National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SMARTPHONE IMPLEMENTATION WITHIN THE DND/CF

Lieutenant-Colonel T.R. Malo

JCSP 38

Master of Defence Studies

Disclaimer

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

PCEMI 38

Maîtrise en études de la défense

Avertissement

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

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES
JCSP 38 - PCEMI 38

MASTER OF DEFENCE STUDIES RESEARCH PAPER

SMARTPHONE IMPLEMENTATION WITHIN THE DND/CF

By/par LCol T. R. Malo

TABLE OF CONTENTS

ABSTRACT

This dissertation examines the case of immediately introducing smartphone technologies within the Canadian Forces. It will be argued that the introduction of information technology has created an information age society where the sharing of information is the predominant form of power within a society. The CF's embrace of smartphone technologies will be the embodiment of recognizing this form of power in a military context and enable the CF to implement "power to the edge" concepts for the front-line soldier. With this background understanding of the rationale to explore these technologies further, this paper provides an overview of the United States Army efforts to deploy smartphone technologies to their front-line soldiers. Through the analysis of this case study, it will be argued that they are implementing the tenets of "power to the edge" through the use of new media tools and technologies. This paper will also provide an overview of OPSEC and IP within a CF context, focusing on those issues that are relevant to smartphones and the mitigation measures that are available to overcome these issues. Through the analysis of these concerns and mitigation strategies, it will be demonstrated that the benefits associated with smartphone technologies far outweigh the risks, especially if proper technologies and procedures are incorporated with their implementation. Empowering all levels of the military chain of command right down to the individual soldier has the potential to improve both the efficiency and efficacy of military operations. Implementing smartphone technologies fosters this empowerment and should be aggressively pursued within a CF context.

CHAPTER 1

INTRODUCTION

> As we prepare for the future, we must think differently and develop the kinds of forces and capabilities that can adapt quickly to new challenges and to unexpected circumstances. We must transform not only the capabilities at our disposal, but also the way we think, the way we train, the way we execute, and the way we fight.
>
> - Donald Rumsfeld[1]

Imagine if you will a new recruit to the Canadian Forces (CF) who has just arrived at the training centre in St. Jean, Quebec. He is issued with all of his military equipment to commence his training. Included with his essential equipment and clothing is the latest model smartphone. One of the first series of lectures he receives instructs him on its use, the capabilities that it possesses and the rules that he must follow to allow him to maximize its potential while at the same time following various rules regarding security and appropriate use within a military context. As a youth within Canadian society, he is well versed in its operations and embraces its capabilities as second nature.

This young recruit immediately commences using this smartphone to maximize his training efficacy. He constantly sends and receives emails from his instructors regarding directions for the various lessons that he is responsible to understand. While studying the material he has been provided in class, he calls up textbooks and manuals online through the integrated browser within the smartphone to obtain a better understanding of the technical topic he has been struggling with for some time. He uses instant messaging functionality embedded within the smartphone to contact his fellow recruits to share ideas about a difficult topic and

---

[1]United States. Department of Defense, *Transformation Planning Guidance* (Washington, DC: Department of Defense,[2003]), 1.

arrange meetings to discuss the topic in person. While struggling with a particularly difficult assignment, he uses whiteboard collaboration tools to work through the document with other members of his class so that they can provide a premium product by the deadline imposed by the instructor. Finally, he can call the training centre's administrative cell to verify his travel arrangements for his trip to Gagetown where he will commence his next phase of training as an infantry soldier.[2]

Now imagine if you will this same soldier, upon completion of all the phases of his training, being sent into an operational theatre of combat such as Afghanistan. While conducting a standard foot patrol in the heart of southern Afghanistan, he calls up navigational maps on his smartphone and uses its integrated Global Positioning System (GPS) capabilities to pinpoint his exact location and plan out his route for the day. During the course of his patrol, he observes someone who he believes may be a high value target that should be detained and returned to base for questioning. Unsure of the target's identity, he captures a picture with the embedded camera and sends it off to the intelligence cell tasked to support him and his peers to confirm the identity of the target in question. Upon receiving confirmation, he confirms the security of the immediate environment by calling up a live video stream of the surrounding area from an Unmanned Arial Vehicle (UAV) that has been tasked to provide this information. Satisfied with the security situation, he proceeds to detain the potential high value target. Concerned about the effort to return this individual to base, he wishes to reconfirm that this is indeed the individual in questions. Thus, he takes a retinal scan and finger print of the individual which he then sends back once again to the intelligence section to receive a second more thorough confirmation of the

---

[2]Chondra Perry, "Army to Test Smartphones for Offices, Battlefields," *US Army* (27 May 2010). http://www.army.mil/article/39953/; Internet; accessed 29 January 2012.

target. Convinced of the individual's identity, he proceeds to return to base to allow for an interrogation of the target by specialists located at the base.[3]

Now this same soldier is located on base with some time off before his next scheduled patrol. He has been fully trained on the use of his smartphone and understands what the Rules of Engagement (ROE) are regarding what information he can share in the public domain. Wishing to stay connected to his family and friends at home, he uses his smartphone to update his Facebook page with pictures of him and his friends in front of the Tim Horton's on base. He reassures his family through Twitter that he is enjoying his time in Afghanistan and that he is truly making a positive difference in the lives of those he touches. While catching up on the news back home in Canada, he reads a blog by a reporter in his home town which inaccurately portrays CF activities in Afghanistan, placing the CF in a negative light and encourages comments and feedback from local citizens. Having been fully briefed on what he can or cannot say in the public domain; this soldier takes the initiative to provide factual information. While not providing his own personal opinion on the topic, these facts refute this reporter's story and set the CF in a positive light in his home town.[4]

In all three examples provided above, the common denominator is the smartphone that has been issued to the soldier. What makes these examples particularly compelling is the fact that the technology to support these scenarios exist today. This is truly not science fiction anymore. Unfortunately, the CF is not poised at this time to take advantage of smartphones and the associated functionality that they provide.

---

[3]Chuong Nguyen, "Army Begins Testing Smartphone for use in Combat," *GottaBe Mobile: Mobile* (3 June 2011). http://www.gottabemobile.com/2011/06/03/army-begins-testing-smartphone-for-use-in-combat/; Internet; accessed 29 January 2012.

[4]Kathy Shaidle, "Wikileaks' 'Iraq: Collateral Murder' Video 'Doesn't Show the Broader Picture'," *Examiner.com: Politics* (12 April 2010). http://www.examiner.com/conservative-politics-in-national/wikileaks-iraq-collateral-murder-video-doesn-t-show-the-broader-picture; Internet; accessed 29 January 2012.

This paper argues that it is time for the CF to incorporate smartphones and associated technologies in both the administrative and operational spheres to empower members in the conduct of their day-to-day activities. The information society in which we find ourselves has fostered a culture that demands the sharing of information to the lowest possible level. Further, the introduction of new media has both enabled and encouraged this sharing of information. The trials of the United States Army to incorporate these devices and capabilities will be examined to demonstrate the feasibility of doing so. This case study will not only demonstrate that it is technically possible but that the benefits that were alluded to above are indeed available to today's soldier. However, these technologies do not come without risk. These empowering technologies must be implemented in such a fashion as to ensure the integrity of the information being shared while protecting it from adversarial manipulation. Furthermore, with appropriate training and direction regarding what information can be shared with these devices, today's frontline soldier can be empowered to act through the tactical, operational and strategic spheres of war. Indeed, society has arrived at a point in time where we have the possibility of what has been called by some, the "strategic private".[5]

To provide a succinct argument regarding the implementation of smartphones within the CF, this paper is broken down in the following manner. Chapter 2 will introduce the theoretical underpinnings to the concept of the information society in which we are currently living, through to the technological implementation of that societal vision. The first section will discuss the transition from the agricultural society through the industrial society to the current information

---

[5]David Schmidtchen, *The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military* (Australia: Longueville Media, 2006), viii.

society and the concept of informationalism as identified by Manuel Castells will be explored to highlight the emergence of the "network society" in today's information age.[6]

From this theoretical understanding, the second section will introduce the "canon" of information age literature produced by the United States defence community, which attempt to embrace the significance of the network society within a defence framework. From *Network Centric Warfare*[7] through *Understanding Information Age Warfare*[8] and finally *Power to the Edge*[9], the United States defence establishment is encouraging the sharing of information to the lowest possible levels so that a complete shared situational awareness is created. This empowers self-synchronization and maximizes the efficiency and efficacy of military organizations.

The third section will define new media and highlight the benefits associated with embracing new media and the devices that facilitate this new medium.[10] It will be demonstrated that it is the utilization of new media that allows for the wealth of information transfer that facilitates the vision identified by the United States defence community for shared situational awareness which can only be accomplished by embracing the tenets of the network society.

Chapter 3 will also provide an overview of the United States Army efforts to deploy smartphone technologies to their soldiers. First, the failed attempts at developing unique military solutions will be explored (Joint Tactical Radio System, Nett Warrior and Sentinel), as well as

---

[6]Manuel Castells, ed., *The Network Society: A Cross Cultural Perspective* (Edward Elgar Publisher, 2005), 464.

[7]David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. (Washington, D.C.: Library of Congress, 2000), 284.

[8]David S. Alberts, John J. Garstka, Richard E. Hayes and David A. Signori, *Understanding Information Age Warfare* (Washington, D.C.: Library of Congress, 2001), 312.

[9]David S. Alberts and Richard E. Hayes, *Power to the Edge: Command, Control in the Information Age* (Washington, D.C.: Library of Congress, 2005), 259.

[10]Lev Manovich, *The Language of New Media*, eds. Noah Wardrip-Fruin and Nick Montfort (MIT Press, 2003), 307.

more recent efforts to use Commercial Off The Shelf (COTS) equipment and technologies. The smartphone trail case study will identify the administrative and operational areas in which they are concentrating their efforts. They are testing both iPhone and Android based devices and along with implementing the new media technologies and devices that empower this functionality, they are working hard to create a strictly controlled access "Apps Store" that will provided various tools of benefit to the common soldier. Examples of the various apps that have already been developed will be provided to provide insight into the potential that these apps have to empower today's modern day warfighter.

Through the analysis of this case study, it will be shown that these efforts are linked to the ideas of network society and power to the edge that was introduced in Chapter 2. It is through the integration of these new technologies that the United States is providing the level of situational awareness necessary to support their efforts to develop the power to the edge concept.

The idea of Canada capitalizing on the United States efforts will be explored next, in terms of both the administrative and operational spheres that Canadian soldiers operate in. The idea of a phased approach to the implementation of these technologies will be explored, first in the administrative sphere to work out both the technical and procedural issues related to the introduction of these new technologies. The lessons learned can then be transported to the operational sphere where concerns about confidentiality, integrity and availability are higher than in the administrative sphere. This will allow the CF time to address the security concerns that would be of greater significance within the operational sphere.

Chapter 4 will introduce the concepts of Information Protection (IP) and Operational Security (OPSEC) that form the two major concerns limiting the implementation of smartphones

in today's militaries.[11] Detail regarding the various security and privacy concerns that have emerged with the introduction of smartphone technologies in the general public will be discussed. Concerns with viruses, hacking, GPS tracking and other privacy problems will be explored as they have an effect on the military implementation of these same technologies.[12] Furthermore, a review of the use of smartphone technologies in the 2006 Israeli-Hezbollah War in Lebanon will be provided to highlight the effects, both positive and negative, that were encountered through the use of these technologies in that conflict.[13]

These concerns will be mapped against the IP and OPSEC concepts introduced earlier in the chapter to provide insight into the reluctance of the Department of National Defence / Canadian Forces (DND/CF) to embrace smartphone technologies and why its current implementation of Blackberries limits possible functionality. This limited Blackberry functionality will be compared against the Royal Canadian Mounted Police (RCMP) Blackberry implementation whereby they have opened up their Instant Messaging (IM) capabilities to improve the effectiveness of the devices. This comparison to a paramilitary Canadian organization with similar security concerns will highlight the possibility of the DND/CF exploring similar or improved functionality, learning from a like-minded national organization.

Emerging encryption standards and capabilities that can be incorporated within smartphone devices will be introduced to demonstrate that these security concerns can be

---

[11]Canada. Department of National Defence, *B-GG-005-004/AF-010 CF Information Operations*, 1998.

[12]Colin Clark. "Smartphones: The Next Security Gap ," *DoD Buzz* (23 February 2011). http://www.dodbuzz.com/2011/02/23/smartphones-the-next-security-gap/#ixzz1Eq4lTrVI; Internet; accessed 29 January 2012.

[13]Deirdre Collings and Rafal Rohozinski, *Bullets and Blogs: New Media and the Warfighter* (Pennsylvania: US Army War College,[2008]), 73-97.

addressed through the appropriate implementation of technology and procedures.[14] The chapter will then discuss the requirement to provide proper training and ROEs to users so that they know how to manage the information they manipulate appropriately while complying with IP/OPSEC concerns. Finally, the chapter will argue in summation that although these IP/OPSEC challenges exist and are significant, they are not insurmountable and can be addressed through both technology and training. The phased introduced of smartphones first in the administrative and then in the operational sphere will be highlighted once again as the best method of implementing this powerful functionality to the warfighter.

Chapter 5 will summarize the previous four chapters by restating the tenets of the network society, power to the edge envisioned in the military establishment and new media which facilitates the implementation of this vision. The United States efforts to implement smartphones and associated technologies will be summarized to demonstrate that Canadians can leverage this effort in their own implementation of the same. A review of the IP/OPSEC challenges that were introduced previously will be provided. This review will demonstrate that they can be overcome in a Canadian application through a systematic, phased implementation of the devices and technologies first in the administrative domain followed by the operational domain. The benefits associated with smartphone technologies far outweigh the risks, especially if proper technologies and procedures are incorporated with their implementation.

---

[14]John Keller. "Military Crypto Modernization Leads to Applications Like Smartphones, Tablet Computers on the Battlefield," *Military and aerospace electronics* (28 November 2011). http://www.militaryaerospace.com/articles/2011/11/military-crypto-modernization.html; Internet; accessed 29 January 2012.

CHAPTER 2

THE INFORMATION SOCIETY

The explosion of information age technologies has given rise to new theories as to how these technologies have influenced society and how these changes in society affect the political, economic, social and military domains. To comprehensively examine why the CF should incorporate smartphones and associated technologies in its working environment, it is necessary to first understand the theories of how information technology has influenced society. Thus, the theoretical underpinnings to the concepts of the information age that we are currently living through to the technological implementation of that societal vision will be introduced. This chapter will argue that the introduction of information technology has created an "information age society" where the sharing of information is the predominant form of power within a society. The CF's embrace of smartphone technologies will be the embodiment of recognizing this form of power in a military context and enable the CF to implement "power to the edge" concepts for the front-line soldier.

This chapter will start by discussing the transition from the hunter-gather age through the agrarian age, industrial age to the now existing information age. The information society will be described in further detail and the concepts of both informationalism and the network society espoused by Manuel Castells will be presented. This theoretical understanding will support the discussion of "power to the edge" advocated by the US military defence establishment. "Power to the edge" is a military implementation of the tenets of the network society established through the works of Alberts, *et al*. This encouragement of a complete shared situational awareness, it is argued, empowers self-synchronization and maximizes military effectiveness on the battlefield. Finally, the technological implementation of the visions of network society and power to the

edge will be detailed by exploring the affordances new media offers and the benefits they entail. By the end of the chapter, it will be demonstrated that it is only by embracing new media that militaries such as the CF can realize the benefits of power to the edge. This will provide the theoretical support for advancing efforts to incorporate smartphone technologies within the CF.

THE NETWORK SOCIETY

Human evolution can be broken down into various stages of existence where a predominant way of life sets the stage for how people interacted and society develops. Robert O'Connell has reviewed the societies of man in relation to the conduct of war and breaks down human history into the societies of hunter-gather, agrarian (or as he labels it, the plant trap), industrial and then information. At the dawn of human history, "humans evolved as hunter-gatherers, living for 99 percent of our line's history in pack-sized bands dictated by the availability of food sources and genetic affinity."[15] These societies tended to be relatively mobile due to their reliance on the natural environment and need to follow the migration patterns of wild herds. Individual societies were relatively small and communications between groups was limited.

With the introduction of agriculture or the agricultural revolution, an agrarian society developed which depended on agriculture as the primary means of providing sustenance. "Before we knew it, we had become farmers, our ancient mobility compromised and our population swelled to the point there was no going back to hunting and gathering."[16] Development of agricultural techniques allowed groups to create permanent settlements and the guaranteed provision of food allowed societal groups to grow. "Social development...was

---

[15]Robert J. O'Connell, *Ride of the Second Horseman: The Birth and Death of War* (New York: Oxford University Press, 1995), 226.

[16]Ibid., 227.

intensified and accelerated...fostering the erection of governmental structures, differential access to resources, and the coercive organization of labor."[17] These governmental structures and organization of labor required the management and exchange of information at a much larger scale than seen previously in the hunter-gatherer age. Thus, communication between societal groups was encouraged.

The continued population growth created by agriculture necessitated new technology and ultimately mass production to support it.

> The resulting labor pool, the application of new financial methods, and the very rapid evolution of machine technology combine to set off the Industrial Revolution – first in northern Europe and then in an ever-expanding zone around the globe…Although elemental shifts in economic roles and functions were the basis of the transformation, it was the manner in which change cascaded into matters of health, reproduction, and politics that truly metamorphosed the way people lived…Most fundamental has been the stabilization of demographic patterns in industrial societies.[18]

With the advent of the industrial revolution, an industrial society formed and was characterized by the use of non-animal external sources of energy like fossil fuels to increase the rate and scale of production. This growth in production sponsored large commercial industries which required the support of increased and improved communications. Mass production and the organizations supporting mass production became predominant within this society.

The proliferation of information sharing, itself, grew with the scale of industrial development. Daniel Bell first espoused the idea of a post-industrial society wherein the majority of the population is employed in the provision of services and not in the production of tangible goods.[19]

---

[17]Ibid., 228.

[18]Ibid., 231.

> A post-industrial society is based on services …What counts is not raw muscle power, or energy, but information…If an industrial society is defined by the quantity of goods as marking a standard of living, the post-industrial society is defined by the quality of life as measured by services and amenities – health, education, recreation, and the arts – which are now deemed desirable and possible for everyone.[20]

As Daniel Bell points out, the use of information to foster the provision of services is key to improving human quality of life in the post-industrial society.

The term information society has been coined to express this transformation from the industrial society to today's society which is dependent on information. Frank Webster's review of the theories of the information society points out that "information is at the core of how we conduct ourselves these days."[21] Jaya Deu Murthy's thorough review of the evolution of the Internet summarizes the information society concept as follows:

> The term 'information society' has been widely used to characterize the changing way of life – technological, economic, occupational, spatial, and cultural – in contemporary society. Information in all perspectives has been labelled as the defining feature of this new information society. The ability to retrieve vast stores of information easily has been accepted to greatly affect one's activities, way of life and society, ultimately differentiating this society from its predecessors. New information and communication technologies are acknowledged as making information available to all people and altering the fundamental nature of society.[22]

The creation, use, distribution and manipulation of information have become the significant economic, political and cultural driving force and are the distinguishing feature of the information society.

---

[19]Daniel Bell, *The Coming of Post-Industiral Society: A Venture in Social Forecasting* (New York: Basic Books, 1976), 348.

[20]Ibid., 127.

[21]Frank Webster, *Theories of the Information Society*, Third ed. (New York: Routledge, 2006), 9.

[22]Jaya Deu Murthy, "Evolution of the Internet and its Impact on Society" (M.A., McGill University (Canada)), http://search.proquest.com/docview/304772727?accountid=9867, 94.

With this view of the importance of information, Manuel Castells, a leading sociologist studying the impact of information on society, introduces the concept of "informationalism" which is the technological paradigm that underlies the social change that is taking place. Informationalism is a combination of three features:

- First is the doubling of processing power every 18 months; otherwise known as "Moore's Law". This increasing processing power has a follow-on effect of halving the cost of processing power every 18 months.
- Second is the nature of digital information where it can be easily manipulated, modified and retooled for different uses.
- Third is the growth and spread of networks which distribute the information generated from the first two features.

Thus, informationalism supports the development of more information which builds upon itself in a continuous process.[23]

Castell further refines the cumulative feedback loop of information building within informationalism by stating that:

> "what characterizes the current technological revolution is not the centrality of knowledge and information, but the application of such knowledge and information to knowledge generation and information processing/communication devices, in a cumulative feedback loop between innovation and the uses of innovation."[24]

Informationalism thus supports the cumulative feedback loop between the generation of new knowledge and information through the manipulation of existing knowledge and information. The cumulative feedback loop of innovation that informationalism supports is reliant on

---

[23]Paul T. Mitchell, "Digital Anarchy: The Challenge Posed by Information to the Military" (Unpublished Paper, Canadian Forces College, Toronto, 2012), 2-3.

[24]Castells, *The Network Society: A Cross Cultural Perspective*, 31.

information technology that saturates all aspects of the information society. "Information technology is to this revolution what new sources of energy were to the successive industrial revolutions, from the steam engine to electricity, to fossil fuels, and even to nuclear power, since the generation and distribution of energy was the key element underlying the industrial society."[25]

Castells views the information society as one in which the dominant functions and processes are increasingly manipulated and managed by networks of people. These networks form the basis of the information society. The concept of networks forming the basis of a society is not something new as networks of people existed since the hunter-gather society through to the industrial society. However, the instantaneous communication capabilities provided through information society technologies has now enabled the extension of these networks to a global scale. The communication links between the nodes of the network, enabling the creation and exchange of information, and the membership within a network, allowing access to this information, help to shape the ideas of the people who reside within it. Thus, the shaping of ideas within the network helps to shape the society itself, creating a "network society."[26]

Castell outlines five critical characteristics that form the basis of the network society:

- Information forms the raw material for productivity and power;
- Pervasiveness of the effects that new technologies have on humans and society;
- the Networking logic of any system or set of relationships using these new information technologies;

---

[25]Ibid., 30.

[26]Ibid., 500.

- the inherent Flexibility of the networks such that process and organizations can be changed by reorganizing constituent parts;
- and the Collapse of information age technologies into a single highly integrated system.[27]

The first characteristic of the network society is that information itself is the raw material for productivity. As Daniel Bell points out, the post-industrial society is defined by the quality of life as measured by services and amenities which are created by the manipulation of information vice physical products. In societies past, the creation of food or consumer products was most important whereas the manipulation of information in the network society is a measure of productivity. The second characteristic of the network society relates to the pervasiveness of the effects the new technologies have on humans and society. Information has always been an important element for the effective management of any society. However, the pervasiveness of information technology within the network society and its ability to impact the lives of all people within the society is at an unprecedented speed and scale compared to previous mechanisms of managing information in past societies. This is especially true if information is now considered the raw material for productivity. The third characteristic of the network society refers to the networking logic of any system or set of relationships using these new information technologies. The ability of the network to morph or adapt automatically as a result of the interactions within it allow the capitalization of these interactions without necessarily requiring direct intervention by members of the network. The information technologies are what allow this adaptability to occur automatically. The fourth characteristic of the network society relates to the inherent flexibility of the network itself. Processes can be altered and organizations and institutions can be changed by reorganizing the configuration of the network. This is different from the third characteristic

---

[27]Ibid., 70-72.

in that there is direct manipulation of the network itself by members of the network. The fifth and final characteristic of the network society is the collapsing of information technologies into a highly integrated system. For example, micro-electronics, telecommunications, opto-electronics, and computers are all now integrated into information systems. [28]

The five characteristics of a network society highlighted above compared to today's existing society suggest that we find ourselves within a network society today. The pervasiveness of information technology, the impact and power of information on our daily lives and the flexibility of organizations and processes using modern information technology are stronger now than in previous societies. Further, the potential strengths of the network society need not be restricted to commercial organizations. There is the possibility of exploring the exportation of the characteristics of the network society into a military context. The following section explores the US defence review of the tenets of the network society and how it may be implemented within a military setting.

POWER TO THE EDGE

Modern militaries continually strive to improve their capabilities to provide a fighting edge against an adversary. Whether it is through the introduction of new weapons systems and technologies or the reorganization of units to be more effective with these new technologies, militaries constantly experiment to provide that fighting edge. The introductions of the machine gun or the tank are examples of new technology that necessitated the reorganization of military units to adapt to the new conditions. The information technology supporting the network society that creates new and powerful relationships within mainstream society has the potential to affect the military in similar ways. Discussions have occurred within modern Western military circles

---

[28]Ibid., 70-72.

regarding the incorporation of new technologies and the social organizations that go with them. These discussions are encompassed within the concept of Network Centric Warfare (NCW) which supporters believe will support quicker, more accurate and more decisive operations on a battlefield due to improved Situational Awareness (SA) at all levels.[29]

Network Centric Warfare

NCW is a recent addition to military lexicon as it was first discussed publically in 1998 by VAdm Arthur Cebrowski and John Gartska.[30] Although the term has recently been coined, the idea of sharing or "networking" information to improve military efficiency has been around at least since the Second World War. Further development of military information networking occurred with the naval technological developments that accompanied the Navy's Maritime Strategy, the Army's AirLand Battle or the Air Force's management of air resources through networking systems implemented within NORAD. Dr. Mitchell goes as far as saying that "one might even trace NCW back as far as the 19th century with the integration of rail transportation into military plans."[31]

> Although the sharing of information in a military context is not revolutionary, what does seem to be revolutionary is the near instantaneous information sharing on a global basis due to developments in IT. The potential offered by these technological developments seem to suggest new approaches to both how time and space function in military operations, and reflects changes in terms of fundamental principles such as that of mass and concentration.[32]

---

[29]Paul T. Mitchell, *Freedom and Control Networks in Military Environments* (Singapore: Institute of Defence and Strategic Studies,[2006]), 1-2.

[30]Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future" January, 1998), http://www.kinection.com/ncoic/ncw_origin_future.pdf (accessed 29 January 2012), 28-35.

[31]Mitchell, *Digital Anarchy: The Challenge Posed by Information to the Military*, 6.

[32]Mitchell, *Network Centric Warfare: Coalition Operations in the Age of US Military Primacy* , 44.

With the introduction of modern day information technology, it can be suggested that it is not only the fundamental principles of time and space or mass and concentration that has changed but also the very structure of military organizations to maximize utilization of these new technologies. This reorganization of military structures is, however, questioned by Dr. Mitchell.

> This vision is potentially revolutionary: in terms of its organisational and procedural implications, it strikes at the hierarchical structures that militaries have always relied on for command and control. It remains to be seen whether militaries will be capable of adapting to such a wide-ranging vision.[33]

Although the ability of a military to adjust its military organization is questioned, it is this proposed reorganization that will be discussed next.

The work of Cebrowski & Gartska has been further refined in three separate publications: *Network Centric Warfare* by Alberts, Garstka and Stein in 1999, *Understanding Information Age Warfare* by Alberts, Garstka, Hayes and Signori in 2001, and *Power to the Edge: Command and Control in the Information Age* by Alberts and Hayes in 2003. Each work builds upon the previous effort with a focus on incorporating information age technologies within the military organization to realize improved operational effectiveness in the conduct of military operations.[34]

The purpose of the first publication, *Network Centric Warfare*, is to "describe the Network Centric Warfare concept; to explain how it embodies the characteristics of the Information Age; to identify the challenges in transforming this concept into a real operational capability; and to suggest a prudent approach to meeting these challenges."[35] Alberts and Gartska argue that networks provide businesses a competitive advantage through the distribution of information which creates a shared awareness. It is this shared awareness that allows the

---

[33]Ibid., 38.

[34]Ibid., 34.

[35]Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 1.

businesses under consideration to make decisions more quickly, efficiently and accurately since all personnel and organizations within the business act on the same information at the same time. The authors of this publication then draw a correlation between business practices affected by the instantaneous sharing of information to military operations within a battlespace.

The concept of shared awareness through information sharing allowing for improved decision making compared to an adversary within a military context is labelled "information superiority". The authors of *Network Centric Warfare* state that:

> [W]e view Information Superiority in military operations as a state that is achieved when competitive advantage (e.g., full-spectrum dominance) is derived from the ability to exploit a superior information position. In military operations this superior information position is, in part, gained from information operations that protect our ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same.[36]

Notice that they indicated that the superior information position is, in part, gained from the flow of information between entities while denying the same to the adversary. The other part that is not specifically stated is that the information being exchanged needs to be equally understood by all entities involved in the information exchange. This unstated requirement is essential to achieve information superiority and is glossed over in this publication.

It can be argued that the authors viewed the common training, culture and military ethos evident within a military environment as facilitating that common understanding of the information being exchanged. This is not a shared belief, especially in a coalition environment. Dr. Mitchell points out that "networks challenge the traditional hierarchical structure of military organisation; in the same manner, they also raise important questions regarding coalitions and

---

[36]Ibid., 54.

how they will operate."[37] The understanding of this shared situational awareness is especially challenging in a coalition environment. NCW proponents would argue that it is possible to provide standardized definitions, publications, appropriate training and education amongst network entities to foster the ability to create a common understanding of the shared situational awareness. Exercises and training within and between different militaries are conducted for exactly this reason of creating a common understanding of a shared situational awareness. Thus, if we accept that common training and culture enables common understanding, than the sharing of information and a common understanding of this information while denying the same capability to an adversary would indeed support information superiority.

Achieving information superiority is the focus of NCW: as its supporters argue, networks supported by modern day information technology enable the generation of combat power from agile yet geographically dispersed forces because of their enhanced shared awareness or "information superiority." This generation of superior combat power results from consistently quicker and more accurate operations compared to an adversary due to a force's improved decision cycle afforded through information superiority. If information superiority is achieved according to the definition, then it stands to reason that a force will be able to get inside an adversary's OODA loop and thus provide superior combat power. NCW therefore:

> [F]ocuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[38]

---

[37]Mitchell, *Network Centric Warfare: Coalition Operations in the Age of US Military Primacy* , 32.

[38]Alberts, Garstka and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 88.

Thus, NCW provides a mechanism through information superiority in which military organizations can potentially achieve self-synchronization.

Proponents of NCW state that self-synchronization

> [I]s a mode of interaction between…two or more robustly networked entities, shared awareness, a rule set, and a value-adding interaction. The combination of a rule set and shared awareness enables the entities to operate in the absence of traditional hierarchical mechanisms for command and control. The rule set describes the desired outcome in various operational situations. Shared awareness provides a mechanism for communicating the ongoing dynamics of the operational situation and triggering the desired value-adding interaction.[39]

Is self-synchronization achievable simply by providing the information technology and networks to facilitate the shared situational awareness that creates information superiority? There are those that do not believe this to be the case. Dr. Mitchell points out that "it may ultimately prove impossible to implement information technologies militarily in the manner predicted by NCW's early proponents."[40] This paper suggests that although it is difficult, it is not impossible to achieve self-synchronization. However, this self-synchronization is not achieved solely through the introduction of appropriate information technologies and networked entities. It is achieved through a combination of information superiority with a common understanding between military entities through appropriate training and exercises. Only then will self-synchronization support the achievement of maximum military effectiveness.

Understanding Information Age Warfare

The purpose of *Understanding Information Age Warfare* is to

> [C]ontribute to our ability to move to the next spiral by providing a more detailed articulation of Information Superiority and Network Centric Warfare…define the specific characteristics and the attributes of key concepts…and offer ways to

---

[39]Ibid., 175-176.

[40]Mitchell, *Network Centric Warfare: Coalition Operations in the Age of US Military Primacy* , 31.

> measure the degree to which these concepts are realized and the impact they have on the conduct and effectiveness of military operations.[41]

The authors begin by attempting to explain how information affects the ability of a military to perform operations through the introduction of a series of interconnected domains: the physical domain, the information domain and the cognitive domain. The "physical domain" is where the military takes action. It is where military forces act, shield and manoeuvre themselves and it is this domain where action can be measured through a variety of direct or indirect means. The "information domain" is where information is created, manipulated and shared, facilitating communication amongst combatants. It is not a domain that can be held or touched, and the act of communication is its primary objective. Finally, the "cognitive domain is located in the minds of those people who are utilizing the network. It is this domain where understanding is created through the assimilation of the data that is conveyed from the physical domain through the communication mechanisms provided by the information domain. This understanding forms the basis for decisions that are made in the cognitive domain.[42]

With this understanding of the three domains, the authors then introduce the concept of primitives that are needed to develop their theory for how information affects the performance of individuals and more importantly, military organizations. "Sensing" can be achieved through either direct human experience within the physical domain or indirect sensing through the use of a sensor. The military is rife with sensors, whether they are from existing weapon systems or from direct observation by soldiers in the field. These sensory impressions become "observations" or "data" that are translated into "information" by placing these data points into some meaningful context. Military sensors, whether electronic or human, manipulate what is

---

[41]Alberts, Garstka, Hayes and Signori, *Understanding Information Age Warfare*, 2-3.

[42]Ibid., 10-14.

sensed into information for use by both themselves and others they are communicating with. "Knowledge" involves conclusions drawn from patterns suggested by available information whereas "awareness" is generated through a comparison between what is known and what is currently being sensed. With sufficient levels of knowledge, one can infer possible consequences and predict future patterns to develop an "understanding" of what the situation is becoming. In a military context, knowledge, awareness and understanding is a cognitive process that occurs in the mind of those receiving information.

This understanding allows for "decisions" to be made in the cognitive domain which trigger "actions" in the physical domain. This translates into actions being taken by military units through direction from the commander. "Information sharing" is what takes place when two or more actors work in the information domain to exchange information whereas "shared knowledge" exists when these same actors work in the cognitive domain to share information. "Shared awareness" is what exists in the cognitive domain when two or more actors share an understanding of a particular situation. "Collaboration" takes place in the cognitive domain and is used when two or more actors are working together towards a common goal. Efforts to generate a common shared situational awareness either through information sharing or collaboration is the goal of NCW entities. Finally, "synchronization" takes place in the physical domain and is the result of a meaningful arrangement of things or events in time and space. [43] The authors argue that it is this set of primitives "from which the concepts that lie at the heart of Information Superiority and Network Centric Warfare can be constructed."[44]

---

[43]Ibid., 14-29.

[44]Ibid., 29.

The authors point out that NCW is about the sharing of information and awareness. "The ability to share information is essential to being able to develop a state of shared awareness, as well as being able to collaborate and/or synchronize."[45] The authors believe that NCW supports the sharing of information which develops awareness which ultimately creates information superiority. In addition, shared knowledge is essential for independent actors to coordinate their actions.

> The degree to which shared knowledge can be developed has a significant influence on the nature of command and control that can be employed, the nature and amount of communications that are needed to develop and maintain shared awareness, and the ease and degree to which forces can be synchronized.[46]

What is derived from this sharing of information, awareness and knowledge is the provision of force enablers for combat troops through the improvement of information provided to commanders.

This information is characterized by its richness (quality) and reach (ability to be shared throughout the network). In a traditional military hierarchy, information with a higher richness traditionally has lesser reach. However, in a properly configured network environment, information no longer has any restrictions to its access as it will be available in real time. This shared situational awareness allows for greater unity of command, better focus for missions, efficient use of scarce resources and improved force protection. NCW thus focuses on the three domains mentioned above. In the physical domain, all forces are connected together in a network to provide "secure and seamless connectivity and interoperability". In the information domain, a military force must be capable of sharing, accessing and protecting "information to a degree that it can establish and maintain an information advantage over an adversary." Finally,

---

[45]Ibid., 24.

[46]Ibid., 26.

forces in the cognitive domain must be capable of developing shared awareness and understanding to allow them to self-synchronize to take full advantage of the network.[47]

Power to the Edge

Understanding Information Age Warfare focuses on the relationship between information, knowledge and awareness. However, it does not go into detail as to how this theory affects military operations in this new networked environment. Therefore, a third publication was required to complete the analysis from a military perspective. The purpose of *Power to the Edge: Command and Control in the Information Age*, is to "explain why we must go down the road less traveled, why current command and control concepts, organizations, and systems are not up to the task at hand, and present the approach to command and control and C2 support systems that is needed. This approach is called *power to the edge*."[48] For militaries to take advantage of the competitive advantage provided by NCW, they must "focus on C2, where information is translated into actionable knowledge."[49] Traditional command and control constructs and hierarchical military organizations are at a disadvantage in the modern day battlefield due to the added complexity and speed of operations that are inherent in modern day operations. The authors state that modern militaries have, thus far, created theatre specific modifications or tweaked their organizations on a case-by-case basis to reduce the inefficiencies they currently experience with their current information exchange organization. Unfortunately, this tweaking has limited effects and does not resolve the issues surrounding the necessity of instantaneous information exchange to support information superiority and allow the realization

---

[47]Ibid., 57-59.

[48]Alberts and Hayes, *Power to the Edge: Command, Control in the Information Age*, 4-5.

[49]Ibid., 4.

of self-synchronization on the battlefield. A more permanent change in military structure and organization is required.

This change in structure and processes is founded on "two key force capabilities needed by Information Age militaries [which] are *interoperability* and *agility*".[50] These capabilities have been required by militaries in past ages to some extent in the conduct of war. However, the introduction and pervasiveness of information technologies in all aspects of the internal workings of a military organization place increasing emphasis on these two force capabilities for militaries to be effective.

Given the requirements for interoperability and agility, centralized command and control becomes increasingly inefficient and counter-productive. As a result, the power to make decisions and create effects on the battlefield need to be devolved to the edge.

> *Power to the edge* is about changing the way individuals, organizations, and systems relate to one another and work. *Power to the edge* involves the empowerment of individuals at the edge of an organization (where the organization interacts with is operating environment to have an impact or effect on that environment) or, in the case of systems, edge devices. Empowerment involves expanding access to information, and the elimination of unnecessary constraints. For example, empowerment involves providing access to available information and expertise, and the elimination of procedural constraints previously needed to deconflict elements of the force in the absence of quality information.[51]

This concept may sound like the concept of mission command where flexibility is given to lower levels of command to conduct operations that are in line with a superior commander's intent. However, power to the edge recognizes the increased awareness associated with shared situational awareness and information superiority. This improved awareness empowers lower level units (edge units) to seize initiatives that traditionally were restricted due to the constraints

---

[50]Ibid., 56.

[51]Ibid., 5.

placed on them with traditional military operations lacking appropriate information at all levels of command. Essentially what the authors are proposing is that the ability to exchange information and empower the frontline combatant is critical to modern day combat effectiveness. They are encouraging the sharing of information and awareness down to the lowest levels. Thus, the power to the edge concept is congruent with the network society concept espoused by Castells. The challenge for modern day militaries is to recognize the benefits associated with the concept of power to the edge and accept that organizational structures may have to change to support it and allow it to happen.

Removing barriers and providing the necessary tools to facilitate this shared information and awareness is a necessary prerequisite to success. This paper will now look at the tools and technologies that have been developed that can support the concept of power to the edge. These technologies can be organized under the heading of new media.

NEW MEDIA

The above discussion centered on the theories of network society by Castells and power to the edge by Alberts, *et al.* For these theories to be realized, they require the support of modern day information technologies which can be organized under the heading of new media. Why new media? Jaya Deu Murthy's review of the evolution of the Internet summarizes the impact of the Internet on society.

> It is apparent that various technological innovations in converging media and transmission methods that the Internet will continue to transform into a more sophisticated medium with significantly larger capabilities. As a result, the Internet will continue to have a decisive impact on society where it is up to humankind to chart its course for the benevolent betterment of society.[52]

---

[52]Murthy, *Evolution of the Internet and its Impact on Society*, 97.

He proposes that the capability and sophistication of new media impacts and changes society. Michael Welch's review of the emerging media revolution argues:

> The ability of new media forms to continue in their propagation and to outpace the efforts of the entrenched elite power base that seeks to dominate them will largely determine their ability to influence a resurgence of democratic society. In particular, their ability to shift from centralized ownership and content origination towards the direction of online communities, which are collaborative in nature, where participants become the principle source of content, will be an important factor in their continuing and growing relevance and influence. In this way, this movement will parallel the convergence of centralized mass media forms with the emergence of the Internet, a highly decentralized and collaborative communication modality.[53]

Welch's premise is that new media is shifting power in a democratic society from centralized ownership and message creation to one of decentralization ownership where participants within the network generate the message through collaboration. New media is supporting the devolution of message creation to all participants within the network. This support is what is required from a network society or power to the edge perspective. It is this devolution of message creation that must be recognized by the hierarchical structure of military command to leverage the power of new media. Thus, new media needs to be defined and the main characteristics of new media need to be described so as to better understand how this technology supports the concepts of the network society and power to the edge.

New media is an all-encompassing term for the many different types of electronic communication means that are now possible through the introduction of modern day computers and smart electronic devices. This term is in contrast to what would be labelled old forms of media such as print newspapers and magazines that are static forms of text and graphics that

---

[53]Michael T. Welch, "The Emerging Media Revolution: Considering the Influence of New Media Forms on Democratic Society" (M.A., Gonzaga University), http://search.proquest.com/docview/304945805?accountid=9867, 40.

cannot be changed. In the publication of *The Language of New Media* by Lee Manovich, the definitions of new media are:

> [T]he cultural objects which use digital computer technology for distribution and exhibition. 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.[54]

This definition focuses on the technologies used for the creation and distribution of a message; however, it does not speak to how these technologies affect the organizations and society which generate the message or the message itself.

Andrew Chadwick's review of the impact of the Internet on politics points out that the Internet is "a source of institutional innovation; it creates some new institutions of its own."[55] Organizational structures are changing to take advantage of the innovation available through new media. He points out that even traditional organizations have realized the potential of the Internet and have modified their internal organization and created new networks amongst previously "untapped reservoirs of citizen support"[56] to capitalize on new media potential. What makes the Internet unique compared to previous forms of communication is its truly global user base[57] and the fact that new media is changing how we convey a message and to whom, thus collective political action is being shaped by the medium itself.[58] This review from a global

---

[54]Lev Manovich, "New Media from Borges to HTML," in *The New Media Reader*, eds. Noah Wardrip-Fruin and Nick Montfort (MIT Press, 2003) (accessed 29 January 2012), 11.

[55]Andrew Chadwick, *Internet Politics: States, Citizens, and New Communication Technologies* (New York: Oxford University Press, 2006), 3.

[56]Ibid., 120.

[57]Ibid., 11.

[58]Ibid., 142-143.

political point of view highlights how new media can affect the organizations and society which generate the message and the message itself. Furthermore, it resonates with the theories of network society and power to the edge. The changing organizational structures and development of networks to capitalize on the benefits of new media are explored in each theory and lend mutual support to each one.

Digital technology platforms and access to the ubiquitous Internet are becoming the source of communication between businesses and consumers, governments and citizens, and between like-minded individuals or societal networks. Today's new media technology hardware is a merging between the computing powers of modern day computers with the convenience of small handheld consumer electronic devices. The predominant form these merged devices come in are in the form of "smartphones" which encompasses cell phone capability, Internet access, music player, camera, video recorder and playback, voice recorder, GPS navigator, mini game console and the platform of choice for mini versions of most popular software applications that support user productivity. In essence, "the smartphone is truly the personal computer of the 21st century, because the cellphone is the single most 'personal' machine people keep with them all the time."[59] Having said this, new media is more than just hardware devices such as the smartphone. It is also about new communication methods in the digital world. "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 new communication ability

---

[59]PC Magazine, "Definition of Digital Convergence," *PC Magazine* (2012). http://www.pcmag.com/encyclopedia_term/0,2542,t=digital+convergence&i=41316,00.asp; Internet; accessed 29 January 2012.

is supported through the new media characteristics of pervasiveness, instantaneous communications, social connectivity and the ability to be interactive.

Pervasiveness and Ubiquity of New Media

Modern day technology is so embedded within modern day society that it has become invisible to the average user. Every aspect of our daily lives is supported by technology, whether it is health, transportation, utilities, government services, communications or our social life. New media epitomizes the pervasiveness and ubiquity of technology in our modern day society. Pervasive technology is a technology that has become diffused throughout our environment whereas ubiquitous technology exists everywhere at the same time. The Internet is an excellent example of a pervasive and ubiquitous technology. It supports every aspect of our society through the power to communicate between various entities and it facilitates the interaction between these same entities. It is an unseen enabler working in the background to facilitate societal interactions. The same can be said of cellular networks that have become a pervasive and ubiquitous technology in our lives. Modern day society expects connectivity everywhere they go around the world. The saturation of smartphones and other new media devices demonstrate the pervasiveness and ubiquitous nature of today's technologies. The pervasiveness and ubiquity of new media supports the characteristics of pervasiveness and information technology collapse into a single integrated system defined within the concept of the network society defined earlier in this paper. They also facilitate shared situational awareness at all times down to the lowest level espoused by the concept of power to the edge. Thus, pervasiveness and ubiquity support both the network society and power to the edge.

---

[60]PC Magazine. "Definition of New Media," *PC Magazine* (2012). http://www.pcmag.com/encyclopedia_term/0,2542,t=new+media&i=47936,00.asp; Internet; accessed 29 January 2012.

This pervasiveness of technology has come to be expected by today's society. Joseph Weizenbaum, a professor emeritus of the computer science department at MIT and well known critic of computers and technology refers to this pervasiveness as a condition. He states:

> No one planned it, there was no conference to decide upon it, and no one can say, "We're getting rid of it." The condition has grown, just like we use automobiles today as a matter of course. But even with this example, you can ask yourself if that makes sense, given the traffic jams, exhaust, and use of oil resources. Today, many people use a huge number of computers – many of them networked – with exactly the same lack of reflection.[61]

The pervasiveness of digital communications technology impacts the expectations of members of society in that they expect to be able to be reached at any time; hence they have attained instantaneous connectivity.

Instantaneous Connectivity

New media is fostering an ability to connect with others in real time to have instantaneous answers; it is outpacing traditional media capabilities to disseminate information in a timely manner. For example, with technologies such as Really Simple Syndication (RSS), members of society can monitor those issues that interest them without the hassle and time consuming activity of manually reviewing websites. Upon subscription to an RSS feed, it "pokes" a user when there are changes to a topic that the user had deemed important; users are simply a button push away from accessing the updated information of interest. This RSS technology directly supports the tenets proposed by Alberts, *et al.* in view of a truly networked environment. RSS allows users of information to transition from a *push* approach to information dissemination to a *post and smart pull*. "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 potentially

---

[61]SAP.info. "The Pervasiveness of Technology Degrades Personal Responsibility," *Events* (5 January 2004). http://en.sap.info/the-pervasiveness-of-technology-degrades-personal-responsibility%e2%80%9d/3525; Internet; accessed 29 January 2012.

interested parties to the problem of having the individual who needs information identifying potential sources of that information."[62] The instantaneous communications fostered by *post and smart pull* applications such as RSS make it easier for the user who has an information requirement to determine the usefulness of the information compared to the producer of the information making the judgement. The mobile Internet engenders expectations of instantaneous communications and access to information. Combining small handheld devices such as smartphones with the mobility supported by modern day cellular networks facilitates social connectivity to a scale never seen before.

Social Connectivity

In a review of the impact of new media in society in *Bullets and Blogs: New Media and the Warfighter*, notes "new media leverage[s] social connections between people based on language, shared interest, family, schooling, etc."[63] Communications between people using social media mechanisms is exploding to an unprecedented scale. The globally accessible website Facebook demonstrates this staggering communications mechanism. This single social networking website has over 800 million active users in 2012 in which over 50% log onto Facebook in any given day. There are over 900 million objects (pages, groups, events and community pages) that people interact with every day and it supports over 70 languages. Almost half of the current active users currently access Facebook through their mobile devices.[64] The growth of Facebook which was launched in 2004 with 1 million users to the statistics in 2012 is truly staggering and represents a fundamental shift in how our networked society of today

---

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

[63]Collings and Rohozinski, *Bullets and Blogs: New Media and the Warfighter*, 9.

[64]Facebook, "Statistics," http://www.facebook.com/press/info.php?statistics; Internet; accessed 29 January 2012.

interacts with one another. Users have become reliant on these new social media technologies to stay in touch in real time and have invested heavily in mobile communication mechanisms to achieve this real time connectivity. It also fosters a form of interactive communications rarely seen outside of the traditional telephony world.

Interactive Communications

New media goes beyond pervasiveness, instantaneous communications and social connectivity into the realm of interactive communications. It goes beyond peer-to-peer communications like Short Message Service (SMS), email and cellular telephony by allowing users to post content in a medium instantly accessible to anyone with interest and allowing the flexibility of other users to respond, comment or correct information immediately. Facebook encourages the sharing of comments and items instantaneously with feedback expected by those viewing the information. However, there are other applications like web log (blog) sites and micro-blogs like Twitter that also provide an interactive peer-to-peer environment. There are even mainstream organizations that have embraced these interactive tools. News outlets like the Canadian Broadcasting Corporation (CBC) allow those who are reading their online articles to post comments which foster interactive communications between others in society who have a view on a particular topic. For example, the Canadian government's introduction of Bill C-30 Investigating and Preventing Criminal Electronic Communications Act sparked significant debate from those supporting and opposing the bill. The differing views expressed by readers posting comments on CBC's webpages sparked open dialogue and a better understanding of the issues to all participating in the discussion.[65] Interactive communications is encouraged throughout our network society.

New Media Characteristics Summary

New media's characteristics of pervasiveness, instantaneous communications, social connectivity and the ability to be interactive support the five critical characteristics of the network society defined by Castells. Today's society expects ubiquitous information exchange and expects quality interactions within the networked environment. Furthermore, new media coupled with mobile platforms such as smartphones provide the technological capabilities necessary to support the military concept of power to the edge whereby shared situational awareness is facilitated to the lowest possible level. It allows for real-time collaboration when conducting intelligence preparation of the battlefield allowing all users tied to the network to provide insight and input into the process. It also allows for two-way interactive communications between various levels of command right down to the soldier on the ground conducting operations. This provides potential for training, improving tactics, receiving instantaneous feedback and providing the shared situational awareness that facilitates self-synchronization. Furthermore, the ability of new media to support interactive communications between various social communities allows the common day soldier to support the positive information campaign in the public domain that is so crucial to furthering support for today's missions.

CHAPTER SUMMARY

To understand why the CF should incorporate smartphones and associated technologies within its working environment, it is essential to understand how information technology has influenced society to make the sharing of information the predominant form of power. Both the

---

[65]Community Team, "How should Canadians Pay for the Online Surveillance Bill?" *CBC News* (22 February 2012). http://www.cbc.ca/news/yourcommunity/2012/02/how-should-canadians-pay-for-the-online-surveillance-bill.html; Internet; accessed 27 February 2012.

network society and the technological tools supporting the network society must be defined to better understand the benefits to the CF. Therefore, this chapter explored the concept of the network society that we find ourselves in today where information itself becomes the focus of power. How the military has translated this network society concept into the concept of power to the edge was then discussed to understand how common shared situational awareness supports information superiority and empowers self-synchronization of military forces to maximize efficiency and efficacy in military operations. The concept and characteristics of new media were then explored to better understand how these technologies empower the vision of power to the edge. It is this understanding of society and technology that provides insight into the rationale for implementing smartphones and associated technologies within the CF.

With a background understanding of the rationale to explore these technologies further, the next chapter will provide an overview of the United States Army efforts to deploy smartphone technologies to their frontline soldiers. Through the analysis of this case study, it will be demonstrated that they are implementing the tenets of power to the edge described in this chapter through the use of new media tools and technologies.

CHAPTER 3

US ARMY CASE STUDY OF SMARTPHONE IMPLEMENTATION

Chapter 2 provided a background understanding of how the network society promotes the use of information age technologies and the benefits associated with incorporating network society concepts within a military framework. Additionally, the benefits accrued through the devices and technologies associated with new media were listed to demonstrate how new media is the technical driver behind the network society. With this background understanding of the rationale to explore these technologies further, this chapter will provide an overview of the United States Army efforts to deploy smartphone technologies to their front-line soldiers. Through the analysis of this case study, it will be demonstrated that they are implementing the tenets of "power to the edge" described in the previous chapter through the use of new media tools and technologies.

This chapter will start by analyzing failed attempts by militaries to develop unique military solutions, thus supporting efforts to use Commercial Off The Shelf (COTS) equipment and technologies. The smartphone trial case study will then be presented, identifying the administrative and operational areas where these smartphones are being deployed and details regarding the implementation will be provided. In addition, the strictly controlled access "App Store" will be introduced and examples of some of the apps that have been developed in both the administrative and operational world will be highlighted to provide insight into the potential these smartphones bring to the modern day warfighter. These examples will show that these efforts are linked to the power to the edge concept introduced in Chapter 2. Once this linkage to theory is articulated, the concept of Canada capitalizing on the US Army efforts will be explored, linking the phased approach that the US Army is conducting to one that should be undertaken by

Canada. Thus, the lessons learned in the administrative world can be transported to the operational sphere where concerns regarding confidentiality, integrity and availability are higher. By the end of the chapter, it will be argued that Canada should immediately explore the introduction of smartphones and associated technologies.

FAILED MILITARY UNIQUE SOLUTIONS

Western militaries have traditionally developed custom systems and equipment for use in unique military operating environments.[66] Civilian pattern equipment traditionally was not rugged enough to handle the austere operating conditions experienced by soldiers in the field. The concept of "milspec" was introduced in the electronics industry when dealing with the building of military electronic equipment to deal with exactly that dilemma.[67] The requirement for milspec equipment fosters a culture of demanding unique military solutions through all aspects of military development and procurement. However, modern day civilian demand for consumer electronics has resulted in industry investing major efforts in this business. Unfortunately, the military culture of demanding unique military solutions instead of exploring civilian designed solutions has not changed to take advantage of industry civilian research and development efforts.

The Joint Tactical Radio System (JTRS) project is an example of this military procurement culture. The US Army stood up a project to develop a "universal" radio capable of replacing most of the radios that are currently used by front-line soldiers. The Ground Mobile Radio which was to be the major deliverable for this project was meant to replace three unique

---

[66]Military radios such as the Joint Tactical Radio System (JTRS) (discussed further in this paper), customized weapons control systems on board naval, land and air platforms are examples of customized systems that were developed specifically for the military. Mitchell, *Network Centric Warfare: Coalition Operations in the Age of US Military Primacy*, 32.

[67]Milspec is a military specification which describes the essential technical requirements for purchased materiel that is military unique or substantially modified commercial items.

radios into a single JTRS device. In October 2011, after 15 years and $17 billion USD, the US Army announced the cancellation of the Ground Mobile Radio. The military's efforts to develop a unique solution proved to be unachievable. [68]

A similar effort has been expended in the area of empowering the front-line soldier with information in support of power to the edge. Initially called Land Warrior and later labelled Nett Warrior, the project's goal was to use a combination of computers and communication devices with cables routed throughout the soldier's body armour to connect the warfighter on the battlefield with his unit or headquarters. Unfortunately, the current capabilities of the Nett Warrior solution lag those available from commercial grade smartphones available today.[69] A similar solution called Sentinel developed by Rockwell Collins exists with similar challenges. Realizing the impact of smartphone development and distribution, the Sentinel solution has embraced an open architecture to allow it to interface with legacy radios, smartphones and tablets.[70]

Recognizing the challenges associated with developing customized military solutions which falls short of the capability of commercially available technology, the US Army office overseeing the Nett Warrior program has placed the multi-million dollar project on hold while it

---

[68]David Axe. "Inside the Army's Doomed Quest for the 'Perfect Radio,'" *Danger Room: Wired* (11 January 2012). http://www.wired.com/dangerroom/2012/01/army-perfect-radio/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WiredDangerRoom+%28Blog+-+Danger+Room%29&utm_content=Google+Reader; Internet; accessed 29 January 2012.

[69]Spencer Ackerman. "Soldiers' Wearable Computers May Get an iPhone Brain," *Danger Room: Wired* (14 April 2011). http://www.wired.com/dangerroom/2011/04/soldiers-wearable-computers-may-get-an-iphone-brain/; Internet; accessed 29 January 2012.

[70]Paul McLeary. "No iPhone Here: More Designs for Networked Soldiers," *Defense Technology: Aviation Week* (15 September 2011). http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a5d493ee3-dba8-41df-be45-55e36a889209&plckScript=blogScript&plckElementId=blogDest; Internet; accessed 29 January 2012.

considers commercial solutions for the intelligence portion of their solution.[71] "Smartphones could be the answer to the Nett Warrior requirement."[72] To realize this vision, the US Army has developed a requirements document detailing a Nett Warrior End-User Device (NW EUD), essentially a smartphone, that can provide "commercial-based, integrated computer, display and data-entry capability for dismounted use in either standalone or networked configuration."[73] Furthermore, the US Army is insisting that the phones be powered by the Android operating system and have integrated camera, GPS and accelerometers, all capabilities that are commercially available today.[74] Essentially, the US Army has recognized that commercial solutions are not only cheaper than military solutions but also are more powerful and flexible than military unique solutions.

The recognition of the power and flexibility of smartphone technologies by both the Nett Warrior and Sentinel programs highlights the pervasiveness of these technologies in our society and the direction these and similar programs will go for future requirements. With this understanding, it is now time to review the US Army smartphone trial.

SMARTPHONE TRIAL

The implementation of smartphone technologies within the US Army is the responsibility of the Connecting Soldiers to Digital Applications (CSDA) project. CSDA is researching the

---

[71]Spencer Ackerman. "Army Hits Pause on "Wearable Computer" Program," *Danger Room: Wired* (28 July 2011). http://www.wired.com/dangerroom/2011/07/army-hits-pause-on-its-wearable-computer-program/; Internet; accessed 29 January 2012.

[72]Christian. "Will Army Smartphones Kill Net Warrior?" *Military.com: KitUp* (24 February 2011). http://kitup.military.com/2011/02/will-army-smartphones-kill-nett-warrior.html#ixzz1JWOM6eze; Internet; accessed 29 January 2012.

[73]Spencer Ackerman. "Army Taps Android Phones for "Wearable Computers"," *Danger Room: Wired* (6 September 2011). http://www.wired.com/dangerroom/2011/09/nett-warrior-smartphone/; Internet; accessed 29 January 2012.

[74]Ibid.

utility of providing soldiers smartphones with unique digital applications (apps) designed to support training, administration and operational functions conducted on the battlefield. CSDA "is a two-phase initiative with about eight pilots that are designed to determine the value of using commercial smartphone technology in administrative tasks and tactical operations."[75] In phase 1, the Army deployed various smartphone platforms with a focus of evaluating apps for education, professional development, access to reference material and administrative tasks. Along with the devices and associated apps, there is a need to provision network services with a data portal where users can access databases containing digital content. Pilot sites are focusing on initial military training including training for military police officers, engineers and infantry soldiers. Apps provide a "persistent learning environment" with significant potential to save time and improve the learning experience. Along with training evaluation, the Army Evaluation Task Force at Fort Bliss, Texas is trialing 200 phones in a company-sized organization to evaluate applications such as those used to identify friend from foe. Phase 2 of the project will evaluate the utility of apps within a tactical environment as well as explore requirements for gateways and base stations to integrate these technologies with tactical radio networks and battlefield command systems.[76]

By porting training applications to a smartphone, soldiers can maximize the use of their spare time to continue training from anywhere on the globe through persistent connectivity. The small form factor, light weight and powerful computing capabilities make it an ideal choice for a mobile platform for the deployed soldier.[77] Security issues are evident in both administrative

---

[75]Perry, *Army toTest Smarphones for Offices, Battlefields*.

[76]Stand-To!. "Connecting Soldiers to Digital Applications," *US Army* (2010). http://www.army.mil/standto/archive/2010/07/15/; Internet; accessed 29 January 2012.

and operational environments within the military. However, security restrictions are traditionally less prevalent within an administrative environment; thus, there is a significantly higher potential to connect all facets of the administrative network through to the mobile smartphone devices. This would enable full functionality and access that is experienced in today's computing environment to the mobile user. Training, administrative and professional development can progress at a faster pace based on the user's abilities vice the user's access to networking infrastructure.

Within an operational environment, evaluations are being conducted at Fort Bliss, Texas and the White Sands Missile Range in New Mexico. During a six week training exercise, soldiers from the Second Brigade Combat Team, First Armored Division, will test the devices in austere desert environments to evaluate how they handle the stress of simulated combat. The Army is experimenting with Apple devices such as the iPhone and iPad as well as Google Android devices.[78] The intent of the US Army's mobile network is to allow soldiers access to key information at any time from any location to

> facilitate fire and maneuver, and survive in close combat; provide collaboration capability to aid in seizing and controlling key terrain; employ lethal and non-lethal capabilities, coupled with sensors, to effectively engage targets at extended ranges; distinguish among friend, enemy, neutral and noncombatant; and integrate indirect fires.[79]

---

[77]David Walsh. "Army Looks to Troops for Smart-phone Tech Advice," *Government Computer News* (17 October 2011). http://gcn.com/articles/2011/10/10/defense-it-1-smartphone-technologies.aspx; Internet; accessed 29 January 2012.

[78]Philip Ewing. "Army Begins Mobile Phone Experiments," *DoD Buzz* (6 June 2011). http://www.dodbuzz.com/2011/06/06/army-begins-mobile-phone-experiments/; Internet; accessed 29 January 2012.

[79]United States Army. "Providing the Network to the Tactical Edge," http://www.bctmod.army.mil/; accessed 29 January 2012.

The intent of the smartphone or tablet computer connected to the network is to allow soldiers the ability to collaborate in new ways, allowing information to be passed to and from higher command to better inform commanders prior to making decisions.

There are numerous ideas as to how to leverage this technology for battlefield advantage. One scenario would have soldiers use these mobile devices to take pictures of suspected targets, forward the pictures to intelligence staff located at headquarters and confirm whether or not the suspected target is of interest. This would ensure time is not wasted relocating innocent targets to headquarters for unnecessary questioning. Apps could be developed to link the GPS capabilities of the devices with embedded maps of the terrain being traversed to provide not only navigation but warning of potential dangers if these maps and geographic coordinates are linked with intelligence regarding locations of Improvised Explosive Devices (IEDs), friendly forces and enemy forces.[80] Biometrics are already being used in Iraq and Afghanistan but the quantity of specialized devices are limited. If these biometric capabilities were embedded in a smartphone, all front-line combatants would be empowered to take photographs, fingerprints and iris scans of suspected targets to provide confirmation of identity, improving the efficiency of combat operations.[81]

Efforts to incorporate smartphones and tablets within the military are not restricted to the US Army. Capt. Jim Carlson, a Cobra pilot in a Marine Light Attack Helicopter Squadron (HMLA) was frustrated with the requirement to carry numerous detailed physical maps onboard helicopters in support of missions. Over 80 pounds of these cartographical maps are brought on

---

[80]Philip Ewing. "The Army's Big Network Experiment," *DoD Buzz* (14 June 2011). http://www.dodbuzz.com/2011/06/14/the-armys-big-network-experiment/; Internet; accessed 29 January 2012.

[81]Nathan Hodge, "Killer App: Army Tests Smartphones for Combat," *The Wall Street Journal* (3 June 2011). http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html; Internet; accessed 29 January 2012.

board on any given mission and the ability to manipulate these maps while conducting operations is challenging at best.[82] With the approval of senior Marine commanders, efforts have been expended to trail the use of tablet devices, in this particular case iPads, to provide electronic maps to the pilots. The app that was developed enables the pilots to zoom in, zoom out and quickly move from one map to another, providing a tangible fighting edge to the aerial combatant.[83]

The various trials listed above rely on connectivity to achieve the desired administrative or operational effect. Conducting trials on US soil with robust cellular coverage does not necessarily reflect the environments that soldiers will experience in areas of conflict. To overcome this connectivity challenge in austere locations, trials are also being conducted on marrying the communication capabilities of field radios with the processing power of smartphones to extend the range and feasibility of these devices in the field. In one particular trial, "JTRS HMS Rifleman and Manpack radios were married with[Program Executive Office Command, Control and Communications – Tactical] PEO C3T prototype handhelds, demonstrating interoperability between programs of record in the 'transport layer' and the 'application layer.'"[84] The ruggedized, Android-based smartphone (PEO C3T) ran two apps:

> Joint Battle Command-Platform, or JBC-P Handheld, and Tactical Ground Reporting, known as TIGR Mobile. JBC-P is the follow-on program for Force XXI Battle Command Brigade and Below, or FBCB2. JBC-P displayed blue icons indicating the real-time GPS locations of friendly forces across a map of the battlefield, where users could also plot enemies or landscape hazards to alert their

---

[82]Mark Riffee. "iPads Now Helping Marines Unleash Hell," *Danger Room: Wired* (16 September 2011). http://www.wired.com/dangerroom/2011/09/death-on-an-ipad/#more-57371; Internet; accessed 29 January 2012.

[83]W. J. Hennigan. "Taking iPads into Battle," *Los Angeles Times* (25 September 2011). http://articles.latimes.com/2011/sep/25/business/la-fi-isoldiers-20110926; Internet; accessed 29 January 2012.

[84]Claire Heininger. "Smartphones Combine With Tactical Radios to Boost Ground Troops," *US Army* (9 March 2011). http://www.army.mil/article/53005/; Internet; accessed 29 January 2012.

> teammates. TIGR enabled users to exchange photos, and to enter and retrieve historical information relevant to the operation.[85]

This trial confirmed that the capabilities envisioned through the implementation of smartphones and associated technologies are feasible in environments that do not have cellular coverage as well as those that do.

The trials detailed thus far have demonstrated both the feasibility and potential for the implementation of smartphones in both administrative and operational environments. The following discussion will focus on providing examples of existing apps to highlight what already exists and encourage thought as to potential future applications.

Apps Store

A proper software development environment controlled by the US Army is required to facilitate the creation of useful apps within both the administrative and operational settings. This controlled setting is required to provide structure and focus effort. The Army's solution to this requirement is the Common Operating Environment (COE).

> The COE is a set of computing technologies and standards that will enable secure and interoperable applications to be rapidly developed and executed across a variety of computing environments: server, client, mobile devices, sensors, and platforms…The COE Architecture and the Army's overarching "End State" Architecture will drastically reduce the time it takes to deliver relevant applications to those who need them. The COE augments Army Software Transformation, an effort to standardize end-user environments and software development kits, establish streamlined enterprise software processes that rely on common pre-certified, reusable software components, and develop deployment strategies that allow users direct access to new capability.[86]

COE's dissemination throughout the Army sets the stage for soldiers to be equipped with smartphones configured with appropriate apps to link them to the information they need. Apps

---

[85]Ibid.

[86]United States Army. "Common Operating Environment," http://ciog6.army.mil/ArmyEnterpriseNetworkVision/tabid/79/Default.aspx; accessed 29 January 2012.

designed within COE are allowed to access the Army's data systems which are encompassed within its Enterprise Network. Whether the software designer is a common soldier or defence company, the COE guides the development of the various communication tools, whether these tools are for radios, smartphones or applications for the smartphones. "The COE is designed to be agnostic to any particular platform, instead elaborating the technical requirements that apps have to meet. Its goal is interoperability, in its founding document's words, so data is 'available anywhere on the network to authorized users from any suitable Army-managed device.'" [87]

The follow on stage to providing appropriate direction regarding software development under the COE construct is to provide a portal to distribute available apps. The Army Marketplace is the solution to this requirement. The Army Marketplace was developed to support the distribution of apps created during the Apps for the Army (A4A) contest sponsored by the US Army which encouraged grass roots development of apps useful to the front-line soldier. The purpose of the Army Marketplace is not only to distribute existing apps but to stimulate discussion and ideas regarding the creation of new ones. The vision for Army Marketplace is to have it become an app in its own right, downloaded onto Army-issued smartphones to encourage the sharing of useful apps.[88]

Understanding that the background software development environment is available and an appropriate distribution channel exists, it is important to get a sense of the types of apps

---

[87]Spencer Ackerman. "Army Wants Low-Level Soldiers Linked Into Its Data Nets," *Danger Room: Wired* (22 February 2011). http://www.wired.com/dangerroom/2011/02/army-wants-low-level-soldiers-linked-into-its-data-nets/; Internet; accessed 29 January 2012.

[88] Spencer Ackerman. "First Look: Inside the Army's App Store for War," *Danger Room: Wired* (27 April 2011). http://www.wired.com/dangerroom/2011/04/armys-app-store-for-war/; Internet; accessed 29 January 2012.

available both in the administrative and operational environments. A sample of the various apps currently available is as follows:[89]

- New Recruit provides basic military information for new recruits including military rank and insignia information, news feeds, physical fitness test calculators and a body mass index calculator.
- Physical Training Program assists soldiers with the development of a unique physical fitness program based on the Army's new Physical Readiness Training program. The app provides access to existing training plans and exercise videos that can assist with physical fitness development.
- Telehealth Mood Tracker is an app that assists with monitoring psychological health over an extended period of time using a visual analog rating scale. Users track their experiences related to deployment psychological health issues.
- Disaster Relief is a web-based tool used to search, edit or create maps that can be viewed via Google Earth and/or Google Maps which helps Army personnel working in humanitarian missions working with non-military members or organizations.
- Movement Projection is a route map app for road navigation that enables soldiers to inject start, stop, waypoints and items of interest so that calculations can be completed on the optimal route based on preconfigured criteria.
- Buddy Tracking is a GPS-based app that enables soldiers to track other soldiers, essentially a smartphone equivalent of Blue Force Tracker.
- COIN is an app that enables soldiers to gather, evaluate and track intelligence information specific to targets of interest. Soldiers conduct data entry while in the field

---

[89]. "Is it Smart for the US Army to Develop Smartphones," *Defense Industry Daily* (24 February 2011). http://www.defenseindustrydaily.com/military-smartphones-dod-apps-06512/; Internet; accessed 29 January 2012.

and COIN transmits the information in real-time to intelligence sections collocated with command units.

- MilSpace is an app that provides customization to the computing experience of a soldier, providing him a single tool to view several sources of information in one location.
- Sensor Sharing is an app that allows soldiers to share information gathered by the smartphone as well as by UAVs with a predetermined list of peers created by the soldier.
- Fingerpaint is an app that allows a soldier to take a picture and draw on the screen with his finger to provide additional information that is then sent back to headquarters for further analysis.
- Inputting Information is an app that allows soldiers to inject intelligence information into the larger Army intelligence network.
- "Mil-Dot Rangefinder for the iPhone takes the math out of ranging targets using a mil-dot scope. Real-time calculations provide instant range measurements in both yards and meters. The simple interface allows for one handed operation and eliminates any need to manually type any measurements to range a target."[90]
- "The SoldierEyes Common Operating Picture… is like a mini Blue Force Tracker…a real-time way for soldiers to monitor where friendly forces are at any given time, represented by little blue boxes. And not just friendlies: Plug in an enemy's position and the cloud shares it with anyone else running SoldierEyes, whether out on patrol or back at the command post. Its GPS components allow soldiers to use the map for navigation while they see where their friends and foes are…Load Augmented Reality, another SoldierEyes sub-app, ditches the map. Instead, it uses your handheld's camera to give

---

[90]Christian. "Range it in with your iPhone," *Military.com: KitUp* (12 July 2010). http://kitup.military.com/2010/07/range-it-in-with-your-iphone.html; Internet; accessed 29 January 2012.

> you a picture of what's in front of you — but with the colored boxes of friendlies and enemies in position on the screen. The idea is make sure that soldiers getting out of their vehicles don't lose a sense of their surroundings once the Humvee doors swing open and they aren't behind a computer screen anymore.[91]

The list of apps above is only a sampling of those available today to the front-line soldier through the use of a smartphone device. This list demonstrates the functionality and utility of the available apps and sparks the imagination as to what can be developed to support the combatant in either an administrative or operational role with future developmental efforts. With this insight into what is feasible from a technology perspective, it is now time to analyze these technological efforts in light of military efforts to advance the network society through the concept of power to the edge to empower the front-line soldier to achieve self-synchronization.

LINK TO THEORY

Chapter 2 introduced the concept of the network society where networks form the basis of society and the network itself begins to shape the ideas and people who comprise the network. The five critical characteristics of the network society are:

- Information forms the raw material for productivity and power;
- Pervasiveness of the effects new technologies have on humans and society;
- The ability of networks to morph or change to adapt to changing situations;
- Flexibility of the networks such that process and organizations can be profoundly changed by simple reorganization of constituent parts; and
- Collapsing of information age technologies into a single highly integrated system.

---

[91]Spencer Ackerman. "Unleash the iPads of War! Military Maps Now Apps," *Danger Room: Wired* (26 October 2010). http://www.wired.com/dangerroom/2010/10/tracking-the-bad-guys-yeah-theres-an-app-for-that/; Internet; accessed 29 January 2012.

These characteristics of the network society are embodied within the military construct of power to the edge whereby individuals at the edge of an organization like front-line soldiers are empowered by expanding access to information and eliminating unnecessary restraints. This empowerment encourages the sharing of information such that a common shared situation awareness is achieved, thus fostering information superiority and the ability of edge entities to self-synchronize their activities to improve the efficacy and efficiency of soldiers on the modern day battlefield.

New media was then defined to distinguish it from old media in that new media encompasses not only the creation of the message but the use of digital technologies to distribute it as well. The four characteristics of new media are:

- Pervasiveness and ubiquity;
- Instantaneous connectivity;
- Social connectivity; and
- Interactive communications.

The culmination of the characteristics identified within the concepts of network society, power to the edge and new media are embodied within the US military's efforts to implement smartphone devices and technologies within the administrative and operational working environment. Smartphones by their very nature and design are new media devices. Taking these devices and reviewing the Physical Training Program app in the administrative world or the SoldierEyes app in the operational world, both of these apps (or any other on the list provided earlier) encompass the tenets of network society and power to the edge. These apps by their very nature focus on the sharing of information to empower the front-line soldier in the performance of his daily tasks. The pervasiveness of the technology, the flexibility of the network to

reconfigure as required to meet the task at hand by adding or deleting users whenever needed and the ability to create a common shared situational awareness are evident in the design of these apps. Their use creates a common shared situational awareness down to the lowest possible level which in this case is the soldier who is the edge entity. This common shared situational awareness creates a sphere of information superiority and further empowers the soldier to self-synchronize his efforts with others to achieve his commander's intent. Thus, the implementation of smartphone technologies is an embodiment of the power to the edge concept.

With this understanding, the question becomes one of whether or not Canada should embark on a similar endeavor. The following section details how Canada should capitalize on US efforts to implement similar technologies within military administrative and operational environments.

DND/CF IMPLEMENTATION APPROACH

Canada's proximity and long standing relationship with the United States has created many similarities between both societies, especially when considering the information age and utilization of information technology in everyday life. North American technology has permeated every aspect of Canadian and American society and has fostered the already discussed network society. This network society construct has fostered a power to the edge approach within the US military and is encouraging a similar approach within a Canadian context. Furthermore, the close military alliance between the two nations requires significant interoperability between weapon systems, organizations and communication systems. The benefits of empowering front-line soldiers with new media capability through the implementation of smartphone technologies and desire to support interoperability between the

two nations encourages a Canadian adoption of smartphone technologies in a military environment.

Canada has a long standing relationship with the US for combined operations, exercises and shared research and development. Canada's involvement with the F35 Joint Strike Fighter (JSF) program is a testament to Canada's close working relationship with its US allies in the development of defence technologies and capabilities. This close relationship can be leveraged with the US in the introduction of smartphone devices and technologies. The technological solutions and organizational constructs developed through the implementation of both phases of the CSDA project within the US Army can be ported into a Canadian context which contains similar organizational constructs and technology implementations with existing Canadian network systems.

The CSDA two phase approach to implementing smartphone technologies first in the administrative environment and then within the operational environment is an excellent approach for a Canadian implementation. The introduction of these technologies within the administrative environment would form phase one of the implementation and will enable Canada to work out the technical, procedural and organizational issues that are encountered through a Canadian trial of the technologies. Experimentation with various apps, organizational constructs and devolution or empowerment down to the lowest possible level can be experimented with for various administrative tasks.

Phase two of the implementation would then focus on the operational environment. The lessons learned in phase one could be extrapolated into the operational environment where the power of these technologies can provide an edge for the warfighter. Security concerns are significantly higher during phase two of the implementation; however, these issues are being

addressed by the US military at this time. The lessons learned by the US implementation can be ported to Canada for the Canadian implementation. The CF can maximize its efficacy and efficiency by implementing a two phased approach for smartphone technology integration within the CF. Furthermore, the CF will be able to realize the concept of power to the edge which will support shared situational awareness and empower front-line soldiers to self-synchronize their actions. The security issues regarding OPSEC and IP are not trivial and need to be addressed. These issues will be discussed in further detail in the following chapter.

CHAPTER SUMMARY

It is important to analyze existing trials to incorporate smartphones and associated technologies within a military environment to support the idea of doing the same within the CF. Therefore, this chapter started by analyzing failed attempts for militaries to develop unique solutions to military requirements to support the idea of implementing COTS solutions within a military environment. The US trial case study was then presented to demonstrate both the feasibility and power associated with implementing this technology both in administrative and operational environments. Various apps were highlighted to further support the utility of the implementation of these technologies and linking the implementation of this information technology to the theoretical underpinnings of network society and power to the edge. The demonstrated utility and linkage supports the concept of conducting a similar introduction of these technologies in a two phased approach within the CF, first in the administrative and then within the operational environment. This implementation will empower edge entities within the CF as far down as the individual soldier to achieve shared situational awareness and enable self-synchronized activities.

With the understanding of the power and utility of smartphone introduction within the CF, the next chapter will provide an overview of the various OPSEC and IP concerns that these technologies represent and various mitigation strategies that are available to overcome them. Through the analysis of these concerns and mitigation strategies, it will be demonstrated that although challenges exist, they are not insurmountable and the benefits associated with these technologies far outweigh the risks.

CHAPTER 4

INFORMATION ASSURANCE CHALLENGES

Chapter 3 analyzed the introduction of smartphones and associated technologies within the US military environment to demonstrate both the feasibility and power associated with implementing this technology within an administrative and operational military working environment. Various apps were highlighted to foster thought as to the possibilities that can be opened up through empowerment of the front-line soldier with an introduction of this capability down to his level. This empowerment fosters the creation of a shared situational awareness and provides an avenue for self-synchronization of edge entities. However, the introduction of these technologies is not without controversy. There are various OPSEC and IP concerns that these technologies potentially introduce and which must be overcome if the introduction of smartphones within the CF is to be successful. This chapter will provide an overview of OPSEC and IP within a CF context, focusing on those issues that are relevant to smartphones and the mitigation measures that are available to overcome these issues. Through the analysis of these concerns and mitigation strategies, it will be demonstrated that the benefits associated with smartphone technologies far outweigh the risks, especially if proper technologies and procedures are incorporated with their implementation.

This chapter will start by introducing the concepts of IP and OPSEC within a CF context. Details regarding various concerns specific to smartphones will then be introduced as they relate to IP/OPSEC issues. Concerns with viruses, hacking, GPS tracking and other privacy problems will be explored from a military environment perspective. The specific example of the use of smartphone technologies in the 2006 Israeli-Hezbollah War in Lebanon will provide concrete examples of these concerns within a modern day conflict. Once an understanding of the

concerns is laid out, various encryption standards and technologies will be introduced to demonstrate that security concerns can be addressed through the appropriate application of encryption technology. With an understanding of these mitigation measures, the CF's stance towards the current Blackberry implementation will be compared to that of the RCMP. This comparison between like-minded Canadian organizations will demonstrate that there is the possibility of exploring additional functionality with today's technology even within our existing IP/OPSEC envelope. This comparison will point out that it is possible for the CF to open up the use of new media technologies with appropriate training and guidance provided to the end-user. This "guidance" will be discussed further by discussing proper training and ROEs that can be provided to users so that they are educated in the manipulation of information to comply with IP/OPSEC concerns. By the end of the chapter, it will be argued that through the use of appropriate mitigation strategies, the employment of smartphone technologies within the CF is both desirable and achievable.

INFORMATION PROTECTION / OPERATIONAL SECURITY

The CF Information Operations (IO) publication B-GG-005-004/AF-010 defines defensive IO as consisting of three elements:

- Offensive Protect: the control of adversary access to those friendly elements of the information environment that are critical to the accomplishment of friendly objectives,
- Defensive Counter-IO: the counteraction of adversary IO attacks and the restoration of the performance and functionality of critical friendly elements, and
- Offensive Counter -IO: the deterrence or neutralization of adversary IO capability.[92]

It further states that "Information Protection (IP) is a combination of the first two elements. The last element is necessary to deter adversary intent to employ IO and exploit and/or neutralize

[92]Department of National Defence, *B-GG-005-004/AF-010 CF Information Operations*, 3-1.

adversary IO capability and opportunity, either preemptively or as a response."[93] Essentially, IP protects the information environment through controlled access for friendly forces while denying access to adversary forces. The CF IO publication further defines IP as:

> IP protects and defends information and information systems by ensuring their availability, integrity, and confidentiality. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IP focuses on the technical capabilities and processes such as multilevel security, firewalls, secure network servers and intrusion detection software, as well as related physical, personnel and procedural security measures (e.g. the measures taken to safeguard cryptographic equipment and material from unauthorized access).[94]

IP is thus a combination of technical and procedural measures to ensure the confidentiality, integrity and availability of information and information systems for friendly forces. IP is the incorporation of mitigating measures to reduce risk of compromise of information to an acceptable level to allow the utilization of technology in the conduct of military operations. Reduction of risk to an "acceptable level" is crucial as risk cannot be completely eliminated. It is through the judicious understanding of risk and risk mitigation that the use of information technology can be successful. The technical and procedural measures relevant to smartphone technologies will be discussed later in this chapter.

The same CF IO publication defines OPSEC as:

> OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:
> a. Identify those actions that can be observed by adversary intelligence systems.
> b. Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful.
> c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.[95]

---

[93]Ibid., 3-1.

[94]Ibid., 3-1 - 3-2.

[95]Ibid., 2-2.

It further states that:

> OPSEC's most important characteristic is that it is a process. OPSEC is not a collection of specific rules and instructions that can be applied to every operation. It is 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. The TFC should provide OPSEC planning guidance to the staff at the time of the commander's intent and, subsequently, to supporting commanders in the chain of command. By maintaining liaison and coordinating the OPSEC planning guidance, the TFC will ensure unity of effort in gaining and maintaining the essential secrecy considered necessary for success."[96]

The statement above highlights the concept of OPSEC being a process whereby guidance or commander's intent is provided throughout the chain of command regarding maintaining "essential secrecy" for success. Satisfactory OPSEC to guarantee "essential secrecy" is achieved when a commander provides direction regarding the management of information which can be understood and followed by all levels of the military organization. This direction can come in the form of training and the provision of ROE's on information sharing and use.

IP and OPSEC concerns must not be used to place unnecessary restrictions on the implementation of new technologies. As Lieutenant-General Caldwell, commander of the US Army's Combined Arms Centre points out:

> Operational security is an enduring concern for military operations. However, we cannot take counsel of our fears at the expense of new media applications. As always, we must strike a balance between caution and engagement. As new technologies continue to emerge, there will be even more challenges to the risk/benefit balance. If we surrender to our fears, we surrender a big chunk of the high media ground. Commanders accept risk in any operation. We are not talking about rejection of risk, but rather about the parameters of the risk we're willing to accept. With the emphasis senior leaders are placing on Web 2.0, I remain confident the Army will find the proper balance."[97]

---

[96]Ibid., 2-2 - 2-3.

[97]Anton Menning. "Lieutenant General William B. Caldwell IV on New Media in Military Operations: An Interview with Commander of the US Army's Combined Arms Center and Fort Leavenworth Kansas," *IO Sphere* (Summer, 2009): 25.

Lieutenant-General Caldwell rightly points out that there must be a balance between caution and engagement through the use of new media. This balance will empower the front-line soldier while placing appropriate restrictions on his use of new media to meet operational concerns. The following section provides additional detail regarding the existing vulnerabilities inherent in the implementation of smartphone technologies.

Existing Vulnerabilities

Smartphones, like any electronic computing device, is a combination of hardware and software combined together to provide specific functionality. The software is the logic that is placed within the computing device to provide the desired functionality. There is significant complexity in today's software used on computing devices. This complexity can be exploited by a malicious individual to inject unintended actions or consequences within the software code loaded on a device unbeknownst to the user. These vulnerabilities form the heart of the concerns military's have regarding the implementation of computing devices within a military environment. The size, mobility and computing power of smartphones in particular cause angst amongst military officials as the potential for loss or compromise is seen as far greater than traditional computing infrastructure located at static locations within military locations. The following provides a sampling of the various vulnerabilities that exist with smartphones and smartphone technologies.

The iPhone is one of the most popular smartphones on the commercial market today and is one of the products being trialed by the US military. Some of the security concerns associated with the use of an iPhone were outlined by Amber Hunt in a review of potential forensics applications for law enforcement officials. These concerns were:

- Every time an iPhone user closes out of the built-in mapping application, the phone snaps a screenshot and stores it. Savvy law-enforcement agents armed with search warrants could use those snapshots to see if a suspect is lying about whereabouts during a crime.
- iPhone photos are embedded with GEO tags and identifying information, meaning that photos posted online might not only include GPS coordinates of where the picture was taken, but also the serial number of the phone that took it.
- Even more information is stored by the applications themselves, including the user's browser history. That data is meant in part to direct custom-tailored advertisements to the user, but experts said that some of it could prove useful to police.[98]

The same information or concerns expressed in a law enforcement environment holds true in a military environment. The GEO tags and GPS information stored on a smartphone or being transmitted by a smartphone's GPS transmitter[99] is attractive information to an adversary tracking the movements of friendly forces. Further, the browser history on a smartphone can provide valuable information regarding current plans and intentions that would assist an adversary in countering blue force efforts. iPhone technology potentially records a wealth of information about a military unit that can be utilized against a military force should an adversary obtain access to a soldier's misplaced iPhone.[100]

The above vulnerabilities highlight the problems associated with the storage of information on a smartphone device that could be exploited should the device be recovered by an adversary. Data storage; however, is not the only concern. There are concerns regarding the use of the device itself through the utilization of apps that manipulate the data on the smartphone.

---

[98]Amber Hunt. "iPhone Makes Great Snitch for Savvy Cops," *Physorg.com* (1 September 2010). http://www.physorg.com/news202568188.html; Internet; accessed 29 January 2012.

[99]. "Securing Smartphones in Battle," *Homeland Security News Wire* (13 October 2011). http://www.homelandsecuritynewswire.net/securing-smartphones-battle; Internet; accessed 29 January 2012.

[100]Christian. "iPhone Could be Cracked by Terrorists and Cops," *Military.com: KitUp* (7 September 2010). http://kitup.military.com/2010/09/iphone-could-be-cracked-by-terrorists-and-cops.html; Internet; accessed 29 January 2012.

The major concern revolves around the injection of a Trojan program onto a smartphone device. Trojans are software programs that perform both a desired function that is expected by the user and a covert function that is unexpected and unknown to the user. As has already been mentioned, there is a wealth of information stored on a smartphone. If a Trojan app were to be loaded on a soldier's phone, valuable information could be surreptitiously leaked to an adversary.[101] Professor Xuxian Jiang from North Carolina State University has reported a number of apps that "contained highly stealthy code that collected users' browsing history, bookmarks, and device information and sent them to servers under the control of the attackers."[102] These apps were able to collect login credentials for popular social media sites or take control of the communications portion of the smartphone unbeknownst to the user.

In addition to the challenges associated with Trojan apps, additional malware (malicious software) loaded on a smartphone could potentially allow a hacker or in a military context, an adversary, to launch an attack on friendly networking infrastructure. That attack could come in the form of an attempt to disrupt communication signals in a given area by disrupting cell tower capabilities. Other possibilities include the creation of "botnets" which is a grouping of remotely controlled computing devices that have been formed into a malicious network designed to disrupt friendly networking capabilities and communications.[103] The key to a successful attack

---

[101]Bruce Schneier. "Android Malware," *Schneier.com: Schneier on Security* (25 November 2011). http://www.schneier.com/blog/archives/2011/11/android_malware.html; Internet; accessed 29 January 2012.

[102]Dan Goodin. "Toxic Plankton Feeds on Android Marked for Two Months," *The Register: Malware* (13 June 2011). http://www.theregister.co.uk/2011/06/13/android_market_still_insecure/; Internet; accessed 29 January 2012.

[103]Colin Clark. "Smartphones: The Next Security Gap," *DoD Buzz* (23 February 2011), http://www.dodbuzz.com/2011/02/23/smartphones-the-next-security-gap/#ixzz1Eq4lTrVI; Internet; accessed 29 January 2012.

for either Trojans or malware is the authorized installation of software on the smartphones that have access to data stores and communication capabilities of the devices.

Mitigation of smartphone vulnerabilities, either physical access to the phone to access data stores or malicious software loaded onto the smartphone, is through the judicial application of IP technologies and procedures. The US Army's attempt to overcome the issue of malware revolves around the introduction of the COE and Army Marketplace introduced in Chapter 3. The Army's COE provides the software development environment to enable secure and interoperable apps to be developed while the Army Marketplace provides the secure apps distribution point for end-users. By restricting smartphones to accessing only the Army Marketplace which stores approved apps free from malware developed in a controlled environment provides a certain level of guarantee as to the integrity of software deployed within the military environment. In addition, the incorporation of appropriate encryption technologies for data storage and communication between devices is seen as a key enabler to resolve adversary access to information stored or transmitted by the smartphone.[104] Proposed encryption standards and technologies along with ROEs directing user management of information will be discussed later on in this chapter.

The list of vulnerabilities above is a sampling of those existing today. This list demonstrates the breadth of vulnerabilities and highlights the areas which must be addressed to mitigate these vulnerabilities. Prior to discussing these mitigation strategies, it is beneficial to provide specific examples of the use of smartphone technologies in the 2006 Israeli-Hezbollah War in Lebanon to further highlight how the concerns of IP and OPSEC can be realized in a modern day conflict.

---

[104]. *Is it Smart for the US Army to Develop Smartphones?*

2006 Israeli-Hezbollah War

The 2006 Israeli-Hezbollah War in Lebanon demonstrated both the positive and negative effects associated with the use of smartphone technologies and new media. The positive aspects were generally experienced by the Hezbollah whose intelligent use of new media maximized their effectiveness and furthered their strategic goals at the expense of the Israeli's. The negative aspects were generally experienced by the Israeli Defence Force (IDF) whose lack of training and provision of ROE's to soldiers resulted in serious OPSEC violations that impacted tactical through strategic goals throughout the conflict. The negative effects of improper use of new media will be discussed first so as to emphasize the concerns already expressed regarding IP and OPSEC within this new environment.

First, IDF did not have a policy in place to deal with personal use of smartphones within the Area of Operations (AOR). With the AOR covered by Israeli service providers, it became standard practice for IDF soldiers to bring personal electronic devices within the AOR and use them as they saw fit. There was no provision of training or ROEs on the proper management of information such that they were used to make calls, send instant messages and take pictures of their surroundings. These actions had two effects on the course of the conflict. First, IDF soldiers would call home and often revealed details of an operational nature that would make its way to mainstream media and websites. These OPSEC violations would impact operations within the AOR. Soldiers were also capable of regularly blogging their comments and concerns. When the IDF experienced increasing difficulties to sustain forces with sufficient material, the soldiers expressed their frustrations on these blog sites. This had a negative effect regarding the morale of the IDF units involved and caused negative public opinion against the political leadership that was already struggling with negative public opinion regarding Hezbollah rocket

attacks in the North and the displacement of the population. The lack of direction provided by the chain of command resulted in negative strategic effects for this conflict.

Second, there is indication that Hezbollah used Open Source Intelligence (OSINT) through the targeting of Israeli media and websites and Signals Intelligence (SIGINT) by tracking the personal cell phones that were brought into the AOR by IDF soldiers. There are signs that Hezbollah used real time OSINT from Israeli press releases along with Google Earth mapping capabilities to plot planned rocket attacks within Israel. The effective use of OSINT with available COTS tools significantly improved the effectiveness of these attacks.

From a SIGINT perspective, the SIGINT information was used in two ways. First, Hezbollah forces were able to report IDF casualties quicker and more accurately than IDF forces which questioned IDF credibility. A negative public perception was created which once again impacted the strategic will of the Israeli population to continue with the conflict. Second, Hezbollah forces were able to determine the location and disposition of IDF forces which allowed them to track these forces and conduct operations that were less favourable to the IDF. It is believed that this SIGINT capability was not restricted to the COTS devices taken into theatre by IDF soldiers. There are unconfirmed reports that the IDF's Mountain Rose tactical cellular communication system may have been compromised which would have provided additional operational details in which to plan Hezbollah attacks.[105] These deficiencies in both IP and OPSEC had a very negative impact on Israeli operations within Lebanon and demonstrate the challenges associated with smartphone technologies in a military environment.

Having reviewed the negative aspects of new media in a combat environment, it is important to review some of the real world positive examples that can be achieved. These

---

[105]Collings and Rohozinski, *Bullets and Blogs: New Media and the Warfighter*, 74-75.

positive results were a product of effective use of new media by Hezbollah forces. Hezbollah has fully embraced new media in all aspects of its political, military and social organization. They have truly embraced the concept of the network society and are leveraging power to the edge for their military forces to maximize their effectiveness. Their embrace of power to the edge is partially a result of their military limitations compared to their opponent which forces them to focus on strategic informational effects.

This focus has forced them to possess the largest media organization in the Middle East with an ability to reach 200 million viewers via satellite broadcast. More importantly, their reach has become truly global through their use of associated web sites, blogs, YouTube videos and social media sites. In addition, Hezbollah has dedicated software development teams to create first-person shooter video games to reinforce their message with the younger population and build a warrior ethos amongst their target audience. With this focus on using new media to promote strategic messaging, Hezbollah forces quickly and accurately reported combat incidents through the use of smartphone technologies and new media to the world public in a manner that supported their message. Gruesome pictures of Israeli destruction were packaged and released to the press along with postings to blogs and photo-sharing sites. Graphic videos were packaged and distributed via YouTube to question the credibility of Israeli actions. Finally, Lebanese bloggers actively disseminated real time information and pictures of Israeli actions which impacted operations and undermined the political will to continue the combat operation.[106] All of these actions demonstrate the power that can be leveraged with smartphone technologies should they be utilized effectively by a military organization.

---

[106]Ibid., 81-84.

With these real world examples provided to highlight the potentials and vulnerabilities associated with the use of smartphone technologies in a military environment, it is now time to review potential encryption technologies for data storage and communication between smartphone devices. These encryption technologies are seen as a key enabler to resolve adversary access to information stored or transmitted by smartphone devices.

ENCRYPTION

Encryption of data stored on a smartphone and encryption of communication channels between smartphones and base stations is seen as a key enabler to resolve IP and OPSEC concerns. Appropriate encryption would deny an adversary access to the information that is being used and shared by smartphone devices and allow for their effective use in an area of operations. This concern regarding security is recognized as the biggest challenge to the incorporation of smartphones in an operational environment. Within the US Army, it is recognized that "Army communication devices currently require NSA Type 1 encryption, but adding this to an Army smartphone would add considerably to the expense and reduce the availability."[107] How to get around this challenge becomes a key consideration.

The first point of discussion is the mandated use of NSA Type 1 encryption technologies. Type 1 or Suite A encryption technologies are military developed secret encryption algorithms that are developed and maintained by NSA. Few vendors are authorized to access these algorithms and develop products that meet NSA Suite A encryption standards. Further, the market is restricted to military clients approved by the US government and so the cost associated with developing smartphones with this capability would be extensive. This challenge has been recognized by NSA; thus NSA has begun reviewing private industry unclassified encryption

---

[107]. *Is it Smart for the US Army to Develop Smartphones?*

algorithms that they can verify and certify for use within deployed military systems. These private industry unclassified encryption algorithms are labeled as Suite B and are considered appropriate for use for secret and below sensitive information that has a short life span before becoming unclassified. Tactical level position reports and information sharing conducted by front-line soldiers in an operational area falls within these parameters. The defence company Thales has developed a "Suite B-certified COTS programmable crypto processor in the Thales Rifleman radio, which is a handheld software-defined radio for infantry soldiers that complies with the DOD's Joint Tactical Radio System (JTRS)."[108]

Another area being explored by NSA is the implementation of a layered COTS solution which is also called Commercial Solutions for Classified (CSFC). CSFC's approach is to layer different vendor's security products on top of each other to provide a solution that is considered sufficient once again to protect secret information. This solution is ideally situated to resolve encryption requirements for smartphones. The intent would be to "make the phone so it can be used in secret, and perhaps even top-secret communications using standard Android stack and protocols, and come up with Suite B-compliant VPN and secure voice capability."[109] Efforts to explore commercial solutions have resulted in requests for additional research by the defence community to secure data stored in Commercial Mobile Devices (CMDs):

> The primary purpose of this RFI is to discover new technologies and methods to support full disk and system encryption of the CMDs (specifically Apple and Android platforms) to include a pre-boot environment to load the operating system. The solution must use an AES-256 bit encryption algorithm compliant with FIPS 140-2 as published by the National Institute of Standards and Technology (NIST).[110]

---

[108]Keller, *Military Crypto Modernization Leads to Applications Like Smartphones, Tablet Computers on the Battlefield*

[109]Ibid.

The US government is recognizing the utility of commercial encryption solutions and exploring them more fully for their eventual implementation in smartphones.

With NSA's willingness to consider Suite B and CSFC encryption solutions, the possibilities for smartphone encryption expand significantly. Commercial solutions already exist or are being developed. CellCrypt, Inc. has developed a secure voice calling app for Android-based smartphones, iPhones and Blackberry's. This secure voice app uses two NSA Suite B approved encryption algorithms. The Blackberry app has an additional feature of encrypting secure messaging. This encryption solution is approved for encrypting sensitive but unclassified information.[111] Another leading software security company, Symantec Corporation, is in the process of developing a product called O3 that will be able to provide secure communications for military wireless networks.[112] These products demonstrate the ability of industry to provide appropriate encryption technologies today that can be used in a military environment. Furthermore, these encryption technologies resolve the problem associated with adversary access to information stored or transmitted by smartphone devices.

With an understanding that encryption exists today to resolve some of the concerns associated with the implementation of smartphones in a military environment, it is now time to take a closer look at the CF's current implementation of Blackberry compared to the RCMP. This comparison will demonstrate that there is a possibility of exploring additional functionality

---

[110]Defense Advanced Research Projects Agency. "Request for Information (RFI) for Full Disk Encryption Method for Commercial Mobile Devices," F*ederal Business Opportunites*. https://www.fbo.gov/index?s=opportunity&mode=form&id=3473e17cb0615b10d9c93533180aa345&tab=core&tabmode=list&=; Internet; accessed 29 January 2012.

[111]Sharon Hess. "Smartphone Encryption App Helps Sensitive Information Get More Secure: Interview with Ian Meakin, VP of Marketing at Cellcrypt, Inc." *Military Embedded Systems* (September 2011). http://www.mil-embedded.com/articles/id/?5349; Internet; accessed 29 January 2012.

[112]Hennigan, *Taking iPads into Battle*

with today's technology even within our existing IP/OPSEC envelope. This can lead the way to looking at smartphone technologies within a military environment.

RCMP BLACKBERRY IMPLEMENTATION COMPARISON

Blackberry technology has been available within the public domain for some time. The ability to send emails, view webpages, view documents, send instant messages and use the cell phone feature of the Blackberry is a significant productivity tool that is utilized in the corporate domain. The CF has recognized these benefits through its implementation of Blackberry functionality within the Defence Wide Area Network (DWAN). However, the CF's implementation has placed restrictions on the implementation of Blackberry technology so that access to the Internet is severely restricted to limited sites approved in advance by IP professionals and a complete ban on the use of Blackberry Messenger (BBM). These restrictions have been incorporated due to IP concerns regarding unrestricted access to the Internet and the inability to log and track BBM conversations. The CF's IP concerns have thus restricted the functionality of these devices.

The RCMP is a like-minded Canadian police organization that has strict regulations concerning the handling of sensitive and/or classified information in the conduct of their day-to-day business. The RCMP has also recognized the benefits associated with Blackberry technologies and have implemented these devices within their administrative networking environment, similar to that which has been done within the CF. As the RCMP have pointed out to their staffs:

> Blackberry smartphones can provide productivity and usable benefits for various business-related tasks. Nevertheless, the flexibility of smartphones incurs organizational risk by providing new ways to compromise sensitive information. Consequently smartphones require specialized security safeguards and usage restrictions within the RCMP.[113]

They have recognized the utility of these devices and the requirement for safeguards associated with their use as has the CF. These "safeguards and restrictions" have come in the form of direction to staff using these devices to restrict "all voice communications…to non-sensitive information" and that they are "approved for Formal RCMP Business up to and including Protected 'A' information only."[114]

The culture of empowering staff with the necessary tools to conduct their daily activities with appropriate direction regarding the use of these tools is evident within the RCMP. This culture has allowed the RCMP to recognize the benefits associated with BBM and empowered this organization to authorize its use with similar "safeguards" as stated for the use of Blackberry's. They have stated that "Blackberry Messenger (BBM) is now approved for registered RCMP corporate BES smartphones."[115] Further, they have provided direction on the use of BBM by stating that "Blackberry Messenger (BBM) conversations are not logged and tracked; be attentive to the information that you share over BBM."[116] The RCMP has provided the appropriate guidance to their staff to use the tools provided to them to maximize their effectiveness.

The difference between Blackberry usage between the CF and the RCMP is not staggering; however, it provides insight into the possibilities that the CF can explore when investigating smartphone technologies. The heart of the CF's reluctance to embrace these

---

[113]S/Sgt Craig O'Neill. "Blackberry / Smartphone Usage," http://infoweb.rcmp-grc.gc.ca/kdivision/broadcasts/2011/111021-bb-smartphone-eng.htm; accessed 23 January 2012.

[114]Ibid.

[115]Ibid.

[116]S/Sgt Rick McIntyre. "Checklist for Corporate Blackberry Users," http://infoweb.rcmp-grc.gc.ca/odivision/news-nouvelles/oenews-infoenligne/2011/11-11-...; accessed 23 January 2012.

technologies rest in the IP and OPSEC concerns that these devices represent. By comparing the CF with the RCMP which are both Canadian government organizations that have similar concerns regarding the sharing and handling of sensitive information, CF options become possible. The CF can explore the use of new media technologies with appropriate training and guidance provided to the end-user. A discussion regarding appropriate training and ROEs will be provided next.

USER TRAINING AND RULES OF ENGAGEMENT

A smartphone is a tool just like a weapon is a tool that can be used by a soldier. Like any tool provided to a soldier, appropriate training and Rules of Engagement (ROEs) are provided so that the soldier can be trusted to use the tool in an approved manner. Militaries are more than willing to provide tools of death and destruction to a soldier with the understanding that they have been properly trained and provided sufficient direction to know when and where to apply these tools. This training and direction does not remove the risk of inappropriate use. However, it is understood and accepted that through the training and direction provided, the risk is reduced to an acceptable level to conduct operations. In essence, the benefits outweigh the risks. The same can be said for new media and smartphones.

This recognition of the benefits associated with new media was realized by the US DoD when they reversed a ban on accessing social media websites and tools on 26 February, 2010:

> "A new policy released today by the Pentagon has reversed multiple bans on social media websites and tools, effective immediately. This policy includes YouTube, Facebook, MySpace, Twitter, Google Apps and other social tools… The change only affects the military's non-classified Internet network, known as NIPRNET. It also gives commanders at all levels leeway in temporarily banning specific social tools. In other words, you can expect some commanders to reinstate some of these bans for security reasons."[117]

---

[117]Ben Parr, "New U.S. Military Policy Opens Up Social Media to the Troops," *Mashable: Social Media* (26 February 2010). http://mashable.com/2010/02/26/military-social-media/; Internet; accessed 29 January 2012.

This new policy is recognition of the benefits associated with these sites as they allow military units to share information, boost morale and strengthen relationships with the public. This policy is not without restriction as it still provides flexibility to commanders to instill restrictions as required for security reasons on a case-by-case basis.

As has already been mentioned, the provision of a tool requires the provision of appropriate training and guidance on the use of the tool for it to be effective. Training and education is the first step towards empowering a soldier in a tool's use. The US Army has recognized the requirement to provide appropriate training on the use of new media in a controlled environment. The US Army Command and General Staff College dictate that all students must blog as a requirement for graduation and have founded a blog library to facilitate access and training in this area. Within its curriculum, instructors provide students with a basic understanding of new media technologies and the nuances of social media. All students are required to write a paper discussing the advantages and disadvantages of allowing soldiers access to new media technologies and they explore how the US military can exploit new media to engage the American public. YouTube, Twitter and Facebook pages are created and updated on a regular basis and wikis are used to disseminate reference material to students and encourage collaboration at all levels throughout the institution.[118] This training regimen can be exported to a CF environment where the same understanding of the possibilities and benefits associated with new media and smartphones can be imparted on Canadian soldiers.

With an appropriate understanding of how to use new media tools including smartphones, there is a requirement to provide direction on the limits of their use. In the context of the US

---

[118]Menning, *Lieutenant General William B. Caldwell IV on New Media in Military Operations: An Interview with Commander of the US Army's Combined Arms Center and Fort Leavenworth Kansas*, 26-27.

policy of allowing access to social media sites, there was a need to provide direction on their use to maintain OPSEC. For example, the US Army has provided direction on soldier's use of Facebook by providing the following guidance:

- Adjust privacy settings to "private" or "friends only."
- Remove any personally identifiable information that gives away too much information about you or your family.
- Avoid sharing details about bases and capabilities by not posting photos of or details about formations, quarters, armored vehicles, and/or weapons.
- Disable the GPS feature on your mobile device or turn off tagging or tracking applications on your Facebook account that give your exact location.
- Educate yourself, your friends and your family about what is and isn't safe to share on Facebook or any other social networking platform.[119]

This guidance provides the necessary detail to allow the soldier to use the tool in such a way as to maintain OPSEC while empowering him to do his job. Risk has not been eliminated but it has been managed and reduced to an acceptable level. The guidance that we see in the realm of social media direction can be extrapolated into the world of smartphone use. Furthermore, this guidance can be exported into a Canadian context to work for the CF's introduction of smartphones. The principles are the same.

With the provision of appropriate training and guidance, it is possible to reduce the risk of OPSEC incidents to an acceptable level. This reduction of risk creates an environment where the employment of smartphone technologies within the CF is both desirable and achievable.

CHAPTER SUMMARY

The introduction of smartphones within the CF opens up significant possibilities for empowering front-line soldiers in the conduct of their day-to-day activities. Their ability to self-synchronize their activities increases the efficiency and effectiveness of a military organization.

---

[119]Ashley Fowler. "Facebook: Please Use Responsibly," *United States Army* (24 January 2012). http://www.army.mil/article/72387/Facebook__Please_use_responsibly/; Internet; accessed 29 January 2012.

However, these smartphones with their associated new technologies introduces vulnerabilities and concerns from an IP and OPSEC perspective. This chapter defined IP and OPSEC from a CF perspective and introduced those vulnerabilities specific to smartphones that relate to these concerns. Using the 2006 Israeli-Hezbollah War and RCMP Blackberry implementation as real world examples of the implementation of smartphones, this chapter was able to identify encryption, user training and the provision of ROEs as mitigating measures to overcome the CF's IP and OPSEC concerns. The benefits associated with smartphone technologies far outweigh the risks, especially if proper technologies and procedures are incorporated with their implementation.

With an understanding of the capabilities and challenges associated with smartphone implementation, the idea of a phased approach to introducing this technology within the CF is further supported. By implementing appropriate training and through the provision of sufficient ROE's on their use, smartphones can be implemented in the administrative environment to improve efficiencies and learn how to use them in a non-classified environment. Lessons learned from this implementation can then be ported to the operational environment where additional security measures through encryption would be incorporated to provide a robust, secure solution that would be effective in a hostile environment. Thus, the modern day warfighter would truly be empowered in all areas of responsibility.

CHAPTER 5

CONCLUSION

The information society that we live in today is characterized by the power associated with information. The creation, use, distribution and manipulation of information have become the significant economic, political and cultural driving forces and are the distinguishing features of the information society. With the continued proliferation of information technology and importance of information within the society, the information society is one in which the dominant functions and processes are increasingly manipulated and managed by networks of people. This network society is composed of communication links and nodes which represent the people within the network. The communication links between nodes in the network and membership to the network itself shape the ideas of the people who reside within the network. The five characteristics for the basis of this network society and from which the network society derives its power are:

- Information forms the raw material for productivity and power.
- Pervasiveness of the effects new technologies have on humans and society.
- Networking logic of any system or set of relationships using these new information technologies.
- Flexibility of the networks such that process and organizations can be changed by reorganizing constituent parts.
- Collapsing of information age technologies into a single highly integrated system.

The military has translated this network society concept into the concept of power to the edge where the focus is to create a common shared situational awareness down to the lowest possible level. This shared situational awareness promotes a common understanding which

supports information superiority and empowers self-synchronization of military forces to maximize efficiency and efficacy in military operations. Information technology tools are required to facilitate this shared situational awareness and these technologies can be organized under the heading of new media. New media are the suite of tools and technologies that not only impact the creation and distribution of a message but the organization and society which generate the message along with the message itself. The new media's characteristics of pervasiveness, instantaneous communications, social connectivity and the ability to be interactive support the concept of the network society and power to the edge. It is this understanding of both technology and society that provides the theoretical framework rationalizing the implementation of smartphones and associated technologies within the CF.

To provide an outside perspective as to the utility of implementing smartphones within a military setting, it is useful to review existing efforts from similarly configured military organizations. From a Western military perspective, the US military is in the midst of trialling smartphones and associated technologies within both an administrative and operational military environment. Their CSDA project is a two phase project whereby smartphones are first introduced in an administrative environment to understand and appreciate the utility of these devices and potential for future development as well as working out the technical challenges associated with these technologies. The second phase introduces these smartphones in an operational environment where the focus once again is to understand the utility and potential future development as well as shifting to address security to overcome the concerns regarding IP and OPSEC. The US efforts to create a COE for software / apps development and Army Marketplace for secure apps distribution along with their phased approach to technology implementation demonstrate both the utility and potential for further exploitation of these

technologies. Further, it provides a template to copy within a Canadian context where the introduction of these technologies would be conducted in a similar two phased approach. First, an administrative implementation should be completed to determine the utility of the devices and work out the technical issues, followed by an operational implementation that would focus once again on the utility of the devices but also focus on security concerns. Both implementations will empower edge entities within the CF as far down as the individual soldier to achieve shared situational awareness and encourage self-synchronized activities as envisioned by the power to the edge concept.

Although the introduction of smartphones within the CF opens up possibilities for use, they represent vulnerabilities and concerns from an IP and OPSEC perspective that must be overcome to allow for their effective use in a military environment. The existing smartphone vulnerabilities related to malware and data storage and transmission were reviewed from a CF IP and OPSEC perspective to highlight those issues that are of specific concern to the CF. The real world examples of the 2006 Israeli-Hezbollah War and the RCMP Blackberry implementation identified encryption, user training and the provision of ROEs as mitigating measures to overcome the CF's IP and OPSEC concerns. The benefits associated with smartphone technologies far outweigh the risks, especially if proper technologies and procedures are incorporated with their implementation.

The employment of smartphones within the CF represents an opportunity to embrace the potential associated with the concepts of the network society and power to the edge in a military context. Empowering all levels of the military chain of command right down to the individual soldier has the potential to improve both the efficiency and efficacy of military operations. However, implementing smartphones introduces challenges and fears that need to be overcome

to ensure success. Similar challenges were voiced when the concept of introducing personal computers in a military context was discussed in the 1990's. It was determined at the time that the benefits outweighed the risks and appropriate mitigation measures were put in place to justify the introduction of the PC. The same can and should be said with the introduction of smartphones. To do any less would ignore the benefits that smartphones impart upon a military organization.

BIBLIOGRAPHY

. "Is it Smart for the US Army to Develop Smartphones?" *Defense Industry Daily* (24 February 2011). http://www.defenseindustrydaily.com/military-smartphones-dod-apps-06512/; Internet; accessed 29 January 2012.

. "Securing Smartphones in Battle." *Homeland Security News Wire* (13 October 2011). http://www.homelandsecuritynewswire.net/securing-smartphones-battle; Internet; accessed 29 January 2012.

Ackerman, Spencer. "Air Force Wants to Wear Computers (After Army Took them Off)," *Danger Room: Wired* (10 January 2012). http://www.wired.com/dangerroom/2012/01/air-force-wearing-computers/#more-69068; Internet; accessed 29 January 2012.

———. "Army Hits Pause on 'Wearable Computer' Program," *Danger Room: Wired* (28 July 2011). http://www.wired.com/dangerroom/2011/07/army-hits-pause-on-its-wearable-computer-program/; Internet; accessed 29 January 2012.

———. "Army Taps Android Phones for 'Wearable Computers'," *Danger Room: Wired* (6 September 2011). http://www.wired.com/dangerroom/2011/09/nett-warrior-smartphone/; Internet; accessed 29 January 2012.

———. "Army Wants Low-Level Soldiers Linked into its Data Nets," *Danger Room: Wired* (22 February 2011). http://www.wired.com/dangerroom/2011/02/army-wants-low-level-soldiers-linked-into-its-data-nets/; Internet; accessed 29 January 2012.

———. "First Look: Inside the Army's App Store for War," *Danger Room: Wired* (27 April 2011). http://www.wired.com/dangerroom/2011/04/armys-app-store-for-war/; Internet; accessed 29 January 2012.

———. "Real Men use Android: Special Forces Favor Google Phone," *Danger Room: Wired* (29 October 2010). http://www.wired.com/dangerroom/2010/10/special-forces-want-android-apps-for-warzone-john-maddens/; Internet; accessed 29 January 2012.

———. "Soldiers' Wearable Computers may Get an iPhone Brain," *Danger Room: Wired* (14 April 2011). http://www.wired.com/dangerroom/2011/04/soldiers-wearable-computers-may-get-an-iphone-brain/; Internet; accessed 29 January 2012.

———. "Unleash the iPads of War! Military Maps Now Apps," *Danger Room: Wired* (26 October 2010). http://www.wired.com/dangerroom/2010/10/tracking-the-bad-guys-yeah-theres-an-app-for-that/; Internet; accessed 29 January 2012.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*. Washington, D.C.: Library of Congress, 2001.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2nd ed. Washington, D.C.: Library of Congress, 2000.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command, Control in the Information Age*. Washington, D.C.: Library of Congress, 2005.

AppFence. "Protecting User Data from Android Applications." http://appfence.org/; Internet; accessed 29 January, 2012.

Army News Service. "Smartphones for all 'Makes Sense in Long Run'," *US Army* (28 February 2011). http://www.army.mil/article/52577/; Internet; accessed 29 January 2012.

Axe, David. "Inside the Army's Doomed Quest for the 'Perfect' Radio," *Danger Room: Wired* (11 January 2012). http://www.wired.com/dangerroom/2012/01/army-perfect-radio/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WiredDangerRoom+%28Blog+-+Danger+Room%29&utm_content=Google+Reader; Internet; accessed 29 January 2012.

Bell, Daniel. *The Coming of Post-Industiral Society: A Venture in Social Forecasting*. New York: Basic Books, 1976.

Buckley, Sean. "US Army Runs Smartphone Trial, could See 'Limited Deployment' Later this Year," *Engadget: News* (16 July 2011). http://www.engadget.com/2011/07/16/us-army-runs-smartphone-trial-could-see-limited-deployment-la/; Internet; accessed 29 January 2012.

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

Castells, Manuel. *Communication Power*. New York: Oxford University Press, 2009.

———. *The Network Society: A Cross Cultural Perspective*: Edward Elgar Publisher, 2005.

Cebrowski, Arthur K. and John J. Garstka. "Network-Centric Warfare: Its Origin and Future."January, 1998.

Cebrowski, Arthur K. and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." *United States Naval Institute. Proceedings* 124, no. 1 (Jan 1998): 28-35.

Chadwick, Andrew. *Internet Politics: States, Citizens, and New Communication Technologies*. New York: Oxford University Press, 2006.

Chadwick, Andrew and Philip A. Howard. *Routledge Handbook of Internet Politics* . Abingdon, Oxon.: Routledge, 2009.

Christian. “IPhone could be Cracked by Terrorists and Cops,” *Military.com: KitUp* (7 September 2010). http://kitup.military.com/2010/09/iphone-could-be-cracked-by-terrorists-and-cops.html; Internet; accessed 29 January 2012.

———. “IPhone in the Zone: Yes we can!” *Military.com: KitUp* (12 May 2010). http://kitup.military.com/2010/05/iphone-in-the-zone-yes-we-can.html; Internet; accessed 29 January 2012.

———. “Range it in with Your iPhone,” *Military.com: KitUp* (12 July 2010). http://kitup.military.com/2010/07/range-it-in-with-your-iphone.html; Internet; accessed 29 January 2012.

———. “Will Army Smartphones Kill Net Warrior?” *Military.com: KitUp* (24 February 2011). http://kitup.military.com/2011/02/will-army-smartphones-kill-nett-warrior.html#ixzz1JWOM6eze; Internet; accessed 29 January 2012.

Clark, Colin. “Smartphones: The Next Security Gap,” *DoD Buzz* (23 February 2011). http://www.dodbuzz.com/2011/02/23/smartphones-the-next-security-gap/#ixzz1Eq4lTrVI; Internet; accessed 29 January 2012.

Collings, Deirdre and Rafal Rohozinski. *Bullets and Blogs: New Media and the Warfighter*. Pennsylvania: US Army War College, 2008.

Community Team. "How should Canadians Pay for the Online Surveillance Bill?" *CBC News* (22 February 2012). http://www.cbc.ca/news/yourcommunity/2012/02/how-should-canadians-pay-for-the-online-surveillance-bill.html; Internet; accessed 27 February 2012.

Dauber, Cori E. *Youtube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer*. Pennsylvania: US Army War College, 2009.

Defense Advanced Research Projects Agency. "Request for Information (RFI) for Full Disk Encryption Method for Commercial Mobile Devices." *Federal Business Opportunites*. https://www.fbo.gov/index?s=opportunity&mode=form&id=3473e17cb0615b10d9c93533180aa345&tab=core&tabmode=list&=; Internet; accessed 29 January 2012.

Ewing, Philip. “Army Begins Mobile Phone Experiments,” *DoD Buzz* (6 June 2011). http://www.dodbuzz.com/2011/06/06/army-begins-mobile-phone-experiments/; Internet; accessed 29 January 2012.

———. “The Army's Big Network Experiment,” *DoD Buzz* (14 June 2011). http://www.dodbuzz.com/2011/06/14/the-armys-big-network-experiment/; Internet; accessed 29 January 2012.

Facebook. "Statistics." http://www.facebook.com/press/info.php?statistics/; Internet; accessed 29 January 2012.

Fowler, Ashley. “Facebook: Please use Responsibly.” *United States Army* (24 January 2012). http://www.army.mil/article/72387/Facebook__Please_use_responsibly/; Internet, accessed 29 January 2012.

Goodin, Dan. “Toxic Plankton Feeds on Android Market for Two Months,” *The Register: Malware* (13 June 2011). http://www.theregister.co.uk/2011/06/13/android_market_still_insecure/; Internet; accessed 29 January 2012.

Gow, James, Bernard Fook Weng Loo, and Rachel Kerr. *Military Transformation and Strategy: Revolutions in Military Affairs and Small States* . London, England: Routledge, 2009.

Heininger, Claire. “Smartphones Combine with Tactical Radios to Boost Ground Troops,” *US Army* (9 March 2011). http://www.army.mil/article/53005/; Internet; accessed 29 January 2012.

Hennigan, W. J. "Taking iPads into Battle." *Los Angeles Times* (25 September 2011). http://articles.latimes.com/2011/sep/25/business/la-fi-isoldiers-20110926; Internet; accessed 29 January 2012.

Hess, Sharon. “Smartphone Encryption App Helps Sensitive Information Get More Secure: Interview with Ian Meakin, VP of Marketing at Cellcrypt, Inc.” *Military Embedded Systems* (September 2011). http://www.mil-embedded.com/articles/id/?5349; Internet; accessed 29 January 2012.

Himanen, Pekka. *The Hacker Ethic, and the Spirit of the Information Age* . New York: Random House, 2001.

Hodge, Nathan. “A Combat Zone iPhone? Soldiers have an App for that,” *Danger Room: Wired* (2 March 2010). http://www.wired.com/dangerroom/2010/03/a-combat-zone-iphone-soldiers-have-an-app-for-that/; Internet; accessed 29 January 2012.

———. "Killer App: Army Tests Smartphones for Combat." *The Wall Street Journal* (3 June 2011). http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html; Internet; accessed 29 January 2012.

Hunt, Amber. “IPhone Makes Great Snitch for Savvy Cops,” *Physorg.com* (1 September 2010). http://www.physorg.com/news202568188.html; Internet; accessed 29 January 2012.

Johnson, David E. *Hard Fighting: Israel in Lebanon and Gaza*. Arlington, VA: RAND Corporation, 2011.

Keller, John. “Military Crypto Modernization Leads to Applications Like Smartphones, Tablet Computers on the Battlefield.” Military and Aerospace Electronics (28 November 2011).

http://www.militaryaerospace.com/articles/2011/11/military-crypto-modernization.html; Internet; accessed 29 January 2012.

Knox, MacGregor and Williamson Murray. *The Dynamics of Military Revolution, 1300-2050* . Cambridge, UK: Cambridge University Press, 2001.

Manovich, Lev. *The Language of New Media*, edited by Noah Wardrip-Fruin, Nick Montfort MIT Press, 2003.

———. "New Media from Borges to HTML." In *The New Media Reader*, edited by Noah Wardrip-Fruin and Nick Montfort: MIT Press, 2003.

McIntyre, S/Sgt R. "Checklist for Corporate Blackberry Users." http://infoweb.rcmp-grc.gc.ca/odivision/news-nouvelles/oenews-infoenligne/2011/11-11-...; accessed 23 January 2012.

McLeary, Paul. "Army Looking at New Battlefield Tablets," *Defense Technology: Aviation Week* (20 October 2011). http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3aca34b929-488c-4110-aa43-cfff80b241a2&plckScript=blogScript&plckElementId=blogDest; Internet; accessed 29 January 2012.

———. "Army Putting Smart Phones, Tablets, to the Test," *Defense Technology: Aviation Weekly* (5 July 2011). http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3Ad35b7ee2-dd18-478e-8a05-c2c10800b718&plck; Internet; accessed 29 January 2012.

———. "No iPhones here: More Designs for Networked Soldiers," *Defense Technology: Aviation Week* (15 September 2011). http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a5d493ee3-dba8-41df-be45-55e36a889209&plckScript=blogScript&plckElementId=blogDest; Internet; accessed 29 January 2012.

Menning, Anton. "Lieutenant General William B. Caldwell IV on New Media in Military Operations: An Interview with Commander of the US Army's Combined Arms Center and Fort Leavenworth Kansas." *IO Sphere* (Summer, 2009): 24-27.

Milian, Mark. “U.S. Army may Soon Equip Troops with Smartphones,” *CNN: CNN Tech* (12 July 2011). http://articles.cnn.com/2011-07-12/tech/army.smartphones_1_iphone-and-android-smartphones-windows-phone?_s=PM:TECH; Internet; accessed 29 January 2012.

Miller, Riel. “Rules for Radicals - Setting the Cyber Frontier,” *IntellectualCapital.Com* (1997 – 1999). 1.

Miller, Riel, Michalski Wolfgagn, and Barrie Stevens. *The Promises and Perils of 21st Century Technology: An Overview of the Issues*. France: Organization for Economic Co-operation and Development, 1998.

Mitchell, Paul T. "Digital Anarchy: The Challenge Posed by Information to the Military." Unpublished Paper, Canadian Forces College, Toronto.

———. *Freedom and Control Networks in Military Environments*. Singapore: Institute of Defence and Strategic Studies, 2006.

———. *Ways of Warfare: Western Military Traditions, the RMA and the War on Terrorism*. Toronto, Canada: Canadian Forces College, 2002.

Mitchell, Paul T. *Network Centric Warfare: Coalition Operations in the Age of US Military Primacy* . London: International Institute for Strategic Studies, 2006.

———. *Networks, Coalition Warfare and US Policy: The New Military Operating System*. London, England: Routledge Global Security Studies, 2009.

Murthy, Jaya Deu. "Evolution of the Internet and its Impact on Society." M.A., McGill University (Canada), 2001.

Nguyen, Chuong. “Army Begins Testing Smartphone for use in Combat,” *GottaBe Mobile: Mobile* (3 June 2011). http://www.gottabemobile.com/2011/06/03/army-begins-testing-smartphone-for-use-in-combat/; Internet; accessed 29 January 2012.

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

O'Neill, S/Sgt C. "Blackberry / Smartphone Usage." http://infoweb.rcmp-grc.gc.ca/kdivision/broadcasts/2011/111021-bb-smartphone-eng.htm; accessed 23 January 2012.

Parr, Ben. “New U.S. Military Policy Opens Up Social Media to the Troops,” *Mashable: Social Media* (26 February 2010). http://mashable.com/2010/02/26/military-social-media/; Internet; accessed 29 January 2012.

Parsons, S. Mark. "The Impact of New Media on Military Operations." Masters of Defence Studies, Royal Military College of Canada, 2010.

PC Magazine. “Definition of Digital Convergence.” *PC Magazine* (2012). http://www.pcmag.com/encyclopedia_term/0,2542,t=digital+convergence&i=41316,00.asp; Internet; accessed 29 January 2012.

———. “Definition of New Media.” *PC Magazine* (2012). http://www.pcmag.com/encyclopedia_term/0,2542,t=new+media&i=47936,00.asp; Internet; accessed 29 January 2012.

Perry, Chondra. “Army toTest Smarphones for Offices, Battlefields,” *US Army* (27 May 2010). http://www.army.mil/article/39953/; Internet; accessed 29 January 2012.

Potter, Ned. “Army's New Secret Weapon: The iPad,” *ABC News: Technology* (27 September 2011). http://abcnews.go.com/Technology/smartphones-military-pentagon-tests-apps-androids-iphones-ipads/story?id=14615595#.TxcJJphyRUQ; Internet; accessed 29 January 2012.

Riffee, Mark. “IPads Now Helping Marines Unleash Hell,” *Danger Room: Wired* (16 September 2011). http://www.wired.com/dangerroom/2011/09/death-on-an-ipad/#more-57371; ; Internet; accessed 29 January 2012.

Salcido, Miguel. “Advantages of using Social Media,” *Organic SEO Consulting* (2011). http://www.organicseoconsultant.com/advantages-of-using-social-media/; Internet; accessed 29 January 2012.

SAP.info. “The Pervasiveness of Technology Degrades Personal Responsibility.” *Events* (5 January 2004). http://en.sap.info/the-pervasiveness-of-technology-degrades-personal-responsibility%e2%80%9d/3525; Internet; accessed 29 January 2012.

Schmidtchen, David. *The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military*. Australia: Longueville Media, 2006.

Schneier, Bruce. “Android Malware,” *Schneier.com: Schneier on Security* (25 November 2011). http://www.schneier.com/blog/archives/2011/11/android_malware.html; Internet; accessed 29 January 2012.

Shaidle, Kathy. “Wikileaks' 'Iraq: Collateral Murder' Video "Doesn't show the Broader Picture',” *Examiner.com: Politics* (12 April 2010). http://www.examiner.com/conservative-politics-in-national/wikileaks-iraq-collateral-murder-video-doesn-t-show-the-broader-picture; Internet; accessed 29 January 2012.

Stand-To!. "Connecting Soldiers to Digital Applications." *US Army* (2010). http://www.army.mil/standto/archive/2010/07/15/; Internet; accessed 29 January 2012.

Terrazas, Michael. “Georgia Tech Turns iPhone into Spiphone,” *Georgia Tech: Newsroom* (17 October 2011). http://www.gatech.edu/newsroom/release.html?nid=71506; Internet; accessed 29 January 2012.

United States. Department of Defense. *Transformation Planning Guidance*. Washington, DC: DoD United States, 2003.

United States Army. "Common Operating Environment." http://ciog6.army.mil/ArmyEnterpriseNetworkVision/tabid/79/Default.aspx; accessed 29 January 2012.

United States Army. "Providing the Network to the Tactical Edge." http://www.bctmod.army.mil/; accessed 29 January 2012.

Walsh, David. "Army Looks to Troops for Smart-Phone Tech Advice," *Government Computer News* (17 October 2011). http://gcn.com/articles/2011/10/10/defense-it-1-smartphone-technologies.aspx; Internet; accessed 29 January 2012.

Webster, Frank. *Theories of the Information Society*. Third ed. New York: Routledge, 2006.

Welch, Michael T. "The Emerging Media Revolution: Considering the Influence of New Media Forms on Democratic Society." M.A., Gonzaga University, 2006.