http://www.nytimes.com/2001/11/22/world/a-nation-challenged-the-law-no-tv-no-chess-no-kites-taliban-s-code-from-a-to-z.html; Internet; accessed 18 March 2010.

YaleGlobal Online Magazine." http://yaleglobal.yale.edu/en/node/6120; Internet; accessed 17 February 2010.

PUBLIC DOCUMENTS

Canada. Department of National Defence. B-GG-005-004/AF-010 *CF Information Operations*. Kingston: DND Canada, 1998.

———. B-GL-300-001/FP-001 *Land Operations*. Kingston: DND Canada, 2008.

———. B-GL-300-003/FP-001 *Command in Land Operations*. Kingston: DND Canada, 2007.

———. "The Maple Leaf." http://www.forces.gc.ca/site/commun/ml-fe/index-eng.asp; Internet; accessed 31 March 2010.

Canada. Canadian Radio-television and Telecommunications Commission. "Broadcasting Regulatory Policy CRTC 2009-329." http://www.crtc.gc.ca/eng/archive/2009/2009-329.htm; Internet: accessed 29 March 2010.

———. "Perspectives on Canadian Broadcasting in New Media." http://www.crtc.gc.ca/eng/media/rp080515.htm; Internet; accessed 17 March 2010.

Canada. Communications Security Establishment Canada. "CSEC: The Anti-Terrorism Act and CSEC's Evolution." http://www.cse-cst.gc.ca/home-accueil/nat-sec/ata-lat-eng.html; Internet; accessed 30 March 2010.

Canada. Department of Justice. "Backgrounder: Parliamentary Review of the Anti-Terrorism Act." http://www.justice.gc.ca/eng/news-nouv/nr-cp/2004/doc_31338.html; Internet; accessed 30 March 2010.

———. "Telecommunications Act." http://laws.justice.gc.ca/en/T-3.4/index.html; Internet; accessed 30 March 2010.

Canada. Government of Canada. *Anti-Terrorism Act - Bill C-36*, 18 December 2001.

———. "Speech from the Throne." http://www.speech.gc.ca/eng/media.asp?id=1388; Internet; accessed 22 March 2010.

Canada. Industry Canada - Spectrum Management and Telecommunications. "Regulating Content on the Internet: A New Technological Perspective." Sinclair, Gerri, Zilber, Julie and Hargrave, Eds. http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09030.html; Internet; accessed 29 March 2010.

Canada. Officer of the Privy Council. "Securing an Open Society: Canada's National Security Policy." http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=natsec-secnat/natsec-secnat-eng.htm#ch3; Internet; accessed 29 March 2010.

Canada. Statistics Canada. A Profile of the Canadian Forces. Abstract. *Perspectives*. http://statcan.gc.ca/pub/75-001-x/2008107/pdf/10657-eng.pdf ; Internet; accessed 21 March 2010.

United States. Central Intelligence Agency. "The World Factbook – Afghanistan." https://www.cia.gov/library/publications/the-world-factbook/geos/af.html; Internet; accessed 4 February 2010.

United States. Department of Defense. "Responsible and Effective use of Internet-Based Capabilities." Deputy Secretary of Defense, Pentagon. http://www.defense.gov/NEWS/DTM%2009-026.pdf; Internet; accessed 31 March 2010 .

United States. Office of the Director of National Intelligence. "Letter from Al-Zawahri to Al-Zarqawi July 9 2005." http://www.dni.gov/press_releases/letter_in_english.pdf; Internet; accessed 24 March 2010.

BOOK AND JOURNAL SOURCES

--. "Cyber Warfare: The Growing Threat." *Trends Magazine* no. 72 (04, 2009): 33-36. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=46791978&site=ehost-live; Internet; accessed 25 January 2010.

--. *Measuring the Information Society: 2010*. Geneva, Switzerland: International Telecommunication Union, 2010. http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_Summary_E.pdf; Internet; accessed 19 March 2010.

Aducci, Romina, Pim Bilderbeek, Holly Brown, Seana Dowling, Nora Freedman, John Gantz, Abner Germanow, Takashi Manabe, Alex Manfrediz, and Shalini Verma. *The Hyperconnected: Here they Come!*. Framingham, MA: IDC, 2008.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. *Understanding Information Age Warfare*. Washington, D.C.: CCRP, 2001.

Alberts, David S., John J. Garstka, and Frederick P. Stein, eds. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2nd ed. Washington, D.C.: CCRP, 1999.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age*. Washington, D.C.: CCRP Publications, 2003.

Andén-Papadopoulos, Kari. "US Soldiers Imaging the Iraq War on YouTube." *Popular Communication* 7, no. 1 (January 2009): 17-27. http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=35905526&site=ehost-live; Internet; accessed 19 March 2010.

Beaumont, Roger A. "A View from the Frontage Road: Musings on the Risks of Traveling the Information Highway." In *Cyberwar 2.0: Myths, Mysteries and Reality*, edited by Alan D. Campen and Douglas H. Dearth. Fairfax, Virginia: AFCEA International Press, 1998.

Bennett, Sue, Karl Maton, and Lisa Kervin. "The 'Digital Natives' Debate: A Critical Review of the Evidence." *British Journal of Educational Technology* 39, no. 5 (2008): 775-786. http://api.ning.com/files/AkclmKAQ9nT0vPJuCYL9261SknCvwP1UJ-RaVQ7kZumzWZVPq5iNlfGrqf0Jpc3wUnK8A07FuVmRXQ1WRqnre5q2z53PRnT0/Thedigitalnativesdebatecriticalreview.pdf; Internet; accessed 22 March 2010.

Block, Melissa. "New U.S. Cyber Command Raises Privacy Concerns." *All Things Considered (NPR)* http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=6XN200906262007&site=ehost-live; Internet; accessed 25 January 2010.

Bonabeau, Eric. "When Intuition is Not enough: Strategy in the Age of Volatility." *Perspectives on Business Innovation* no. 9 (2009): 41. www.leader-values.com/Downloads/CBI/Journal_Issue_9.pdf; Internet; accessed 17 February 2010.

Bonabeau, Eric. "Don't Trust Your Gut." *Harvard Business Review* 81, no. 5 (05, 2003): 116-123. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9721855&site=ehost-live; Internet; accessed 15 February 2010.

Bousquet, Antoine. "Chaoplexic Warfare Or the Future of Military Organization." *International Affairs* 84, no. 5 (09, 2008): 915-929. http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=34611879&site=ehost-live; Internet; accessed 6 January 2010.

Bryant, David J. "Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making." *Military Psychology* 18, no. 3 (07, 2006): 183-206.

http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=23121993&site=ehost-live; Internet; accessed 11 January 2010.

Caldwell, IV, W., Dennis M. Murphy, and Anton Menning. "Learning to Leverage New Media." *Military Review* 89, no. 3 (May, 2009): 2-10. http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=43247723&site=ehost-live; Internet; accessed 17 March 2010.

Caldwell, IV, W., Lcol Shawn Stroud, and Anton Menning. "Fostering a Culture of Engagement." *Military Review* (September, 2009). http://www.trackpads.com/magazine/190.html; Internet; accessed 17 March 2010.

Carper, Thomas R. "Federal Cyber Defense." *FDCH Congressional Testimony* (October 2009). http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=32Y2370953251&site=ehost-live; Internet; accessed 25 January 2010.

Castells, Manuel. "Epilogue: Informationalism and the Network Society." In *The Hacker Ethic and the Spirit of the Information Age*, edited by Pekka Himanen, 155-178. New York: Random House, 2001.

———. . *Informationalism, Networks, and the Network Society: A Theoretical Blueprint*. The Network Society: A Cross-Cultural Perspective. Northampton, MA: Edward Elgar, 2004.

Collings, Deirdre and Rafal Rohozinski. *Bullets and Blogs: New Media and the Warfighter*. Carlisle barracks, Pennsylvania: Center for Strategic Leadership, US Army War College, 2008.

Dartnell, Michael. "Web Activism as an Element of Global Security." In *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni, 61-78. New York, NY: Routledge, 2009.

Dearth, Douglas H. "The Human Factor in Future Conflict: Continuity and Change." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 7-17. Fairfax, VA: AFCEA International Press, 2000.

———. "Introduction and Overview." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000.

———. "Operationalizing Information Operations: C2W…RIP." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000.

Deibert, Ronald J., and Rafal Rohozinski. "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet." Deibert, Palfrey, Rohozinski, Zittrain, (eds.), *Access Denied* (MIT Press: 2007).

Douglis, Fred. "On Social Networking and Communication Paradigms," *IEEE Internet Computing*, 12, no. 1, pp. 4-6, Jan./Feb. 2008, http://doi.ieeecomputersociety.org/10.1109/MIC.2008.17; Internet; accessed 18 April 2010.

Echevarria II,Antulio J. "Globalization and the Clausewitzian Nature of War." *European Legacy* 8, no. 3 (0601): 317-332.

Fulghum, David A. and Douglas Barrie. "Stealthy and Subtle." *Aviation Week & Space Technology* 171, no. 17 (9 November 2009): 76-78. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=45604601&site=ehost-live; Internet; accessed 25 January 2010.

Fulghum, David A. and Graham Warwick. "Cyberstruck." *Aviation Week & Space Technology* 170, no. 17 (27 April 2009): 20-21. http://search.ebscohost.com/login.aspx?direct=true&db=axh&AN=BAST09129376&site=ehost-live; Internet; accessed 25 January 2010.

Gardner, Hall. "War and the Media Paradox." In *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni. New York, NY: Routledge, 2009.

Garfield, Andrew. "Information Operations as an Integrating Strategy: The Ongoing Debate." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000.

Gorman, Siobhan. "FBI Suspects Terrorists are Exploring Cyber Attacks." *Wall Street Journal - Eastern Edition* 254, no. 119 (18 November 2009): A4. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=45591446&site=ehost-live; Internet; accessed 25 January 2010.

Gray, Colin S. "How has War Changed since the End of the Cold War?" *Parameters: US Army War College* 35, no. 1 (Spring 2005): 14-26. http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=16345898&site=ehost-live; Internet; accessed 6 January 2010.

Hoskins, Andrew and Ben O'Loughlin. "The Internet as a Weapon of War? Radicalisation, Publics and Legitimacy." In *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni, 31-47. New York, NY: Routledge, 2009.

Kahneman, Daniel and Gary Klein. "Conditions for Intuitive Expertise: A Failure to Disagree." *American Psychologist* 64, no. 6 (09, 2009): 515-526. http://search.ebscohost.com/login.aspx?direct=true&db=pdh&AN=amp-64-6-515&site=ehost-live; Internet; accessed 15 February 2010.

Karatzogianni, Athina, ed. *Cyber Conflict and Global Politics*. New York, NY: Routledge, 2009.

Keggler, Johnny and Tim Mahon. "Preparing for Cybergeddon." *Armada International* 33, no. 2 (04, 2009): 34-36.

http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=37707141&site=ehost-live; Internet; accessed 25 January 2010.

Kimbrell, Nicholas. *Israelis Bring Down Hizbullah Website - Report*: Daily Star, The (11/2008 to 4/2009), 2009. http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=2W62W62254149483&site=ehost-live; Internet; accessed 25 January 2010.

Klein, Gary and Karl E. Weick. "Decisions." *Across the Board* 37, no. 6 (06, 2000): 16. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=3224038&site=ehost-live; Internet; accessed 15 February 2010.

Lefebvre, Stephane, Michel Fortmann, and Thierry Gongora, eds. *"The Revolution in Military Affairs": Its Implications for Doctrine and Force Development within the U.S. Army*. The Operational Art: Developments in the Theories of War, edited by B. J. C. McKercher andMichael A. Hennessy. Westport, CT: Praeger Publishers, 1996.

Lynn, John. "The Evolution of Army Style in the Modern West, 800 - 2000." *The International History Review* xviii, no. no. 3 (August 1996, 1996): 505-545.

MacIntosh, J. P. and Mils Hills. "The Psychology of Future War: Asymmetric Risk and Decision-Taking." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 49-76. Fairfax, VA: AFCEA International Press, 2000.

Mackay, Hugh. *Investigating the Information Society*. New York: Routledge, 2001.

Manovich, Lev. "Introduction: New Media from Borges to HTML." In *The New Media Reader*, edited by Noah Wardrip-Fruin and Nick Monfort. Cambridge, MA: MIT Press, 2003. http://www.manovich.net/DOCS/manovich_new_media.doc; Internet; accessed 3 April 2010.

———. *The Language of New Media*. Cambridge, M.A.: The MIT Press, 2001.

Marcy, Scott A. "Operational Art: Getting Started," *Military Review* 9 (September 1990); 107.

Mattox, John Mark. "The Clausewitzian Trinity in the Information Age: A just War Approach." *Journal of Military Ethics* 7, no. 3 (November 2008): 202-214. http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=34011173&site=ehost-live; Internet; accessed 11 January 2010.

McCormick, Michael. "The New FM 100-5: A Return to Operational Art." *Military Review* 77, no. 5 (September 1997): 3. http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=224830&site=ehost-live; Internet; accessed 6 January 2010.

McKercher, B. J. C. and Michael A. Hennessy, eds. *The Operational Art: Developments in the Theories of War*. Westport, CT: Praeger Publishers, 1996.

McLuhan, Herbert Marshall. *Understanding Media: The Extensions of Man*. New York: McGraw-Hill, 1964.

McNamara, Michael R. "Dysfunction in Cyberspace: The Insider Threat." In *Cyberwar 3.0: Human Factors in Information Operations and Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 1-17. Fairfax, VA: AFCEA International Press, 2000.

Metz, Steven. "The Next Twist of the RMA." *Parameters: US Army War College* 30, no. 3 (September 2000): 40. http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=3552880&site=ehost-live; Internet; accessed 29 January 2010.

Mitchell, Paul T. . *Network Centric Warfare and Coalition Operations: The New Military Operating System*. New York, NY: Routledge, 2009.

Morozov, Evgeny. "The Fog of Cyberwar." *Newsweek (Atlantic Edition)* 153, no. 17 (27 April 2009): 50-51. http://search.ebscohost.com/login.aspx?direct=true&db=heh&AN=39344395&site=ehost-live; Internet; accessed 25 January 2010.

Nel, D. F. and Kroeze, J. H. "Information Technology as an Agent of Post-Modernism." http://cogprints.org/6207/ ; Internet; accessed 11 March 2010.

Oblinger, Diana G. and James L. Oblinger. "Is it Age Or IT: First Steps Towards Understanding the Net Generation." In *Educating the Net Generation*, edited by Diana G. Oblinger and James L. Oblinger, 2.0-2.20: EDUCAUSE, 2005. www.educause.edu/educatingthenetgen/; Internet; accessed 22 March 2010.

Paret, Peter, Gordon A. Craig, and Felix Gilbert, eds. *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*. Princeton, NJ: Princeton University Press, 1986.

Post, Jerrold M. *The Mind of the Terrorist: The Psychology of Terrorism from the IRA to Al-Qaeda*. New York: Palgrave MacMillan, 2007.

Prensky, Marc. "Digital Natives, Digital Immigrants." *On the Horizon* 9, no. 5 (October 2001). http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf; Internet; accessed 22 March 2010.

———. "Digital Natives, Digital Immigrants Part II: Do they really *Think* Differently?" *On the Horizon* 9, no. 6 (December 2001). http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part2.pdf; Internet; accessed 22 March 2010.

Rheingold, Harold. *Smart Mobs: The Next Social Revolution*. Cambridge, MA: Basic Books, 2002.

Robbin, Alice and Wayne Buente. "Internet Information and Communication Behavior during a Political Moment: The Iraq War, March 2003." *Journal of the American Society for Information Science & Technology* 59, no. 14 (December 2008): 2210-2231. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=35485690&site=ehost-live; Internet; accessed 19 March 2010.

Rogan, Hanna. "Abu Reuter and the E-Jihad: Virtual Battlefronts from Iraq to the Horn of Africa." *Georgetown Journal of International Affairs* 8, no. 2 (August 2007): 89-96. http://search.ebscohost.com/login.aspx?direct=true&db=poh&AN=33185673&site=ehost-live; Internet; accessed 19 March 2010.

Rosenbloom, Andrew. "The Blogosphere." *Communications of the ACM* 47, no. 12 (December 2004): 31-62. http://search.ebscohost.com/login.aspx?direct=true&db=axh&AN=BAST04167361&site=ehost-live; Internet; accessed 11 February 2010.

Schaap, Arie J. "Cyber Warfare Operations: Development and use Under International Law." *Air Force Law Review* 64, (June 2009): 121-173. http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=45162334&site=ehost-live; Internet; accessed 25 January 2010.

Sheridan, Greg. "Cyber Warfare a Real-Time Threat." *Australian, the* (04/03, 2009): 2-2. http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=200904031002872112&site=ehost-live; Internet; accessed 25 January 2010.

Showalter, Denis. "Prussia, Technology, and War: Artillery from 1815 to 1914." In *Men, Machines and War*, edited by Keith Neilson and Ronald Haycock, 113-151. Waterloo, ON: Sir Wilfred Laurier University, 1988.

Siegel, Pascale Combelles. "Perception Management: IO's Stepchild." in *Information Warfare: Separating Hype from Reality*, edited by E. Leigh Armistead, Washington, DC: Potomac Books, 2007.

Stevenson, Nick. *Understanding Media Cultures*. 2nd ed. London: Sage Publications, 2002.

Stone, John. "Politics, Technology and the Revolution in Military Affairs." *Journal of Strategic Studies* 27, no. 3 (September 2004): 408-427. http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=14794788&site=ehost-live; Internet; accessed 11 January 2010.

Terry, James P. "The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What are the Targeting Constraints?" *Military Law Review* 169, (September 2001): 71 - 99. http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/277085~1.pdf; Internet; accessed 29 March 2010.

Touri, Maria. "Transparency and Accountability in the Age of Cyberpolitics." In *Cyber Conflict and Global Politics*, edited by Athina Karatzogianni, 48-58. New York, NY: Routledge, 2009.

Vego, Milan. *Joint Operational Warfare*. Newport, RI: U.S. Naval War College, 2007.

Vlahos, Michael. "The Emergence of the Infosphere and its Impact on Military Operations." In *Cyberwar 2.0: Myths, Mysteries and Reality*, edited by Alan D. Campen and Douglas H. Dearth. Fairfax, Virginia: AFCEA International Press, 1998.

von Lubitz, Dag,K.J.E., James E. Beakley, and Frédéric Patricelli. "'All Hazards Approach' to Disaster Management: The Role of Information and Knowledge Management, Boyd's OODA Loop, and Network-Centricity." *Disasters* 32, no. 4 (December 2008): 561-585. http://search.ebscohost.com/login.aspx?direct=true&db=cmedm&AN=18479475&site=ehost-live; Internet; accessed 11 January 2010.

Waltz, Edward. *Information Warfare: Principles and Operations*. Norwood, MA: Artech House, Inc., 1998.

Weimann, Gabriel. *Terror on the Internet*. Washington, D.C.: United States Institute of Peace, 2006.

Wood, Jason. "Survival of the Fittest: The Evolution of U.S. Military Command and Control Structures during and After the Cold War." *Comparative Strategy* 25, no. 2 (04, 2006): 121-131. http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=21193545&site=ehost-live; Internet; accessed 6 January 2010.

Wortzel, Larry M. "Cybersecurity." *FDCH Congressional Testimony* http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=32Y1080199602&site=ehost-live; Internet; accessed 25 January 2010.