National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# WHAT IS THE THREAT TO CANADA: THE GOVERNING PARADIGM FOR MANAGING DEFENCE SCIENCE AND TECHNOLOGY STRATEGY

Commander M.M. Lewis

## 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
2011 – 2012

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

# WHAT IS THE THREAT TO CANADA: THE GOVERNING PARADIGM FOR MANAGING DEFENCE SCIENCE AND TECHNOLOGY STRATEGY

By Commander M.M. Lewis



Word Count: 14 016

Compte de mots : 14 016

## Abstract

The defence of Canada involves protecting Canadians; protecting its sovereignty, Canadian rights and freedoms, values, and way of life. Today, Canadians live in a world characterized by uncertainty that was defined by the attacks in the United States on September 11th, 2001 and reinforced by terror attacks in Mumbai, Madrid, London to mention only a few. Famines in Africa, fighting in the Middle East, ethnic genocides and other atrocities that occur around the world also shape Canadian policies. This paper argues that Canadian defence technology needs to reflect this changing world security.

Serious consideration should be given to studying terrorists' goals and methods for the purpose of understanding how defence technology can be utilized against Canada by enemies, and recognizing how defence technology can be utilized to minimize the exposure to terrorism. This paper examines Canadian doctrine that builds on collaboration and preparedness with the intent of identifying the threat to Canada and defining the appropriate task tailored capabilities to counter those risks. This paper illustrates that developing a governing paradigm for managing a defence Science and Technology (S&T) strategy as a counter-terrorism measure is one that maximizes collaboration at all levels. Analysis and development of defence S&T enabled solutions can improve interoperability by implementing pan-military technological solutions to military problems incorporating civilian best practices.

# TABLE OF CONTENTS

*Threats have changed, not revolutionary maybe, but more evolutionary and have become somewhat of a devolution of high technology. So you've got this really interesting nexus of high-tech and low-tech and this disparate threat that makes it very hard to pin down exactly the approach.*

- General Martin E. Dempsey

## INTRODUCTION

The defence of Canada involves protecting Canadians; protecting its sovereignty, Canadian rights and freedoms, values, Canadians' way of life. This defence of Canada extends 200 miles from Canadian shores and across the entire country – the second largest in the world and includes three of the seven oceans of the world. Since 1812, no foreign aggressor has occupied Canadian soil, but this is not to say Canada has not contributed militarily in the global arena. Having fought two world wars, a conflict in Korea, and served the cause of peace on countless United Nations' (UN) peacekeeping missions around the world, Canada has established an international presence. Further, during the Cold War era Canada contributed to a collective security umbrella arrangement and constructed policies. Today, Canadians live in a world characterized by uncertainty that was defined by the attacks in the United States on September 11th, 2001 and reinforced by terror attacks in Mumbai, Madrid, and London to mention only a few. Famines in Africa, fighting in the Middle East, ethnic genocides and other atrocities that occur around the world also shape Canadian policies. The wars and conflicts in places like Libya, Syria, Balkans, Africa, the Middle East and more recently with the organization State in Iraq and Syria (ISIS) are a result of hostilities and feelings of ill will and vengeance that are thousands of years old. The situation in Afghanistan was not new

– the mujahideen that the United States (US) and the North Atlantic Treaty Organization (NATO) fought were once considered allies during the Soviet occupation of Afghanistan from 1979 to 1989 and were supplied with US arms and training in their battle against the Soviets. Canada is not a superpower with the ability to cure all the ills of the world. The Cold War legacy cast Canada as a country that exercised influence in the world through political forums such as high level topical meetings with the US and through military alliances such as NATO. Respecting the size and resource rich nature of Canada, it seems only rational to conclude that a principal strategic focus of the Canadian Armed Forces (CAF) must be on the defence of Canada. Predicated on CAF's defence obligations, this paper will present a case for a governing paradigm for managing Canadian defence technology in the face of the current security environment.

This paper will argue that the Strategy 2020[1] framework is relevant as a counter-terrorism defence strategy and continues to represent the spirit of the Canadian First Defence Strategy (CFDS) and thus can be used as a governing paradigm for managing the defence Science and Technology (S&T) strategy. This leads into exploring the determination of the threat to Canada. As will be shown in the body of this paper, Canada, like any country has inherent risks from terrorism. The risk of destruction or crippling of ports and shipping lanes, vital to the economic trade of the region, can quickly weaken the country's economic position. Canada must study terrorists' goals and methods for the purpose of understanding how technology can be utilized against this country by enemies, and recognize how defence technology can be utilized to minimize the exposure to terrorism. Canada must create doctrine that builds on collaboration and

[1] Department of National Defence, *Defence Strategy 2020*, Shaping the Future of the Canadian Forces A Strategy for 2020 (Ottawa, 1999), i.

preparedness within a scalable construct with the intent of identifying the threat(s) to Canada and defining the appropriate task tailored capabilities to counter those risks. Canada must exploit and analyse intelligence faster than the highly mobile enemy in order to maximize the readiness of the CAF's combat forces, and leverage Canadian technical expertise. Lastly, Canada must seamlessly integrate with the United States and other Allies with the intent of leveraging joint exercises and combined operations to bring about the greatest worldwide coverage and greatest degree of situation awareness to commanders.

**Research Questions**

In support of the position that the Strategy 2020 framework is relevant as a counter-terrorism defence strategy and can be used as a governing paradigm for managing defence S&T strategy, the question of "what is the threat to Canada during times of uncertainty" will be studied. Secondly, the question of "how to leverage crucial defence S&T in order to protect Canada against terrorists" will be explored.

**Methodology and Outline**

To fully support the thesis and research questions posed above, this paper will focus on the following themes, divided into chapters for ease of flow and presentation. In order to examine the governing paradigm for managing defence S&T strategy, three targets from Strategy 2020 will be superimposed against Canada's defence technology as follows:

- develop new task tailored capabilities to deal with asymmetric threats;

- re-focus defence Research and Development (R&D) on the operational needs of the department capitalizing on leading edge technologies, while exploiting Canadian technical expertise, especially in the areas of space, remote sensing, telecommunications and information management; and

- manage Canada's interoperability relationship with the US and other allies to permit seamless operational integration at short notice.

The final sections make recommendations as to how the CAF can adapt and expand the use of S&T in the field of terrorist threats to Canada.

## CHAPTER 1: LITERATURE REVIEW

There are several elements that require review prior to progressing into the main body of this paper. Firstly, it is important to understand the context of Canada that this paper will explore. This is to say the composition of the CAF, CAF's mission, Canadian history, and the current state of defence technology in DND/CAF. Secondly it must be noted that the world has changed since end of the Cold War. It has become characterized by persistent continuous low to medium intensity conflicts in failed or failing states.[2] This causes a great deal of uncertainty of how to categorize the conduct and character of the enemy. In light of this terrorist threat, this paper will explore the appropriate defence S&T to protect the backbone of the critical infrastructure such as power distribution networks, communication systems, financial networks, and so forth. Lastly, the paper will review of the theoretical foundations of the continuously changing landscape of defence technology followed by an examination of DND's publication Strategy 2020. Simply put, there needs to be an understanding of all these elements in order to determine the appropriate defence S&T strategy in support of the thesis.

### Context – Thyself

The CAF consists of approximately 68,000 men and women[3] recruited from across the country who reflect Canada's cultural, linguistic and regional diversity. The CAF is a very large and very old organization. Many of today's CAF traditions and heritage are drawn from colonial militias dating back to the earliest French and British

---

[2] United States Army, *Adapting Our Aim: A Balanced Army for a Balanced Strategy* (Washington, DC: Government Printing Office, 2009), 2.

[3] National Defence and the Canadian Armed Forces, "About the Department of National Defence and the Canadian Armed Forces," last accessed 2 May 2014 ,http://www.forces.gc.ca/en/about-us.page.

settlements in North America. The mission of the CAF is to defend Canada in cooperation with the United States, defend Canadian interests and its values, while contributing to international peace and security in partnership with allies from other countries. Defence is one of the few Canadian national institutions that come solely under the federal government, which is the only authority in matters of defence and protection of Canadian sovereignty.[4] Protecting Canada deploys various defence S&T which will be explored throughout this paper. Concern for Canada's aging S&T must address the long-term sustainability, as well as hardware and software compatibility with future generations of new S&T. The costs associated with recapitalizing large S&T projects which are pan DND/CAF can be expensive. However, Canada is not alone in the need to upgrade costly S&T. The 2010 Spring Report from the Auditor General of Canada writes that a "2008 survey of chief information officers in state governments in the United States noted that modernizing aging IT systems and infrastructure presented a significant financial, technical, and program management challenge in that country."[5] This observation is important. It speaks to the fact that other governments, and by extension their militaries, suffer from the similar dilemma of aging technology, and thus presents opportunity. Likewise, CAF S&T from a hierarchical, institutional, and organizational perspective must invest in better defence knowledge, better defence technology, and better military capabilities for the Forces. Recognizing that one of the CAF's mandates is to cooperate with the US while fostering partnerships with allies from other countries necessitates a joint/combined approach to improving interoperability by

[4] National Defence and the Canadian Armed Forces, "About the Canadian Armed Forces," last accessed 2 May 2014, http://www.forces.gc.ca/en/about/canadian-armed-forces.page.

[5] Office of the Auditor General of Canada, "Aging Information Technology Systems," *Report of the Auditor General of Canada to the House of Commons*, Ottawa, Spring 2010.

using compatible S&T. Developing compatible S&T to be utilized with like-minded countries produces many benefits from economies of scale, increased speed of integration during exercise/operations, better interoperability, and many more. These concepts are discussed in greater detail in a later chapter.

**Context - Thy Enemy**

A popular adage by goes "better an unsuccessful defence in the enemy's country, than a successful defence in Canada"[6], as alluded to the devastation that is avoided at home in fighting an enemy far from Canadian shores. During the Cold War, such a notion may have had some merit. The world, at that time, lived in fear of nuclear war. There were defined enemies and the world was polarized into East and West - into NATO and the Warsaw Pact. As a member of NATO, Canada knew what the threat was and it knew how to counter it. During this era, certainty was an ally. With the fall of the Berlin Wall in 1989 the security environment changed. The Soviet bear was tamed and the world was no longer divided along polarized East-West lines. It became characterized by continuous low to medium intensity conflicts in failed or failing states where peace was unenforceable, the enemy was undefined, and defence technology was improving at an ever increasing pace. The future is difficult to predict. "This is because our adversaries 'get a vote' and are inclined to attack weakness rather than strength. This makes a breadth of preparation and education flexible enough to allow for rapid change imperative."[7]

---

[6] Various public speeches, where the spirit of this quote was raised by General Hillier.
[7] John Brown, "Defense Transformation Redux," *Army Magazine,* 62, no. 11 (2012): 26.

In this new world disorder, Canada must be prepared to fight, as General Hillier said, the snakes and not the bear.[8] One can hunt a bear, one can counter a bear, but how does one hunt or counter a snake? How does one defeat an unseen enemy? The attacks in Madrid and London painfully illustrated this principle. These attacks were carried out by "home grown" terrorists, unseen, unknown snakes that can strike from anywhere with very little sophisticated defence technology. Canadians are not fighting a war on terrorism; Canadians are fighting a war of ideologies from which terrorism is used as a means to an end. Unfortunately, the structure for managing Canadian defence technology needs to reflect the changing world security. The Department of National Defence (DND) and the CAF have faced challenges that take these former points into consideration when formulating defence S&T strategy. The Deputy Minister of National Defence and the Chief of Defence Staff (CDS) write, in "an era of continuing global instability, resource constraints and the diffusion of advanced technologies, S&T and the broader innovation system are indispensable capabilities that support operational excellence and effective, evidence based decision-making. It is this context which both shapes and defines Canada's new Defence and Security S&T Strategy."[9]

Defined as a broad range of fields that have both scientific origins and immediate practical application with fields ranging from information and communications technologies, cyberspace warfare, maritime/airspace intelligence through use of satellites, and many more, S&T play an important part in the DND/CAF. In its simplest characterization, S&T makes use of knowledge, tools, machinery, systems/methods in

---

[8] House of Commons, Standing Committee on National Defence and Veterans' Affairs, *Minutes of Proceedings and Evidence*, no. 1, May 19, 2005, 1.

[9] Defence Research and Development Canada, "Science And Technology In Action: Delivering Results For Canada's Defence And Security," lasted accessed 19 May 2014, http://www.drdc-rddc.gc.ca/en/publications/defence-st-strategy.page.

order to solve a problem or perform a specific function. Equally important, Canada's strength in S&T plays a key role in furthering defence capability, technical innovation, and international compatibility with likeminded country's defence systems. In 1996, the Canadian Federal Government recognized the importance of scientific excellence in defence S&T.[10] This is important in determining if Canada is losing ground from a global perspective. Further studies explored the current state of Canadian S&T identifying "Canada as one of seven 'scientifically advanced' countries that stand to gain the most from foreseen advances in technology and will be best equipped to absorb the world's leading new technologies ."[11] Strength in S&T for defence applications is essential in order to research, innovate, and develop viable responses to enemy technology. The connection between S&T and the practical demonstration of new defence innovations can save soldiers lives during combat by implementing technological solutions to military problems. At a pan-government level, military S&T must leverage fundamental national research missions in areas such as defence[12], with one such example being the Defence Research and Development Canada (DRDC).

**Context - The Threat**

What is the threat to Canada and how is it countered? This is the basic underlying question that any governing paradigm for managing defence S&T strategy should address. Compounding this strategy is the continuously changing landscape of defence

[10] Hussein Rostum, Mark MacDonald, and Doug Williams, "Measuring and Ensuring Excellence in Government Science and Technology: Canadian Practices," *The Council* (2001): 1.

[11] Committee on the State of Science & Technology in Canada, *The State of Science & Technology in Canada*. Council of Canadian Academies (2006), 116.

[12] Rashib Nikzad, "The Changing Role Of Government Labs In Science And Technology Policy." *Regional Science Inquiry* 1 (2013): 118.

technology and uncertainly that entails world events. Central to this paper is DND's Strategy 2020 publication[13], commonly referred to simply as Strategy 2020.

Strategy 2020 resulted from a DND analysis. It built upon several lessons learned, explored past studies, and past initiatives. Strategy 2020 most importantly personified the spirit of the 1994 Defence White paper's strategic assessment. Strategy 2020 took into consideration stakeholders' needs and expectations, and assessed CAF's strengths and weaknesses. Most germane to this paper, Strategy 2020 "analyzed emerging defence issues such as those associated with the 'Revolution in Military Affairs'."[14] A revolution in military affairs (RMA) is polymorphic in nature –no one definition can capture its essence. It morphs continually based on technological change, it morphs based on the enemy at any given time, past battle experiences, future expected battlefields, asymmetrical warfare constructs, rust out, organizations, hierarchies, institutionalism, nationalism, the international system, defence spending levels, lessons learned, civil-military gaps, ours and the enemy's capability along all strategic and tactical levels, to mention only a few examples. RMA is in a constant state of flux with multiple perspectives, yet it maintains its ancestry in defence. Defence technology must be proactive, reactive, and a measured response notwithstanding the polymorphic nature of RMA. This being the case, defence S&T must constitute and capture the notion of "just enough" and "just in case" defence levels.

Defence S&T is a wide field of study with myriad of disciplines within it. This paper will consider specific Strategy 2020 targets and superimpose these onto a defence

[13] Department of National Defence, *Defence Strategy 2020*, Shaping the Future of the Canadian Forces A Strategy for 2020 (Ottawa, 1999).

[14] *Ibid*., i.

technology context. This will take into consideration the future security environment discussed above. For the purpose of narrowing this paper, the following chapters will examine and focus on three Strategy 2020 objectives with heavy influences on defence S&T.

## CHAPTER 2: DEVELOP NEW TASK TAILORED CAPABILITIES TO DEAL WITH ASYMMETRIC THREATS

One target of the Strategy 2020 framework is to "develop new task tailored capabilities to deal with asymmetrical threats."[15] This ties directly in with the thesis of this paper which is the determination of the threat to Canada and the development of a governing paradigm for managing defence S&T strategy.

Within the environmental context stated above, Canada's 18 major ports handle approximately 309.7 million tonnes of cargo annually, valued at more than $162 billion dollars, with a further 200 million tonnes of cargo handled by an equally important regional port system consisting of several hundred ports from the Atlantic to the Pacific to the Arctic.[16] Shipping represents a very significant element in Canada both from a domestic (e.g. seaway) and as an international economic corridor for trade. With such an enormous amount of trade flowing through Canada's ports, the threat of a terrorist attack to a port/lock/seaway would cause a monumental economic disruption.

Within the construct of counter-terrorism, DND/CAF "have broad based involvement in the Government's counter-terrorism efforts and can work either as the lead or a supporting department."[17] Therefore it is critical that defence S&T develop new task centric capabilities based upon a comprehensive strategy for the protection of Canada's economic region. This being the case, it is fundamental to broaden the scope and breadth on these topics before promulgating defence S&T policy. Greater visibility

---

[15] *Ibid*., 9.

[16] Association of Canadian Port Authorities, "Public Relations - Port Industry Facts," last accessed 13 May 2014, http://www.acpa-ports net/pr/facts.html.

[17] Ministry of Public Safety, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (Ottawa: Canada, 2011), 35.

of Canada's ports, seaway/shipping channels, and water traffic is a major S&T consideration when one weighs the potential impact of a terrorist attack. William Shilling notes that since the "September 11, 2001, attacks by terrorists on the World Trade Centre and the Pentagon, stepped-up vigilance and patrols by the US Navy and US Coast Guard along the coastal areas of the United States have greatly increased"[18] as well as adding 670 radiation detection monitors at its ports of entry. Nowhere has it become more critical to have the right tactical information, about the right location, at the right time then when fighting against an asymmetrical enemy – where the right response is paramount to minimizing further damage and/or limiting disruptions.

TERRORISTS - GOALS

Much has been written about terrorism and terrorists. Yet, a review quickly reveals that there is no consensus about terrorist groups' strategies and goals. One school of thought believes that publicity is a highly sought reward to terrorists and viewed it as the "oxygen of terrorism."[19] Terrorists increasingly seek shocking and deadly acts in order to obtain the greatest media coverage possible. The thinking behind these acts also goes to believing that such publicised acts could disrupt/dissolve a coalition as witnessed after the Madrid attacks of 2004. Publicity can also garner support and sympathy to support the terrorist's strategic initiatives, and in a sense, bring street credibility to their fellow terrorist brethren.

---

[18] William Schilling, *Nontraditional Warfare: Twenty-first-century Threats and Response* (Washington, D.C. Brassey's, 2002), 106.

[19] Brigitte Nacos, *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post-9/11 World* (Toronto: Penguin, 2008), 223.

Conversely, another school of thought believes that some terrorists have no publicity goals. For instance, bin Laden's goals were not primarily media attention, but rather to kill as many godless materialistic Americans as possible. These terrorists attempt to disorientate people through "acts of symbolic violence"[20] with a view of disrupting a government's authority. In fact, research now points to "fanaticism rather than political interests is more often the motivation."[21] No policy changes or concessions would appease these radical anonymous terrorists. As such, terrorists and their decision making processes do not conform to a cookie-cutter model. This makes determining a terrorists group's centre of gravity, which might be articulated as their incentive, very difficult. It makes establishing a cohesive defence technology doctrine to defend Canada difficult.

Much in the same way that an allied coalition can act as a force multiplier, likewise transnational state sponsored support for terrorist groups act as a force multiplier. For instance, the government of Iran has often been accused by the international community of funding, providing equipment and training, and giving sanctuary to terrorists.[22] "In addition to this, the "preponderance of evidence is that people participate in terrorist organization for the social solidarity…to experience social solidarity with other members."[23] When one combines the social appetite of a terrorist wanting to be part of a brotherhood with state sponsored terrorism one quickly finds a deadly bond.

---

[20] Peter Neumann and M.L.R Smith, *The strategy of terrorism: How it works, and why it fails* (New York: Routledge Taylor & Francis Group, 2008), 35.

[21] Matthew Morgan, *The Origins of the New Terrorism* (Parameters 34, no. 1, Spring 2004): 30.

[22] Council on Foreign Relations, "State Sponsors: Iran," last accessed 6 August 2014, http://www.cfr.org/iran/state-sponsors-iran/p9362.

[23] Max Abrahms, "What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy," *International Security* 32, no. 4 (Spring 2008): 94.

This being the case, what is the likelihood of another terrorist attack like the ones witnessed on 9/11, and what would be the consequences? What is the likelihood of Canada experiencing a terrorist attack on its homeland, or being launched through Canada? These are keys questions in determining and defining the threat to Canada. Naturally, because of its close proximity to Canada there has been a great deal of discussion on this matter over the years with the US, which is recognized as being one of the closest bilateral defence relationships in the world. These discussions take place within the academic community, with senior military leaders, and senior Canadian government officials. It is commonly accepted that the US and Canada will very likely encounter terrorist threats in the future. This is simply due to the fact as the US and Canada grow in military strength, the opposite side of the continuum is that smaller enemy forces, unable to win with force-on-force action, will resort to other means of hurting their adversary. The outcome is asymmetrical warfare. This is further compounded by the fact of the military's growing dependence on high defence technology. Enemies recognize that they no longer have to defend against massive warships and powerful warplanes, instead, the enemy simply has to prevent that military warcraft from operating, conceivably through cyberterrorism sabotaging the onboard electronic computer missile guidance system or disabling the Global Position Satellite (GPS) system, for instance.

Finally, thought must be given to a worse demise, Canada's defence technology being used against itself. The world witnessed this on 9/11 with terrorists taking control of aircraft and using them as weapons, and to a lesser degree the Somalia pirates hijacking vessels and demanding ransom. It might sound like science fiction or a bad

movie plot, but what if an enemy did not even have to hijack an airplane or naval vessel? Imagine the chaos of an enemy gaining remote control of Canadian defence technology and using that technology to fire its weapons upon friendly troops. As long as terrorists are goal oriented to hurt their adversary by any means possible, they will only be hampered by their lack of imagination.

## TERRORISTS - METHODS

From a defence S&T perspective, asymmetric threats are difficult to predict and combat. In fact, it is for this very reason that enemies utilize such strategies in order to overcome larger enemies with defence technological superiority. Brown writes, "Much has been said and written about the 'asymmetric threats' of the 21st century and how technology is providing potential enemies new means of defeating conventional militaries."[24] This trend was witnessed regularly in Afghanistan with Improvised Explosive Devices (IED) and roadside bombings. Terrorist methods also extend to the use of explosive devices (individual suicide bombers, vehicle-based explosives, bag bombs, etc), shootings (close quarter attacks targeted against Westerners), kidnapping (demanding the release of other terrorists from prison), assassination (of government leaders or diplomats to cause political movement to collapse), and the big tactics of bioterrorism (weapons of mass destruction, biological, chemical, etc). Regardless of the utilized tactics, terrorists' methods are motivated to hurt their adversary by disrupting the general population with a view of lowering their morale. One thought is to dissuade politicians from entering a war by swaying the general population's views on the matter.

[24] K.J. Brown, "CF Transformation: Evolution, Revolution or Innovation? RMA induced by changes in threats: The asymmetric environment" (Royal Military College of Canada, 2006), 5.

It was not long ago when downtown Toronto was effectively shut down for days due to an electrical power outage. The city was at a complete stand-still. Imagine for a moment if that was a terrorist attack. If it was terrorists that attacked the city or city officials in order to get Canadian politician's attention it would have worked. Kydd and Walter write that by "targeting the government's more visible agents and supporters, such as mayors, police, prosecutors, and pro-regime citizens, terrorist organizations demonstrate that they have the ability to hurt their opponents and that the government is too weak to punish the terrorists or protect future victims. Terrorists can also use an intimidation strategy to gain greater social control over a population."[25] Continuing with the Toronto example, by day three it can be argued that Toronto citizens were ready for any concessions, in particular if the attack was all about a foreign policy decision. It simply boils down to the fact that it is difficult, or near impossible, to accuracy predict terrorists' methods, where, when, and how the next terrorist attack will occur. Consequently, Canadian defence S&T strategies must do two things: 1) recognize and study from a defensive perspective how technology can be utilized against this country by enemies, and 2) recognize and study from an offensive perspective how defence technology can be utilized to prevent/intercept/respond to terrorist/enemy activity from utilizing asymmetric warfare techniques against this country by utilizing pre-emptive strikes or similar techniques. Make no mistake, this is no simple task. The attack on the USS Cole on 12 October 2000 was an example of a "highly sophisticated vessel, capable of shooting down incoming sea-skimming missiles and plotting complex battle scenarios in its

[25] Andrew H Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (2006): 66.

combat information center, brought down by a bomb on a raft."[26] How does one counter uncertainty that is brought about from asymmetric warfare? Canada's defence S&T doctrine must formulate new task tailored capabilities that are mission and task centric to deal with asymmetrical threats.

## TASK TAILORED CAPABILITIES

Because of the Internet's amplifying power, cyberspace and cyber warfare has quickly become an integral part of the command picture on terrorist threats. Generals recognize that propaganda, espionage, and reconnaissance form part of political and military conflict. Hackers are trying to steal Canadian secrets and classified data with a view of discovering military vulnerabilities. They want Canadian innovations that provide a competitive advantage in the technological marketplace. Computer hackers can read, delete, and modify information travelling between computers. Friendly forces can very quickly lose any advantage. Worse still, enemy hackers can attack or divulge critical military R&D. It is for these reasons that to "make rapid advances in defending against attacks, the state of the art evaluation of network security mechanisms must be improved."[27] Imagine the horrific impact of the North American Aerospace Defense Command (NORAD) computer network being hijacked through a massive Denial of Service (DoS) which simply floods the target with bogus information so that it cannot respond to legitimate requests/services thus rendering it useless. Equally, terrorists could use NORAD's systems to communicate inaccurate information (data modification)

---

[26] Author Unknown, "Asymmetric Warfare, the USS Cole and the Intifada", *The Estimate – Political and Security Analysis of the Islamic World and its Neighbours*, 12, no. 22 (2000): 1.

[27] R. Bajcsy, T. Benzel, M. Bishop, B. Braden, C. Brodley, S. Fahmy, and C. Rosenberg, et al, "Cyber Defense Technology Networking And Evaluation," *Communications Of The ACM* 47, no. 3 (2004): 58.

potentially having aircraft fly into mountains. Data hacking can be a critical vulnerability to power grids, oil refineries, weapons systems, targeting systems, military satellites, command and control modules, to mention only a few examples. This exposes great risk considering command teams might make important decisions predicated upon maliciously altered data and thus dramatically affect Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).

A key advantage of cyber warfare for an enemy is that the data is collected remotely. Gone are the clandestine days of person-to-person drops under park benches. When a data breach occurs, it may not be detected for months, or years, and the data breadth may contain millions of classified documents. Another asymmetric element of cyber warfare is propaganda. Electronic propaganda is extremely easy to create, quick to distribute via the Internet, and can form a powerful message to the world. It is the electronic equivalent of dropping behind enemy lines. The end result is that task tailored capabilities need to be designed to properly secure friendly computer servers through use of cryptology. Further, testing needs to be conducted against friendly computer servers looking for vulnerabilities, whereby enemy computer hackers can crack the code and have access to classified networks. On the flipside of this conundrum, friendly forces can likewise hack enemy computer systems and networks looking for indications of a future asymmetrical terrorist plot.

Another example of new task tailored capabilities to deal with terrorist threats is the use of Unmanned Aerial Vehicles (UAVs). UAVs were initially used for surveillance, however their mission is evolving to also include combat. Many countries state that UAVs represent the future and defence spending on UAV technology is a high

priority, "several emerging technology areas will likely shape the US military over the next decade and beyond, including unmanned systems, autonomous systems, cyber weaponry…among others."[28] The notion of reducing military casualties, the incredible duration of time UAVs can spend on station when loitering without consideration to aircrew rotations and exhaustion, and the vast modularity of mission fit and mission specific UAV adaptations make it a very appealing argument to senior military leadership. UAVs are a compelling addition to the CAF where the human is a limitation to mission success. Militaries with a reduction in military personnel like Taiwan[29], and militaries with a strict zero-growth manning level policy are relying on UAVs to complement their capabilities as witnessed by Singapore's "increased reliance on unmanned defence technology for the army, navy, and the military."[30]

A key element of UAVs is their persistence, that is to say their ability to loiter over a target for long periods of time. Although not a typical UAV example, three of the most persistent loiters are from the NASA Mars Program. The Mars Rovers Spirit and Opportunity have spent 10 years on Mars, and Curiosity has been there two years. These rovers are a good indication of the diverse possibilities of UAVs where it is inconceivable to place humans in those conditions. Canadians are witnessing this trend of UAVs and more commonly with the Explosive Ordnance Disposal (EOD) bomb squads who send robots into dangerous hot spots to assess a situation without putting human life at risk.

---

[28] Michael Horowitz, "Coming next in military tech," *Bulletin Of The Atomic Scientists* 70, no. 1 (2014): 55.

[29] "Armed Forces And Government Spending," *Taiwan Defence & Security Report* no. 2 (Q2 2012): 58.

[30] "Armed Forces And Government Spending," *Singapore Defence & Security Report* (Q3 2009): 29.

UAVs can penetrate deep into terrorist territory, and pre-position itself awaiting an opportunity to strike an enemy target, and it can operate in dangerous environments without risk to human life. UAVs are silent force multipliers requiring fewer personnel in a combat zone to project power, yet without projecting vulnerability of decreased troops. Gone are the days of force-on-force action, and huge battles of attrition. Instead, these concepts are replaced by utilizing UAVs against manned enemy targets.

Modern technology also makes asymmetric warfare more effective, unfortunately, as enemies seek vulnerabilities to systems that friendly forces rely upon, which is why Canada must collaborate to constantly refresh its strategic S&T. As one example of an Other Government Department (OGD) acting as a primary delivery agent that provides the DND a refreshed strategic focus is the DRDC which supports defence and security operations with knowledge and technology in order to provide S&T to meet operational requirements.

This union of DND/CAF, OGDs, and civilian enterprises working in collaboration for the development of new defence technologies can be complex considering the Government and the military are motivated to maintain minimum levels of armed forces in order to satisfied foreign policy objectives and domestic responsibilities, while at the same time to appease its constituents who are adamant about a cost effective government. This richness of participation becomes even more cumbersome at the international level. "International collaboration by companies and government on defence research can yield substantial benefits, but it is inhibited by national and commercial security and by the complexity of reconciling and synchronising the interest and budgets of different nations

while navigating through their various legal and administration systems."[31] Nevertheless, it is the Government that dictates DND/CAF's budget levels, and also dictates the Regular and Reserve Force manning levels. By virtue of these spending levels, government will establish defence S&T strategy objectives, and also the foreign policy in terms of DND's deliverables on international matters such as its contribution to the global war on terrorism. The CAF's defence technology strategies are at the mercy of its political masters, as seen during the 1990s when the defence budget was severely cut-back. As a result, the CAF had emerged from a decade of darkness and had suffered from asset rust out. This trend was more recently experienced with some of Canadian allies, where the "days when we could afford to do everything in-house have gone … [w]e rely on heavily the rest of UK and the rest of the engineering and technology base."[32]

Since 9/11 voters have been more willing to except higher government spending for the sake of pre-emptive tactics and homeland security. This is also true in Canada with respect to new task centric capabilities where cooperation between different OGDs is essential (e.g. Emergency Response, Coast Guard, CAF, Royal Canadian Mounted Police (RCMP) etc). Since government finances are being challenged and scrutinized daily, economies of scale and efficiencies gained by working together help share best practices and integrate business best practices in order to achieve pan DND/CAF savings, while still exploiting new defence S&T. The combination of working with OGDs, civilian enterprises, and adopting best business practices can accelerate delivery of new

[31] David Kirkpatrick, "The Future Of UK Defence Research," *Defence & Peace Economics* 19, no. 6 (2008): 485.

[32] Heath Reidy, "The Best Defence," *Professional Engineering* 22, no. 5 (2009): 25.

task tailored technical capabilities. "Operational and budgetary factors bring about an increasing commonality between the civil and military sectors with benefit to all concerned."[33] This allows DND/CAF to prepare for an uncertain future by identifying the problem, and seeking the best solution available without "reinventing the wheel" as the popular adage goes. Further, a collaborative approach reduces the exposure of risk by sharing it.

An equally important element is that DND/CAF work collectively to develop world class S&T for Canada. One consideration is the security risk. A balance must be struck between the risk of exposure of defence S&T versus the benefit of sharing that defence technology. Information/intelligence leaks can damage the Nation's credibility or worse expose weakness to Canadian enemies who will leverage that weakness in their asymmetrical tactics. "Suspected terrorists have changed how they communicate and have become more difficult to track as a result of former contractor Edward Snowden's disclosures about U.S. surveillance operations, according to current and former officials who say that the changes have led to a significant loss of intelligence."[34] This makes working collectively rewarding, but complex.

A collaborative working relationship with OGDs can bring about the most cohesive integrated solution. This collaborative approach is in contrast to many terrorist organizations which comprise of multiple locally based tribal networks with hundreds of

---

[33] "Undersea Defence Technology," *Sea Technology* 54, no. 5 (May 2013): 45.

[34] Ken Dilanian, Los Angeles Times, "Terrorists harder to track after Snowden's leaks, officials say," last accessed 22 May 2014, http://articles.latimes.com/2013/jun/28/world/la-fg-wn-snowden-terrorists-communications-20130628.

"free agent" foreign fighters.[35] Perhaps terrorists have a unity of mission, but rarely do they have a unity of command. Instead, terrorist groups tend to have persistent fissures among insurgent leadership at local levels.[36] Naturally, this reduces the speed and decisiveness of their information operations (IO) and media campaign. When one considers that IO and media campaigns are one of terrorists' central efforts, any disruption reduces their agility and versatility. It creates gaps that friendly forces can leverage in order to get inside the terrorist decision cycle of observe, orient, decide, and act (OODA Loop). It is for these reasons that DND/CAF's collaborative multi-agency training and exercises with OGDs takes advantage of those gaps and enhances the ability at predicting asymmetrical threats. It is the exploitations of terrorists' strengths and turning them into weaknesses. The irony is that asymmetrical warfare is all about doing everything possible to negate the strengths of their opponent, yet in this case, friendly forces instead are leveraging the enemy's weaknesses.

[35] Jenna Jordan, "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes," *International Security* 38, no. 4 (2014): 30.

[36] Michael Freeman, "A Theory of Terrorist Leadership (and its Consequences for Leadership Targeting)," *Terrorism and Political Violence*, ahead of print (2014): 1.

PREPAREDNESS – RESILIENCE - SCALABILITY

Leveraging an enemy's weakness is the very concept that is key in Canada's Ministry of Public Safety *Building Resilience Against Terrorism*.[37] Released in 2011, *Building Resilience Against Terrorism* was Canada's strategy for government departments and agencies involved in counter-terrorism. It laid out the ground work for a unified approach for Canada via four elements: Prevent, Detect, Deny and Respond. Canada's strategy defined these elements as the following:

> **Prevent** individuals from engaging in terrorism;
>
> **Detect** the activities of individuals and organization who may pose a terrorist threat;
>
> **Deny** terrorists the means and opportunity to carry out their activities; and
>
> **Respond** proportionately, rapidly and in an organized manner to terrorist activities and mitigate their effects.[38]

These elements are effective because they are scalable. In other words, depending on the level of threat and consequence of an effective terrorist attack, Canada would apportion an amount of resources to that problem. *Building Resilience Against Terrorism* doctrine is intended to track the current world trends in terrorism and asymmetrical warfare. By use of intelligence, with the goal of near perfect intelligence, Canada is better able to identify enemy capabilities, tactics, techniques, and their procedures. This allows Canada to develop emergency response plans and to collectively generate response modeling and scenario development. Logically, such emergency response plans

---

[37] Ministry of Public Safety, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (Ottawa: Canada, 2011), 14.

[38] *Ibid.*

developed within the model of *Prevent, Detect, Deny and Respond* rely heavily on information flow, command and control structures (federally and provincially), and interagency communication. It is all these elements taken together that assist in determining the threat to Canada, and channel Canada's energy to developing the appropriate defence S&T with the benefit of working with OGDs to accelerate delivery of those technical capabilities.

Canada, like any country has inherent risks from terrorism. The risk of destruction or crippling of ports and shipping lanes, vital to the economic trade of the region, can quickly weaken the country's economic position. Risk of cyber warfare, Denial of Service, IO and media campaigns, and electronic propaganda against Canada are genuine threats. Canada must study terrorists' goals and methods for the purpose of understanding how technology can be utilized against this country by enemies, and recognize how defence technology can be utilized to minimize the exposure to terrorism. As discussed earlier, a key doctrine that builds on collaboration and preparedness is the scalable construct of *Canada's Strategy Building Resiliency Against Terrorism* with the intent of identifying the threat to Canada and defining the appropriate task tailored capabilities to counter those risks.

The focus of this paper will now shift to examining a second target of the Strategy 2020 framework. This target seeks to exploit Canadian technical expertise with a view of capitalizing on leading edge defence technology. Through these initiatives, Canada would apportion budget funding for R&D in order to maximize the readiness of future CAF's combat forces.

## CHAPTER 3: RE-FOCUS DEFENCE RESEARCH AND DEVELOPMENT (R&D) ON THE OPERATIONAL NEEDS OF THE DEPARTMENT CAPITALIZING ON LEADING EDGE TECHNOLOGIES, WHILE EXPLOITING CANADIAN TECHNICAL EXPERTISE, ESPECIALLY IN THE AREAS OF SPACE, REMOTE SENSING, TELECOMMUNICATIONS AND INFORMATION MANAGEMENT.

A second target of the Strategy 2020 framework is to "re-focus defence R&D on the operational needs of the department capitalizing on leading edge technologies, while exploiting Canadian technical expertise, especially in the areas of space, remote sensing, telecommunications and information management."[39] This ties directly in with the thesis of this paper which is the determination of the threat to Canada, followed by developing a governing paradigm for managing a defence S&T strategy as a counter-terrorism measure.

DND/CAF have a reputation for being a decade behind in their R&D and in terms of adopting new S&T. In efforts to shrink these delays, the "Conservative government is reducing the Department of National Defence's influence in steering big-ticket military purchases after a string of delays and cost overruns in acquiring hardware for the Canadian Armed Forces."[40] When DND/CAF investigate the possibility of pursuing new S&T they tend to apply traditional capital budgeting models for all capital investments even though these have proved less than effective when assessing the value of new and emerging technology. Traditional models tend to look at discrete projects rather than the investment in S&T infrastructure, testing new business models, or other pan-military S&T capabilities that could benefit the whole organization. Training, education, and

[39] Department of National Defence, *Defence Strategy 2020*, Shaping the Future of the Canadian Forces A Strategy for 2020 (Ottawa, 1999), 9.

[40] Steven Chase, "Ottawa to curb military's role in procurement after costly delays," *Globe and Mail*, 5 February 2014.

awareness of S&T often fall short. Care must be taken to ensure DND/CAF's S&T is not slapped together in a flippant manner based solely on how much funding is available at that particular time or with little regard to taking a comprehensive look at life cycling and development. Likewise, CAF must place the same level of importance on its S&T resources as it does on operational requirements – in other words *the what and the how* of conducting warfare - keeping in mind these two elements should work in unison. DND/CAF must not just fight, but it must also prepare to fight smarter. Investing in R&D on the operational needs and capitalizing on leading edge technologies means fighting smarter, not harder. This paper will examine examples of utilizing a governing paradigm for managing defence S&T.

SPACE

Strategy 2020 laid the ground work for focusing R&D and Canadian technical expertise in the area of space. The Government was interested to continue its participation in major space projects such as with the International Space Station (ISS). This focus on R&D also translates into military applications which seek Canadian technical expertise. In this vein, the CAF Director General Space has the duty to "capitalize on unique Canadian technologies."[41] More and more the CAF operate in an information-driven world where space has now become vital to military planning and situational awareness of its territory. Canadian maritime and airspace awareness is critical, with satellites able to offer dependable near real-time data of approaching marine vessels and inbound aircrafts. CAF access to space and space capabilities has drastically

[41] Chris MacLean, "Director General Space: An interview with BGen Rick Pitre," *FrontLine Defence 2013* Vol 10, No 6.

increased over the years, and the CAF has found itself in a collaborative partnership. Examples of partnerships that leverage space-enabled capabilities can be found behind the Sapphire satellite project, with the Canadian Space Agency, as well as the Canadian industry. Sapphire is a military satellite whose mission is to prevent collisions in space. A second example of partnerships is with the Wideband Global Satellite Communication (SATCOM) system which consists of a 10-satellite constellation that permits Canada to communicate over voice and data anywhere in Canada. For greater secure military communication requirements, this space-capability is enhanced with the Protected Military SATCOM[42] program which operates in high-jamming environments especially for contingency and expeditionary operations. Much in the same way that the military must operate in potential high-jamming environments that affect their communications, the military must also have access to secure global navigation satellite systems. Such satellite systems affect the ability of the Navy, Army, Air Force, and Special Operations Forces (SOF) to track asymmetrical threats nationally and prosecute targets with the highest degree of accuracy.

## REMOTE SENSING

As mentioned earlier, Canada's 18 major ports handle approximately 309.7 million tonnes of cargo annually, valued at more than $162 billion dollars, with a further 200 million tonnes of cargo handled by an equally important regional ports system consisting of several hundred ports from the Atlantic to the Pacific to the Arctic Ocean. Protecting Canada's entire supply chain of maritime transport logistics from pirates and

[42] Protected Military SATCOM is a highly secure satellite whereby critical military voice/data is transmitted without being jammed, detected, or intercepted.

terrorism is essential. This makes it critically important that the focus of Canadian defence R&D is protecting this vital economic interest from terrorist activity. One way that DND/CAF is capitalizing on leading edge S&T and remote sensing is through the use of its joint multi-agency Marine Security Operations Centres (MSOC). Located in Esquimalt, BC, and Halifax, Nova Scotia.[43] These MSOCs collect and analyse vast amounts of information in order to strengthen Canada's marine security by identifying possible security threats.

MSOCs utilize sophisticated defence S&T to track vessels in Canadian waters. Utilizing geospatial intelligence (GEOINT), MSOCs "manage, analyze and exchange maritime intelligence, surveillance and reconnaissance data."[44] MSOCs provide situational awareness to support operational commanders by providing comprehensive intelligence reports. For example, during a briefing to an operational commander on a vessel that is approaching Canadian waters, an analyst in the MSOC can display a photograph taken from aerial surveillance only moments earlier. Drilling down further into the data provides the MSOC analyst Jane's information on that particular vessel (e.g. country of origin, compliment, speed, typical cargo, previous infractions, etc). In the middle of a weather brief if the operational commander suddenly asks for the status of an ongoing Search And Rescue (SAR), the analyst has only to go to a specific web page that covers that event – which is updated by the minute.

The more important characteristic of this S&T is that it is not based on being in the same location as the MSOC analyst or the same location as the sensors/information.

---

[43] A third MSOC monitors the Great Lakes-St Lawrence Seaway. It is located in Niagara Falls, Ontario, and is managed by the Royal Canadian Mounted Police (RCMP).

[44] Canadian Coast Guard, "Marine Security Operations Centres (MSOC)," last accessed 20 May 2014, http://www.ccg-gcc.gc.ca/eng/CCG/Maritime-Security/MSOC.

This intelligence is made *securely* available to warships and OGDs via remote access to facilitate coordination. Often times, the MSOC interconnected system will tap into OGDs/Agencies, such as the RCMP, to provide up-to-date information on a current joint operation.

The preceding might seem like a simple example, but recall that information and communication is critical to operational commanders. Events/attacks happen with little warning, therefore DND/CAF requires comprehensive S&T to facilitate communication and increase response time.

## GEOSPATIAL INTELLIGENCE

History has shown that it is difficult to identify[45] and track terrorist groups.[46] Several US agencies have established terrorist tracking mechanism (Most Wanted Lists, No Fly List, etc) for the sole purpose of finding particular terrorists. Terrorists have learned to adapt to Western intelligence, even going so far as to conceal their funding sources and making it extremely difficult to discover.[47] However, rather than finding a specific terrorist, Canada must learn to find terrorists in the generic sense. This is to say, instead of locating and finding one terrorist for the purpose of bringing that individual to justice, as an alternative, Canada should look for the indications of budding terrorist activity with a view of preventing a future terrorist attack. It is for these reasons that Canada must heavily invest in R&D in the areas of GEOINT which includes: surveys,

---

[45] National Commission on Terrorism, and United States of America. "Countering the Changing Threat of International Terrorism." (2000).

[46] Homeland Security Watch, "Agreed: Terrorist tactics are tough to track," last accessed 16 July 2014, http://www.hlswatch.com/2013/12/05/agreed-terrorist-tactics-are-tough-to-track.

[47] Ekrem Emeksiz, "International Terrorism Financing" (City University of New York (CUNY) - John Jay College - International Crime and Justice MA Program, 2013), 8.

maps, charts, remote sensing data and images, aerial photographic services, Global Positioning System (GPS), Geographic Information Systems (GIS), geocoding, and so forth.[48] GEOINT seeks to exploit and analyse geospatial data and information in order to geographically reference activities. Because terrorists tend to be very mobile, GEOINT is most useful against an asymmetrical threat because it provides timely intelligence using current geospatial data. Terrorists historically strike densely populated areas with the intention of causing the high amount of casualties.[49] Urban areas are the modern day jungle where insurgents and terrorists can easily hide and be supported. They look to cripple communication lines, pollute drinking water, strike in shopping malls/Western style hotels, military barracks, etc. Terrorists understand well that densely populated areas are more prone to media coverage, thus highlighting the civilian casualties and suffering. In order to improve the situational awareness and targeting of these terrorists, defence S&T must develop real-time intelligence and GEOINT through the use of sensors and thus provide a relevant common operating picture. In this vein, Network Centric Warfare is a concept for the linking of sensors, and weapon systems so that information can be rapidly displayed to command leadership who require near-real time intelligence in order to make decisions during operations. This is one of the premises of the US' initiative to digitize the battlefield thus minimizing the fog of war. Digitizing the battlefield is a complex task. Painful trade offs must be made such as electronic gathering of data focusing on the intelligence of "red forces", versus the electronic gathering of data focusing on infrastructure data. Quickly a soldier can become

---

[48] Michael Lee, "Geospatial Intelligence (GEOINT) and Intelligence Surveillance and Reconnaissance (ISR) convergence," *SPIE Defense, Security, and Sensing* 8740, (2013): 3.

[49] Hank Savitch, and Grigoriy Ardashev, "Does terror have an urban future?," *Urban Studies* 38, no. 13 (2001): 2515.

overwhelmed by the amount of data. To assist Canadian soldiers on expeditionary operations, lessons can be learned from the US' 1st Space Brigade commercial imagery teams. In 2012-2013, these teams were capable in fewer than 24 hours of producing and disseminated imagery to those at the front line. The imagery products were used for analysis and reallocation of assets making them "more combat-effective."[50]

## INFORMATION MANAGEMENT

Strategy 2020 speaks to the need of changing DND/CAF's business management practices brought about by technological revolution. DND/CAF's investment in R&D on the operational needs of the department must also capitalize on advancements in Information Management (IM). R&D is critical to avoid dependencies upon legacy systems. Reuse of "legacy systems is frequently touted as the solution to cost, efficiency, and time-to-delivery problems; however, cost overruns and technical difficulties can significantly diminish any perceived benefits."[51] One significant DND/CAF defence S&T initiative is to modernize many of the business processes and legacy systems related to finances and the maintenance of military equipment with the new Defence Resource Management Information System (DRMIS). DRMIS is used primarily to capture and record every element of the business processes of defence resources. DRMIS is a computer-based tool created from the amalgamation of the previous Materiel Acquisition & Support Information System (MASIS) and Financial Management Accounting System (FMAS). One module of DRMIS received a significant overhaul intended to simplify

---

[50] Richard P. Formica, "The Present and Future Of Army Space And Missile Defense," *Army Magazine* 63, no. 10, 2013, 142.

[51] Meredith Eiband, Timothy J. Eveleigh, Thomas H. Holzer, and Shahryar Sarkani, "Reusing DoD Legacy Systems: Making the Right Choice," *Defense Acquisition Research Journal* 20, no. 2 (2013): 154.

tracking equipment availability thus ensuring the highest levels of operational readiness. The DRMIS upgrade shows that DND/CAF had the right idea; implement a defence S&T project that aligns itself with corporate goals and apply IM to target a specific area where process improvement is desperately needed. CAF's front-line combat ability is a high priority, likewise supporting personnel, and performing the required maintenance in order to keep ships, airplane, and land vehicles fully operationally and performing at their highest levels. The level of defence S&T change required by DND/CAF to undertake the significant amalgamation to DRMIS had a high degree of risk and required a complex, holistic solution beyond simple automated tracking of parts by converting paper-based systems to electronic files. This defence S&T change and risk are further defined by the author as the requirement to support core DND/CAF business functions, while maintaining the sustainment of ongoing deployed operations/unit, compounded by the need for secure access to military data across all environmental components. DRMIS was implemented by creating SAP extension modules to the existing MASIS and Financial Management Accounting System (FMAS). To accomplish the project, defence S&T development resulted from changes in DND/CAF commensurate with business process reengineering more commonly witnessed in civilian enterprises. The end result was improved readiness of the operational combat fleet.

DND/CAF as a large government organization had many alternative S&T approaches it could have taken to implement DRMIS. One of DND/CAF's intentions was to reduce the number of legacy systems throughout the department by integrating business processes. A defence S&T project of this magnitude, complexity, and risk was best handled through outsourcing, which relieved DND/CAF of the burden associated

with hiring specialized IT workers on contract to internally develop and implement DRMIS. Most likely this would have increased project risk and may not have resulted in the most advanced S&T solution simply by the fact that DND/CAF does not possess the same level of technical expertise as those from civilian enterprises. It also enabled DND/CAF to focus on executing its core competency of deploying military resources in support of domestic security and government foreign policy objectives rather than programming software. Notwithstanding that the outsourcing approach also has trade-offs needed to achieve success, DND/CAF was required to give up control over its S&T processes in exchange for an off-the-shelf solution that DND/CAF was not realistically in a position to develop.

In the end, there were substantial defence S&T benefits and breakthroughs to DND/CAF operations when DRMIS was introduced. A KPMG case study stated that some of the post-implementation process changes and performance metrics achieved with the introduction of this new technology are:

> All financial systems and processes were successfully tested for stability, reliability and interoperability within the new DRMIS platform, while more than 6,500 finance end-users were trained on the new system in both Canada and in Canadian Forces deployments around the world. The amalgamated system also provided DND with a software platform that could easily be expanded in the future to both accommodate new business areas and replace other legacy systems running throughout the organization.[52]

For the most part, DND/CAF's implementation of DRMIS using the defence S&T strategy at the national and international levels exemplifies some of the positive aspects

[52] KPMG. *Creating a More Integrated Defence Force.* Canada's Department of National Defence. Case Study – Technology Utilization (November 2012).

of developing new and emerging technology. DRMIS was an outsourced solution to address serious deficiencies and duplication in Forces' processes identified during strategic level review. Most importantly, DRMIS was a systematically conceived S&T solution, not the consequential outcome of a bulk purchase of S&T spending without the implementation of a coherent strategy.

## CANADIAN TECHNICAL EXPERTISE

Strategy 2020 speaks to capitalizing on leading edge technologies, while exploiting Canadian technical expertise. As another example of this, this paper will examine the Public Works and Government Services Canada (PWGSC) approach to leveraging collaborative efforts and research through a government initiative called the Build in Canada Innovation Program (BCIP). This program draws comparisons from the US military's Quick Reaction Fund which touts benefits of "quicker fielding of new or improved technologies, cost savings, …, innovative technologies from smaller firms and companies that have not done business with DOD in the past."[53] Canada's version, BCIP, "helps companies bridge the pre-commercialization gap by procuring and testing late stage innovative goods and services within the federal government."[54] Specifically there is a military component to the program which provides real-world evaluation of pre-commercial goods and services for use in military applications. The result is the exploitation of Canadian innovative technology through the provision of world class scientific technical solutions. Other examples around the globe include NASA's use of

---

[53] Department of Defense, *Defense Technology Development: Management Process Can Be Strengthened for New Technology Transition Programs* (GAO-05-480. GAO Reports 1, 2005), 3.

[54] Public Works and Government Services Canada, Military Component, "Overview of BCIP," last accessed 17 May 14, https://buyandsell.gc.ca/initiatives-and-programs/build-in-canada-innovation-program-bcip/overview-of-bcip.

the CANADARM, the International Space Station's use of CANADARM2, and the Defense Advanced Research Projects Agency (DARPA) Grand Challenge which encourages "inventors to develop robots that could be placed in dangerous situations instead of soldiers."[55] It is also worth mentioning that the Canadian Space Agency has been heavily involved in space technology for years, now it is a matter of DND/CAF leveraging that R&D and leading edge technologies to benefit Canadian military operations.

Earlier in this paper, the topic of terrorist plots to contaminate drinking water was introduced. What does civilian technical expertise in defence S&T and water have in common? As one example, while acknowledging the importance of water and the risk of a limited supply, the civilian "defence industry has been working on ways to make drinkable water out of mud, removing bacteria, viruses…"[56] Another example is within the BCIP posting of November 2012 where industry feedback with the integration of the DRMIS is solicited. BCIP was looking to leverage a collaborative effort to shape the DRMIS requirements, examine potential alternative solutions, and help define a procurement strategy to meet CAF's objectives.[57] And again later in January 2014, CAF sought assistance from civilian commercial expertise in the form of In-Service Support (ISS) Maintenance Services, which include updating systems as technologies evolve, the development and integration of extensions of existing functionality for financial, materiel

---

[55] B. Sampson, "Robots to the rescue," *Professional Engineering* 21, no. 15 (2008): 35.

[56] Denis Merklinghaus, "The Defence of Water in the International War on Terror," *Military Technology* (July 7, 2008): 7.

[57] Public Works and Government Services Canada, "DRMIS Integrated Support Services: Industry Engagement (W8474-126279/A)," last accessed 16 May, https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XQ-003-25106.

acquisition and supply, program and investment and planning management.[58] By tapping into civilian commercial technological developments, the CAF garners quicker access to these S&T developments and expertise, as opposed to having to develop it. Specifically, "leveraging civil investment and ensuring that defence investment is targeted in areas where it can most add value is critical."[59] The end result is pushing/disseminating R&D costs downstream, yet still benefiting upstream from the enhancement of defence S&T capabilities. This concept was also utilized by the US Navy in 2010 when it embarked upon improvements to its acquisition initiatives seeking the best possible dollar value. [60] The US Navy's streamlining of acquisition improvements, while leveraging civilian enterprise and building expertise in manufacturing improved the speed to the fleet of projects by years resulting in cost savings of $650 million.

Remaining with the discussion of capitalizing on leading edge technologies, another government programme that leverages civilian technical expertise in the development of policy is Canada's International Security Research and Outreach Programme (ISROP). ISROP is part of the International Security and Intelligence Bureau of Foreign Affairs, Trade and Development Canada. "ISROP represents the Government's vision for guiding Canada's development of international security policy."[61] Specifically, a key element of ISROP's doctrine revolves around Canada's

---

[58] Public Works and Government Services Canada, "DRMIS Integrated Support Services: Request for Proposal (RFP) for the In Service Support," last accessed 16 May 14, https://buyandsell.gc.ca/cds/public/2013/12/04/39d4915ffd9fd4f8e8d5893f1bb88e3a/ABES.PROD.PW__XQ.B003.E26653.EBSU000.PDF.

[59] RAND Corporation, "Future Technology Landscapes," last accessed 29 May 2014, http://www.rand.org/randeurope/research/projects/future-technology-landscapes html.

[60] Mark Vandroff, "Navy Raises the Bar," *Defense AT&L* 42, no. 5 (2013): 18.

[61] Foreign Affairs, Trade and Development Canada, "International Security Research and Outreach Programme: Terrorism," last access 17 May 2014, http://www.international.gc.ca/isrop-prisi/index.aspx?lang=eng.

Counter-Terrorism Strategy, and one particular ISROP Research Priority for 2013-2014 was terrorism trends. Much in the same manner that BCIP seeks industry feedback from civilian experts as described above, ISROP seeks Canadian researchers and experts to submit proposals in order to conduct research that the Canadian Government considers relevant to its security priorities and policies. It is valuable for consideration within the CAF's defence S&T strategy and therefore reviewed in this paper.

ISROP sought civilian researchers to submit proposals with a view of seeking to learn more on crime and terrorism, connections to terrorist and international criminal organizations, and what implications that would mean for Canada's security and foreign policy. Submissions to ISROP's research competition are expected to demonstrate "new ideas/perspectives on policy-relevant issues."[62] The end result is that government officials obtain research products from experts on specific issues, which unsurprisingly broadens their scope and breadth on topics before promulgating policy. This goes hand in hand with initiating a dialogue on emerging technologies with the Canadian community. In a sense, it is a joint venture and mechanism to discuss the development, and potential transfer of technology to the Government. This partnership is central to success of managing defence S&T strategy. It broadens the Government's collaborative approach from federal, and provincial agencies of government to also include civil society. Interestingly, ISROP has a high success rate averaging 4-5 civilian commissioned research projects per year.

Civilian technical expertise is also exploring areas that DND/CAF does not possess any experience. For DND/CAF to explore and invest in new highly technical

[62] *Ibid*.

concepts, it would have to invest heavily in infrastructure, highly educated staff, and start from the beginning. However, by leveraging non-military technical skills, DND/CAF leapfrogs the early stages of development and is able to quickly implement prototypes. One example of an exceptionally technical field is the use of polymer nanocomposites in defence applications and platforms. This defence technology can be used in fire retardation, signature reduction from radar and microwave sensors, to body armour. To wit, the use of nanocomposites in ballistic protection will lead to "more flexible armour with reduced weight."[63] This would represent a tremendous benefit for soldiers operating in austere combat zones such as Iraq and Afghanistan. Conversely, it would take DND/CAF decades to even begin to approach the level of proficiency as technical firms.

This chapter began by stating that DND/CAF have a reputation for being a decade behind private organizations in their R&D and in terms of adopting new S&Ts. Nevertheless, the "global defence industry is constantly on the lookout for technologies which have been proven in the civilian domain, which can be 'spun onto' military subsystems and platforms."[64] Canadians are reminded that developing defence technologies is an intangible concept and can be likened to an insurance policy that protects the home. Like a home fire, one never knows where or when an unseen enemy strike will occur. One may never need home insurance policy, but one keeps paying on the premium ... just in case. Without a home insurance policy, when disaster strikes, the family loses the home; without a sound Canadian defence S&T strategy, when disaster strikes the citizens lose their country. Likewise, in matters of defence technology, it is

---

[63] R.V. Kurahatti, A.O. Surendranathan, S.A. Kori, N. Singh, A.V.R. Kumar, and S. Srivastava, "Defence Applications of Polymer Nanocomposites," *Defence Science Journal* 60, no. 5 (2010): 556.

[64] Tom Withington, "Flying Off the Shelves: Naval Applications for Civilian Technology," *Naval Forces* 32, no. 6 (2011): 55.

up to DND/CAF and through their elected government, to decide how to best protect the country and prepare the armed forces. It is for these reasons that Canada continue to invest in R&D initiatives in the areas of space to upgrade its classified communication networks and ensuring they cannot be jammed by enemies, remote sensing as seen with the MSOC example above, geospatial intelligence in order to exploit and analyse intelligence faster than the highly mobile enemy, information management such as DRMIS in order to maximize the readiness of the CAF's combat forces, and leverage Canadian technical expertise through programs such as the BCIP and ISROP.

The focus of this paper will now shift to examining a third target of the Strategy 2020 framework. This target seeks to manage CAF interoperability with the US and other allies. The importance of interoperability to Canada is that it reduces the exposure of risk of terrorism by bringing about the collective muscle of multi-national defence combat forces. It means finding efficiencies through interservice and allies to leverage the commonality of joint/combined C4ISR in order to best adapt and react to the ever changing terrorist threat and thus develop a comprehensive defence S&T strategy.

## CHAPTER 4: MANAGE CANADIAN INTEROPERABILITY RELATIONSHIP WITH THE US AND OTHER ALLIES TO PERMIT SEAMLESS OPERATIONAL INTEGRATION AT SHORT NOTICE.

A third target of the Strategy 2020 framework that this paper will review is to "manage [Canadian] interoperability relationship with the US and other allies to permit seamless operational integration at short notice."[65] This ties in with the thesis of this paper which is the determination of the threat to Canada, followed by developing a governing paradigm for managing a defence S&T strategy as a counter-terrorism measure. Why is the interoperability relationship with the US and other allies important to Canada? Put simply, terrorism is a global threat and Canada cannot combat it alone. Only through encouraging Canadian defence systems and defence organizations to work together, on a pan-Canadian and global scale, can the risk of exposure to terrorism and asymmetrical threats be minimized.

In its simplest term, interoperability means to inter-operate. This can involve social and political levels, engineering systems, technology, armed forces, and so many more. Force interoperability is defined in NATO "as the ability of the forces of two or more nations to train, exercise and operate effectively together in the execution of assigned missions and tasks...to achieve Allied tactical, operational and strategic objectives."[66] Only through such interoperability can Canada seamlessly operate, within a coalition for instance, at short notice. However, interoperability must begin at home before being expanded to other nations. This paper will now examine interoperability within the CAF's component commanders.

---

[65] Department of National Defence, *Defence Strategy 2020*, Shaping the Future of the Canadian Forces A Strategy for 2020 (Ottawa, 1999), 10.

[66] NATO, *Glossary of Terms and Definitions*, (NATO AAP-06).

## INTEROPERABILITY – INTERSERVICE AND INTERAGENCY

DND and by extension the CAF, being complex and hierarchical government organizations, naturally encounter bureaucracy and opposition to organizational change during implementation of defence S&T projects with significant impact on the way personnel operate. There is long-standing naturally occurring competition between the Navy, Army, and Air Force elements of CAF. This rivalry can negatively exacerbate S&T during periods of downsizing from the perspective of personnel and government budget funding allocations. These factors, by extension, affect DND's ability to develop national and international defence S&T doctrine. Like any industry with multiple large groups, when resources are limited and materiel is scarce, component commanders might become quick to point the finger and lay blame for inefficiencies.

The Program Management Board (PMB)[67] is chaired by the Vice Chief of the Defence Staff (VCDS) and allocates precious future year funding while balancing the operational needs of the CAF as an entire entity. It is here that some of the most visible interservice rivalry can crop up. Between the Navy, Army, and Air Force, each component commander, logically, wishes to push ahead their respective initiatives that will be best suited for their future defence technology. "Navy, Army, or Air Force projects should have a common goal and, where appropriate, develop along a common path. [The Auditor General of Canada] found that projects often proceeded along service-

[67] PMB is responsible for strategic planning options and resource allocations in order to develop the capabilities required to produce strategically relevant, operationally responsive, and tactically decisive military forces. Membership includes Defence Assistant Deputy Ministers and Environmental Component Commanders.

specific 'stovepipes'".[68] Imbalance, or perceived imbalance, is the impetus for interservice rivalry. Rivalry can also expend upward beyond the DND, to OGDs, who likewise, are competing for scare government resources.

When it comes to Canadian interagency[69] interoperatibility, the question is always *where is the best place to start* keeping in mind the scope of the direct threat to Canada and how best to react within a defence technology perspective. Avoiding stovepipes between the various organizations is always high on the list. This avoids planning in isolation, redundancy, loss of efficiencies, and much more. To wit, during an integrated domestic Government of Canada response, all involved federal government institutions assist in determining overall objectives, contribute to joint plans, and maximize the use of all available resources.[70] The Minister of Public Safety leads the Federal Government in the co-ordination of their coordinated response. For all operations but defence and aeronautical SAR, the CAF will be in a supporting role for domestic operations in accordance with the Emergency Management Framework for Canada. At the federal level, one can expect coordinated responses from federal governments and their partners, and coordinated responses from provincial, territorial and municipal emergency services. Departmental leads in joint planning must be sensitive to differing perspective and differing cultures of their departments. For instance, the Department of Industry, the Department of Transport, and the DND might not share all the same priorities, yet under

---

[68] Office of the Auditor General of Canada, "National Defence - C4ISR Initiative in Support of Command and Control," *Report of the Auditor General of Canada to the House of Commons*, Ottawa, April 2005.

[69] For the purpose of this paper, "interagency" includes Departments, Entities in Departments, Other Entities associated with Departments, Statutory & other Agencies, Agents of Parliament, Departmental Corporations, and Service Agencies.

[70] Government of Canada - Public Safety, "Emergency Management Planning," last accessed 25 June 2014, http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/mrgnc-mngmnt-plnnng-eng.aspx.

the Department of Finance and Treasury Board's (TB) authority may be required to cooperate. This can lead to a confusing and cumbersome operational planning process, hence why it is critical, as much as possible, to train together, exercise together, and to operate together. The Department of Fisheries and Oceans working in conjunction with DND/CAF conducting fisheries patrols off Canada's coasts is an example of such a cooperative approach. DND/CAF and the RCMP cooperate on drug interaction initiatives. The Canada Border Services Agency, DND/CAF and the Department of Foreign Affairs and International Trade (DFAIT) cooperate at various levels for tracking terrorists and CAN/US border control. In each of these examples, there is the sharing of defence S&T, which includes intelligence, communication, personnel, resources, and so forth. The overriding premise must also be on the end state, which is protecting Canada's interests.

Canada's interoperability and interagency defence S&T strategy to protect Canada's interests must be rooted first with homeland defence, and thereafter in international responses. An example of this is set out under the Canadian Joint Operations Command (CJOC) representing the basic building blocks from which to begin an interoperability defence technology framework. CJOC treats Canada as an operational theatre and has six Joint Task Forces: North, Pacific, West, Central, East and Atlantic. This framework represents a solid foundation for building a Canadian defence technology doctrine that embraces the defence of Canada as a whole of government approach. CJOC is comprised of maritime, land, and air capabilities, both Regular Force and Reserve, which are designed to defend Canada. Further, CJOC has task forces deployed on

expeditionary operations around the world. In fact, CJOC epitomizes the concept of interoperability with global operations spanning the world.[71]

As pointed out earlier in this paper, the MSOC is vitally important and relevant in today's fast paced interconnected defence technology world. The MSOC provides capabilities to CJOC in the defence of Canada, much in the same way that the Joint Force Air Component Commander and the Maritime Component Commanders are integrated into the CJOC framework forming a complete Canadian defence technology matrix. This interoperable framework of partners in operations also "develops, generates and integrates joint-force capabilities to ensure harmony of activity"[72] in the following areas of defence S&T: C4ISR, information operations/influence activities, space operations, cyber, and operational support activities.

INTEROPERABILITY - ALLIES

Recognizing that terrorism is an international threat, crossing all borders, Canada must strengthen its military relationships with allies ensuring interoperable forces. Interoperability must take full advantage of C4ISR to provide world situational awareness to commanders with a view of determining how best to allocation resources and maintain a strategic focus.

Not surprisingly, all three Strategy 2020 targets listed in this paper thus far are also reflected in the current CFDS. In terms of C4ISR, Canadian defence S&T doctrine

[71] The only global operations that CJOC is not involved with are those of the Canadian Special Operations Forces Command (CANSOFCOM) and North American Aerospace Defense Command (NORAD).

[72] National Defence and the Canadian Armed Forces, "Canadian Joint Operations Command," last accessed 26 June 2014, http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page?

must acknowledge the risks of being an early adopter of new military technologies to combat against asymmetric treats and capitalizing on leading edge technologies conceding that "modern and state-of-the-art military systems are becoming increasingly complex and reliability problems may invariably surface due to design deficiencies, systems integration, or immature technology."[73] A reliable and effective way of mitigating against early adoption problems is to share the risk. In other words, with an interoperability relationship with the US and other allies, equipment compatibility with Canadian principle allies, and joint and combined exercise programs to include all environments and exchanges with the US, Canada would benefit from economies of scale. "National Defence estimates that by 2015 it will have invested almost $10 billion on projects to improve the way it gathers, processes, and uses military information. This is needed to provide commanders with better information for decision making in order to exercise faster and more effective command and control in both joint and combined operations. It is also to allow National Defence to keep up with the progress and changes being made by allies."[74] To facilitate interoperability, CAF "strategic, operational, and tactical doctrine must be consistent with the doctrine of our principal allies and alliances…with the armed forces of the United States (US), the United Kingdom (UK), Australia (AUS), and New Zealand (NZ)."[75] Canada would not be required to lead the way, rather Canada could chose to accept proven defence technologies and/or share the risk of trying to innovate new unproven defence technologies. This trend is also evident

[73] Wayne ER and Kim Hua, "Reliability Growth Planning and Analysis of a Combat System: Using Duane Model and Crow Extended Reliability Growth Model," *Defence Science and Technology Agency DSTA Horizons* (2007): 97.

[74] Canada. Office of the Auditor General of Canada, "National Defence—C4ISR Initiative in Support of Command and Control," *Report of the Auditor General of Canada to the House of Commons*, April 2005.

[75] Department of National Defence, B-GJ-005-000/FP-001, Doctrinal Interoperability With Allies, *Canadian Forces Joint Publication*, (Ottawa: Canada, 2009), 1-4.

in other markets such as South America where defence cooperation and interoperability is capitalizing on new products. For instance, "Venezuela is importing on a massive scale, buying exclusively from the US and the most relevant European countries; and cooperation agreements are being met by Argentina, Brazil, and Chile followed by Columbia and Peru."[76]

CAF's international operations, such as the Global War On Terrorism, must be harmonized with Canada's overall foreign policy, which states that "[c]ounter-terrorism requires effective international cooperation and coordination"[77] Because terrorists can strike from anywhere with very little sophisticated defence technology, CAF and allies must focus on interoperability. The interoperability also applies to leveraging each other's S&T. If Canada does not keep its own defence technology doctrine current and relevant, or it arbitrarily dismisses a major innovation, it could quickly find itself obsolete and incapable of functioning jointly on a C4ISR level with modern allies. Such a fundamental change or major innovation could affect how Canada is perceived and whether or not it is invited to participate in a coalition. A major innovation can have a dramatic affect on how forces interoperate. For instance, if the US upgrades their classified communication suites and can no longer communicate with CAF, this could pose serious mission gaps and issues. More drastically, if terrorists start employing new innovations or a new operational procedure and one allied force in a coalition does not adjust, it could pose a serious compromise to the entire coalition. When this is viewed against the quickly changing world as a backdrop, such as the recent talks between the

[76] Juan Carlos Cicalesi, *"*Defence Technology in Latin America*," Military Technology* 37, no. 4 (2013): 38.

[77] Foreign Affairs, Trade and Development Canada, "Terrorism - International Cooperation," last accessed 27 May 2014, http://www.international.gc.ca/crime/terrorism-terrorisme.aspx?lang=eng.

US, South Korea (ROK), and Japan who are currently negotiating a memorandum of understanding on sharing military intelligence[78], Canada's necessity for comprehensive information management and interoperability on short notice becomes ever more significantly fundamental to its defence technology objectives. This dilemma is also being witnessed with the US ballistic missile defence capabilities as they struggle to identify capability gaps. The solution is the timely identification of threats through "persistent intelligence, surveillance, and reconnaissance capabilities at both the global and regional level."[79]

## INTEROPERABILITY - EFFICIENCIES

Thus far, this paper has explored interoperability by looking inward (interservice), by looking outward (allies), and now it will combine the two points of view to understand efficiencies of interoperating.

Canada will continue to operate in mixed environments for the foreseeable future. DND/CAF will have forces deployed across the globe working with allies. This chapter has argued that interoperability reduces operational complexity and risk. The more Canadian defence systems work together, the more substantial the benefits all organizations will enjoy. One would hope that the synergy created by multi-national defence operations would yield world lessons learned and best-of-breed defence technologies. Deep integration of exchange command teams, and joint operations also leverages Canada's existing defence investments, with an eye on future developments. Deep integration needs to incorporate the defence industrial base, both leveraging

[78] The Diplomat, "South Korea and the Trilateral Dilemma, " last accessed 28 June 2014, http://thediplomat.com/2014/06/south-korea-and-the-trilateral-dilemma/.

[79] Richard Weitz, "US Missile Defense," *World Affairs* 176, no. 2 (2013): 86-87.

defence technology and allowing defence imbeds, who are soldiers working inside defence industries providing first-hand insight into defence requirements and military specification (MILSPECS). The result is to have "an industrial base, preferably an integrated civilian/defense base, capable of supporting national security needs within the constraints of a smaller budget and rapidly changing technology environment."[80] This effectively extends the functionality of Canadian defence systems, while trialling new defence technology to ensure compatibility with allied systems. The end result is reached with the seamless operational integration.

## INTEROPERABILITY - IDEOLOGIES

In the context of the enemy, the argument was presented earlier that Canada is fighting a war of ideologies from which terrorism is used as a means to an end. If this is the case, how does one fight ideology through the use of defence technology? How can Canada and its allies focus R&D efforts and S&T initiatives towards such a nebulous concept as ideology? Lastly, how can fighting ideology improve Canada's interoperability and operational integration? It is interesting to note that this has all happened before, and there are valuable lessons that can be harvested from those events. This paper will explore the well known example of the British Malaya campaign which focused on the nature of the insurgency, the strategies, techniques, and methods used by governments and supporting armed forces to defeat the insurgents.

[80] Linda Brandt, "Defense conversion and dual-use technology: The push toward civil-military integration," *Policy Studies Journal* 22, no. 2 (1994): 360.

The source of the insurrection was the Malayan Communist Party (MCP).[81] From 1945-1948 it had adopted a united front strategy, using political and union activity. Neither the government nor the economy had recovered from wartime, the administration and security forces were undermanned, and the political future of Malaya was still uncertain – prime breading grounds for insurgents. As such, the insurgents' strategies and techniques consisted of small scale attacks and sabotage intended to disrupt Malaya's rubber exports and thus weaken its value to Britain. However, with the passage of time the insurgent actions increased their level of violence. They aggressively provoked armed conflict with intimidation, assassination, sabotage, and rioting.

The lesson to be learned from this example is to exploit intelligence from the locals in order to ascertain the movements and intentions of the insurgents in the form of counter-insurgency information. Once again, this falls in line with Canada's Ministry of Public Safety strategy labelled *Building Resilience Against Terrorism,*[82] which advocates "Prevent" as one of their key tenets. Recognizing that many terrorist organizations are comprised of multiple locally based tribal networks, advantage can be gained through psychological warfare against these insurgents aimed at weakening their group morale and encouraging infighting.[83] These measures target the insurgent leadership to increase tensions between key leaders and their followers – preventing a cohesive terrorist plot to develop and slowing the execution of their plans. Although the British Malaya example was at a time of not overly sophisticated defence S&T, the principles remain the same.

---

[81] Paul Dixon, "'Hearts and Minds'? British Counter-Insurgency from Malaya to Iraq," *The Journal of Strategic Studies* 32, no. 3 (2009): 369.

[82] Ministry of Public Safety, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy,* (Ottawa: Canada, 2011), 14.

[83] Department of Defense, Report to Congress, "Insurgents Weaknesses and Vulnerabilities," *Report on Progress Toward Security and Stability in Afghanistan and United States Plan for Sustaining the Afghanistan National Security Forces* (April 2010), 21.

The trouble with some intelligence is that it is a trailing-indicator, meaning the event has usually already taken place. The ideal intelligence for a commander is a leading-indicator, meaning a predictor of what might happen. Nowadays C4ISR can provide a fairly robust understanding of the battlefield in near real time. In terms of harvesting leading-indicator intelligence on potential terrorists' plans or goals, governments mine social media looking for the prediction of future terrorist attacks or foreign uprisings. Virtually "all terrorist organizations have websites. However, al Qaeda is the first to fully exploit the internet"[84] including vast use of social media. Intelligence analysts sift through millions of online posts on familiar sites such as Twitter and Facebook. It is the golden age of obtaining open intelligence as people post every thought in their blogs. Although terrorists now know that such blogs are mined, intelligence gathering can also hack computer systems, track the volume of online traffic, the momentum of posts and utilize spyware which tracks computer systems. The aggregate of this information could point to an area of terrorist interest.

The flip side of social media is the ability for government to also post and blog online. President Obama was a huge advocate of the White House providing a window into his policies and commenting upon events stating that his "administration is committed to creating an unprecedented level of openness in government…to ensure the public trust and establish a system of transparency, public participation and collaboration."[85] The White House permits questions to be asked, with responses posted

---

[84] United States. Homeland Security Subcommittee Hearing. "Jihadist Use of Social Media - How to Prevent Terrorism and Preserve Innovation." last accessed 9 June 2014, http://homeland.house.gov/hearing/subcommittee-hearing-jihadist-use-social-media-how-prevent-terrorism-and-preserve-innovation.

[85] The White House. "We The People, Your Voice In Our Government." Last accessed 9 June 2014, https://petitions.whitehouse.gov/.

online as well. This type of S&T replaces the days of walking through villages and speaking with locals as witnessed during the British Malaya campaign. Governments can influence the information and opinions being formed. From this perspective, and the strategy of "Prevent", negative ideologies may be reshaped.

It is submitted that the most influential voice in shaping ideologies comes from the collective global forum.[86] In other words, if global opinion on a sensitive political subject is fractured and not unified, then there are likely dissidents on that topic. These dissidents will be voicing their opinions, trying to attract other likeminded dissidents – a type of warmongering. Historically, attempts have been made to break up a coalition, for instance the attempts to disrupt/dissolve the coalition as witnessed after the Madrid attacks,[87] by leveraging world opinion and the opinions of their voting constituents. However, if global opinion is not fractured with most countries agreeing on the subject, then there would be minimal polarized world opinions. When forming an international coalition, for instance, knowing global opinions helps improve Canada's interoperability and operational integration by ensuring the Canadian voting constituents solidly back Canada's involvement.

## SEAMLESS OPERATIONAL INTEGRATION

As the so called Global Village continues to bring nations together so do the technological advancements making the world that much more connected. More and more countries are opening their borders and have increased their level of interdependence with other nations. This makes Strategy 2020's framework for

[86] Manfred Steger, Ideology. Blackwell Publishing Ltd, 2002.

[87] William Rose, Rysia Murphy, and Max Abrahms, "Does terrorism ever work? The 2004 Madrid train bombings," *International Security* 32, no. 1 (2007): 185.

managing interoperability relationship with the US and other allies to permit seamless operational integration more relevant today than when the doctrine was published. To wit, an "Alliance of 28 nations can only work effectively together in joint operations if provisions are in place to ensure smooth cooperation. NATO has been striving for the ability of NATO forces to work together since the Alliance was founded in 1949."[88] Further, Canada's Ministry of Public Safety framework[89] of Prevent, Detect, Deny and Respond are all highly more successful in stopping terrorists' attempts with a cooperative approach and seamless operational integration. It is for all these reasons that Canada, the US, and its allies must work together for international peace and security.

Seamless operational integration must first start at home in Canada. CAF environmental commanders, Navy/Army/Air Forces, must work in unison. The days of interservice rivalry must give way to joint operations with greater synergies. Likewise, DND/CAF must work with OGDs and other agencies. The MSOC example mentioned earlier is a demonstration of the potential gains of working together. Doing so will ensure maximization of limited resources, and more importantly a focused common purpose.

DND/CAF must work to achieve and maintain interoperability with other forces, such as the US. A focus of interoperability steers future Canadian development in key C4ISR areas. This focus is two fold: 1) credibility with Canadian partners; and 2) ability to participate by virtue of having compatible equipment. Make no mistake, this is a difficult task when dealing with other nations. For instance, US mission objectives and

---

[88] NATO, "Interoperability: Connecting NATO Forces," last accessed 7 June 2014, http://www.nato.int/cps/en/natolive/topics_84112.htm.

[89] Ministry of Public Safety, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy,* (Ottawa: Canada, 2011), 14.

priorities may differ from Canadian objectives and priorities. Likewise, a coalition's rules of engagement may differ from Canadian caveats. This may pose the problem of a lack of mutual understanding and thus no common nomenclature (such as strategy, defence technology, military doctrine, level/quality of military training, military culture, and so forth) to best adapt and react to the ever changing terrorist threats.

CJOC's joint operations and exchanges with Canadian partners help to build better understanding. Joint operations allow Canadian systems to work together, and thus find new solutions where those systems may have previously lacked compatibility. In order to be truly beneficial, exchanges must take place at the command and leadership levels. It is at these levels that senior command staff are then able to germinate and cross-pollinate lessons learned to the junior staff with a view of developing new doctrine that is compatible with allies.

Joint operations, however, can be advantageous and disadvantageous. For instance, under NATO's Mutual Support Agreements (MSA), the CAF could be required to ensure the provision of logistics support to other forces. This could place additional strain on Canadian logistic and sustainment organization. Conversely, Multinational Integrated Logistics Units (MILUs) take advantage of economies of scale and thus would yield several advantages to the CAF. Regardless, the overriding concept should be that operational integration with allies must function as an effective learning environment. It should be seamlessly integrated into the operational structure and still maintain the operational necessity of providing responsive support to any commander during a deployment. That unity of effort between the CAF and allies must not lack the full-bodied flavour that should be representative of *seamless operational integration*.

Synchronization of effort will be the central distinction between mission failure and mission success.

Canada must continue to nurture its interoperability through joint operations and exchanges otherwise these traits can atrophy. Upon assuming his duties as Supreme Allied Commander, Europe and Commander of U.S. European Command in May 2013, General Philip M. Breedlove at his confirmation hearing before Senate stated that the "the risk of losing this interoperability was one of his key concerns in thinking about how the North Atlantic alliance moves forward beyond Afghanistan."[90] This collaboration is further epitomized in defence S&T research, in particular with Canada's work on the Radarsat Constellation mission, where allies are "very interested in what we're up to and how a country like Canada…is capable of pulling off such a capable system."[91] Under CJOC's expeditionary purview, Canada is an active participant on large scale exchanges. For instance, Canada is currently involved in the world's largest international maritime exercise called Rim of the Pacific Exercise (RIMPAC 2014) along with 21 other nations. With the goal of operational integration, Canada has contributed: HMCS Calgary (FFH 335), 1 Submarine, CC-130T Hercules, CC-150T Polaris, CF-18 Hornet, CP-140 Aurora, Diving Detachments, Explosive Ordnance Disposal Unit, and Land Forces.[92]

The underlying premises must always be the acknowledgement that Canada cannot do it all alone. Canada must endeavour to inter-operate at every opportunity.

---

[90] General Philip Breedlove, testimony delivered at the Senate Armed Services Committee Confirmation Hearing on the Nomination of Air Force Gen. Philip Breedlove to be U.S. European Command Commander and Supreme Allied Commander, Europe, *CQ Congressional Transcripts* (April 11, 2013).

[91] Chris MacLean, "Surveillance of Space: Collaboration," *FrontLine Defence 2014* Vol 11, No 1.

[92] U.S. Pacific Fleet, Leading America's Rebalance to the Pacific, "RIMPAC", last accessed 21 June 2014, http://www.cpf navy.mil/rimpac/2014/.

This entails interoperability at the interservice level between the component commanders, as well as interagency side by side with OGDs, DFAIT, RCMP, to mention only a few. Further, seamless integration must also extend to working with allies. Leveraging the pan-allied C4ISR during joint exercises and combined operations brings about the greatest worldwide coverage and greatest degree of situation awareness to commanders. With the stand-up of CJOC, combining the best of all defence S&T worlds on a global scale, Canada is well on its way to seamless operational integration.

## CONCLUSION

This paper argued that the Strategy 2020 framework is relevant as a counter-terrorism defence strategy and continues to represent the spirit of the Canada First Defence Strategy (CFSD) and thus can be used as a governing paradigm for managing defence S&T strategy. This led into exploring the determination of the threat to Canada. Each of the three Strategy 2020 targets examined can be leveraged for managing defence technologies. Upon further reflection on what has been presented, it quickly becomes evident that DND/CAF's defence technology is a unique product. It is unique by the fact that Canada must prepare a response to a national crisis, which may or may not happen, and prepare for international responses as well. Both of these responses are predicated on the polymorphic and dynamic nature of terrorists. With a view of determining task tailored capabilities, this paper studied the threat of economic disruptions, use of intimidation strategies, and terrorists' goals. Understanding terrorists' centre of gravity and the likelihood of the risk to Canada are paramount. Further, terrorists' methods are difficult to predict, thus making Canada's defensive posture and thus what S&T to develop difficult to ascertain. This also applies to the risk of cyber warfare and Canada's collaborative use of C4ISR with OGDs, and civilian enterprises to take advantage of the fact that "much military R&D in the public domain has focused on protecting soldiers in the asymmetric counterinsurgency warfare that has dominated the last decade."[93]

DND/CAF have the reputation for being a decade behind in defence S&T and suffer from the utilization of legacy systems. The organizational bureaucracy and S&T project management rigidity resulting from government procurement policies can, and

[93] Malcom Philips, "Nano Defence Technology," *Military Technology* 36, no. 5 (2012): 77.

have, generated their fair share of negative examples related to poorly implemented defence technology. This is despite the extraordinary fact that "leaders are constantly met with new technology in the commercial space that is faster, more efficient and easier to use."[94] This concern is further compounded by the fact that when dealing with non-traditional enemies, speed is critical. The lesson learned by utilizing a holistic approach to re-focusing R&D, DND/CAF are now capitalizing on leading edge technology and exploiting Canadian know-how. This can be witnessed through the leveraging of civilian technical expertise to upgrade DRMIS, as well as the collaborative approach to remote sensing by use in the MSOCs. Space is an expensive proposition. By use of a collaborative approach with respect to classified networks for voice and data, as well as GEOINT for near real-time intelligence, yet continually investing into newly emerging technologies, Canada will enhance battlespace awareness, achieve quicker response times, and obtain real-time reconnaissance from remote sensors.

To maximize interoperability with the US and Allies, Canada must emphasis deep operational integration for the Global War on Terrorism. This can be achieved for homeland defence by use of interservice and interagency collaboration, as well as international responses by way leveraging joint exercises, operations, and exchanges of command teams. CJOC is the lead organization for orchestrating interoperability at the continental level, expeditionary level, and for support operations. The net effect is that DND/CAF's response time to terrorist threats is minimized and combat forces' level of readiness is maximized. Final consideration must be made for the mutual sharing of

[94] A. J. Clark, "Why Government Should Take Advantage of Private Sector's Technology Investments," *National Defense* no. 704 (2012): 61.

C4ISR to achieve efficiencies and synergies as part of the global village for S&T for defence. All this with a view of permitting seamless operational integration.

It is conclusive that developing a governing paradigm for managing a defence S&T strategy as a counter-terrorism measure is one that maximizes collaboration at all levels, and maximizes use of C4ISR to prevent terrorism. Analysis and development of defence S&T enabled solutions can improve interoperability by implementing pan-military technological solutions to military problems incorporating civilian best practices.

# BIBLIOGRAPHY


Abrahms, Max. "What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy." *International Security* 32, no. 4 (Spring 2008): 94.

Alexander, Bevin. *How Wars Are Won: The 13 Rules of War from Ancient Greece to the War on Terror*. Random House LLC, 2007.

"Armed Forces And Government Spending." *Singapore Defence & Security Report* (Q3 2009): 29-34.

"Armed Forces And Government Spending." *Taiwan Defence & Security Report* no. 2 (Q2 2012): 58-63.

Author Unknown. "Asymmetric Warfare, the USS Cole and the Intifada." The Estimate – Political and Security Analysis of the Islamic World and its Neighbours, 12, no. 22 (2000).

Bajcsy, R., T. Benzel, M. Bishop, B. Braden, C. Brodley, S. Fahmy, and C. Rosenberg, et al. "Cyber Defense Technology Networking And Evaluation." *Communications Of The ACM* 47, no. 3 (2004): 58-61.

Bergmann, Kym, "Anti-Ship Missile Defence Impressive Progress." *Asia-Pacific Defence Reporter* 39, no. 2 (2013): 12-14.

Brandt, Linda. "Defense conversion and dual-use technology: The push toward civil-military integration." *Policy Studies Journal* 22, no. 2 (1994): 359-370.

Breedlove, General Philip. Testimony delivered at the Senate Armed Services Committee Confirmation Hearing on the Nomination of Air Force Gen. Philip Breedlove to be U.S. European Command Commander and Supreme Allied Commander, Europe, *CQ Congressional Transcripts* (April 11, 2013).

Brown, John S. "Defense Transformation Redux." *Army Magazine,* 62, no. 11 (2012): 23-26.

Brown, K.J. "CF Transformation: Evolution, Revolution or Innovation? RMA induced by changes in threats: The asymmetric environment." Royal Military College of Canada (2006).

Canada. Association of Canadian Port Authorities. "Public Relations - Port Industry Facts." Last accessed 13 May 2014. http://www.acpa-ports.net/pr/facts.html.

Canada. Canadian Coast Guard. "Marine Security Operations Centres (MSOC)." Last accessed 20 May 2014, http://www.ccg-gcc.gc.ca/eng/CCG/Maritime-Security/MSOC.

Canada. Canada's International Policy Statement. *A Role of Pride and Influence in the World – Defence*. Ottawa, 2005.

Canada. Defence Research and Development Canada. "Science And Technology In Action: Delivering Results For Canada's Defence And Security." Lasted accessed 19 May 2014. http://www.drdc-rddc.gc.ca/en/publications/defence-st-strategy.page.

Canada. Department of National Defence. B-GJ-005-000/FP-001. *Canadian Forces Joint Publication.* Ottawa: DND Canada, 2009.

Canada. Department of National Defence. *Defence Strategy 2020, Shaping the Future of the Canadian Forces A Strategy for 2020*. Ottawa: Canada, 1999.

Canada. Department of National Defence. *The Defence Portfolio 2002.* Ottawa: Canada, 2002.

Canada. Foreign Affairs, Trade and Development Canada. "International Security Research and Outreach Programme: Terrorism." Last accessed 17 May 2014. http://www.international.gc.ca/isrop-prisi/index.aspx?lang=eng.

Canada. Foreign Affairs, Trade and Development Canada. "Terrorism - International Cooperation." Last accessed 27 May 2014. http://www.international.gc.ca/crime/terrorism-terrorisme.aspx?lang=eng.

Canada. House of Commons, Standing Committee on National Defence and Veterans' Affairs. *Minutes of Proceedings and Evidence,* no. 1, May 19, 2005, 1:21.

Canada. Ministry of Public Safety. *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy*. Ottawa: Canada, 2011.

Canada. National Defence and the Canadian Armed Forces. "About the Canadian Armed Forces." Last accessed 2 May 2014. http://www.forces.gc.ca/en/about/canadian-armed-forces.page.

Canada. National Defence and the Canadian Armed Forces. "Canadian Joint Operations Command" Last accessed 26 June 2014. http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page?.

Canada. Office of the Auditor General of Canada. "Aging Information Technology Systems." *Report of the Auditor General of Canada to the House of Commons*. Ottawa, Spring 2010.

Canada. Office of the Auditor General of Canada. "National Defence—C4ISR Initiative in Support of Command and Control." *Report of the Auditor General of Canada to the House of Commons.* April 2005.

Canada. Public Works and Government Services Canada. "DRMIS Integrated Support Services: Industry Engagement (W8474-126279/A)." Last accessed 16 May. https://buyandsell.gc.ca/procurement-data/tender-notice/PW-XQ-003-25106.

Canada. Public Works and Government Services Canada. "DRMIS Integrated Support Services: Request for Proposal (RFP) for the In Service Support." Last accessed 16 May 14. https://buyandsell.gc.ca/cds/public/2013/12/04/39d4915ffd9fd4f8e8d5893f1bb88e3a/ABES.PROD.PW__XQ.B003.E26653.EBSU000.PDF.

Canada. Public Works and Government Services Canada. Military Component. "Overview of BCIP." Last accessed 17 May 14. https://buyandsell.gc.ca/initiatives-and-programs/build-in-canada-innovation-program-bcip/overview-of-bcip.

Chase, Steven. "Ottawa to curb military's role in procurement after costly delays." *Globe and Mail*, 5 February 2014.

Cicalesi, Juan Carlos. "Defence Technology in Latin America." *Military Technology* 37, no. 4 (2013): 38-40.

Ciuriak, D. "Emerging Powers: Governance In A Changing Global Order." *Summary of Proceedings*. Annual Conference, Queen's Centre for International Relations (Kingston, June 14-16, 2005).

Clark, A.J. "Why Government Should Take Advantage of Private Sector's Technology Investments." *National Defense* no. 704 (2012): 61-63.

Council of Canadian Academies. Committee on the State of Science & Technology in Canada. *The State of Science & Technology in Canada*. Council of Canadian Academies, 2006.

Council on Foreign Relations. "State Sponsors: Iran." Last accessed 6 August 2014. http://www.cfr.org/iran/state-sponsors-iran/p9362.

Dibb, Paul. "The Revolution In Military Affairs And Asian Security." *Survival* 39, no. 4 (1997): 93-116.

Diehl, Paul F. "The political implications of using new technologies in peace operations." *International Peacekeeping* 9, no. 3 (2002): 1-24.

Dilanian, Ken. Los Angeles Times. "Terrorists harder to track after Snowden's leaks, officials say." Last accessed 22 May 2014.

http://articles.latimes.com/2013/jun/28/world/la-fg-wn-snowden-terrorists-communications-20130628.

Dixon, Paul. "'Hearts and Minds'? British Counter-Insurgency from Malaya to Iraq." *The Journal of Strategic Studies* 32, no. 3 (2009): 353-381.

Egozi, Arie. "Advanced Technology Solutions." *Defence Review Asia* 7, no. 5 (2013): 15-20.

Eiband, Meredith, Timothy J. Eveleigh, Thomas H. Holzer, and Shahryar Sarkani. "Reusing DoD Legacy Systems: Making the Right Choice." *Defense Acquisition Research Journal* 20, no. 2 (2013): 154-173.

Emeksiz, Ekrem. "International Terrorism Financing." (City University of New York (CUNY) - John Jay College - International Crime and Justice MA Program, 2013): 1-28.

Freedman, Lawrence. "Grand Strategy in the Twenty-First Century." *Defence Studies* 1, no. 1 (2001).

Freedman, Lawrence. *The Revolution in Strategic Affairs*. Adelphi Paper: London, 1998.

Michael Freeman. "A Theory of Terrorist Leadership (and its Consequences for Leadership Targeting)." *Terrorism and Political Violence*, ahead of print (2014): 1-22.

Formica, Richard, P. "The Present and Future Of Army Space And Missile Defense." *Army Magazine* 63, no. 10 (2013): 141-144.

Graves, Brad. "How Military Technology Changes the World We Live In." *San Diego Business Journal* 34, no. 5 (2013): 16-17.

Graves, Brad. "Under The Radar." *San Diego Business Journal* 31, no. 42 (2010): 1-46.

Government of Canada - Public Safety. "Emergency Management Planning." Last accessed 25 June 2014. http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/mrgnc-mngmnt-plnnng-eng.aspx.

Harris, D. "Human Factors Integration In Defence." *Cognition, Technology & Work*, no. 3 (2008): 169-172.

Hartley, Keith. "Collaboration And European Defence Industrial Policy." *Defence & Peace Economics* 19, no. 4 (2008): 303-315.

Hiller, R. "Top General Calls Liberal Rule 'Decade Of Darkness.'" *Ottawa Citizen*, February 2007.

Homeland Security Watch. "Agreed: Terrorist tactics are tough to track." Last accessed 16 July 2014. http://www.hlswatch.com/2013/12/05/agreed-terrorist-tactics-are-tough-to-track.

Horowitz, Michael. "Coming next in military tech." *Bulletin Of The Atomic Scientists* 70, no. 1 (2014): 54-62.

Ihori, Toshihiro. "Arms race and economic growth." *Defence & Peace Economics* 15, no. 1 (2004): 27-38.

Ito, Peter, David M. Moore, Stuart Young, Kevin Burgess, and Peter Antill. "Impact of U.S. Export Control and Technology Transfer Regime on the Joint Strike Fighter (JSF) Project-Views of Key UK Stakeholders." *International Journal Of Defense Acquisition Management* 4, (2011):1-52.

Jordan, Jenna. "Attacking the Leader, Missing the Mark: Why Terrorist Groups Survive Decapitation Strikes." *International Security* 38, no. 4 (2014): 7-38.

Kirkpatrick, David. "The Future Of UK Defence Research." *Defence & Peace Economics* 19, no. 6 (2008): 479-491.

Kurahatti, R.V., A.O. Surendranathan, S.A. Kori, N. Singh, A.V.R. Kumar, and S. Srivastava. "Defence Applications of Polymer Nanocomposites." *Defence Science Journal* 60, no. 5 (2010): 551-563.

KPMG. *Creating a More Integrated Defence Force.* Canada's Department of National Defence. Case Study – Technology Utilization (November 2012).

Lee, Dong Sun. "A nuclear North Korea and the stability of East Asia: a tsunami on the horizon?" Australian Journal Of International Affairs 61, no. 4 (2007): 436-454.

Lee, Michael. "Geospatial Intelligence (GEOINT) and Intelligence Surveillance and Reconnaissance (ISR) convergence." *SPIE Defense, Security, and Sensing* 8740, (2013): 1-3.

Lionetti, Donald M. "Air Defence Technology is Ready Now - Why Wait to Deploy It?" *Military Technology* 34, no. 7 (2010): 169.

MacLean,Chris. "Director General Space: An interview with BGen Rick Pitre." *FrontLine Defence 2013* Vol 10, No 6.

MacLean, Chris. "Surveillance of Space: Collaboration." *FrontLine Defence 2014* Vol 11, No 1.

Merklinghaus, Denis. “The Defence of Water in the International War on Terror.” *Military Technology* (July 7, 2008): 7.

Merritt, Zina D., Kimberly Seay, Emily Biskup, Cindy Brown Barnes, Cynthia Grant, Neelaxi Lakhmani, Jason Lee, Alberto Leff, John Martin, and Charles Perdue. Defense Logistics: Improvements Needed to Enhance DOD's Management Approach and Implementation of Item Unique Identification Technology. No. GAO-12-482. Washington: DC, 2012.

Morgan, Matthew. “The Origins of the New Terrorism.” *Parameters* 34, no. 1, (Spring 2004): 30.

Mumford, Richard. “Second Defence Technology Centre is Launched” *Microwave Journal* 46, no. 10: (2003): 52.

Nacos, Brigitte. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post-9/11 World.* Toronto: Penguin, 2008.

National Commission on Terrorism, and United States of America. "Countering the Changing Threat of International Terrorism." (2000).

NATO. *Glossary of Terms and Definitions.* (NATO AAP-06).

NATO. “Interoperability: Connecting NATO Forces.” Last accessed 7 June 2014. http://www.nato.int/cps/en/natolive/topics_84112.htm.

Neumann, Peter and M.L.R Smith. *The strategy of terrorism: How it works, and why it fails.* New York: Routledge Taylor & Francis Group, 2008.

Nikzad, Rashid. "The Changing Role Of Government Labs In Science And Technology Policy." *Regional Science Inquiry* 1 (2013): 117-126.

Orbons, SJEF. “Do Non-Lethal Capabilities License to 'Silence'*?”* *Journal Of Military Ethics* 9, no. 1 (2010): 78-99.

Philips, Malcom. “Nano Defence Technology.” *Military Technology* 36, no. 5 (2012): 76-78.

RAND Corporation. “Future Technology Landscapes.” Last accessed 29 May 2014. http://www.rand.org/randeurope/research/projects/future-technology-landscapes.html.

Reidy, Heath. “The Best Defence.” *Professional Engineering* 22, no. 5 (2009): 25-26.

Rose, William, Rysia Murphy, and Max Abrahms. "Does terrorism ever work? The 2004 Madrid train bombings." *International Security* 32, no. 1 (2007): 185-192.

Rosen, S.P. "New Ways of War – Understanding Military Innovation." *International Security*, Vol 13, 1998.

Rosen, S.P. *Thinking About Military Innovation. Winning the Next War: Innovation and the Modern Military.* Cornell University Press, 1998.

Rostum, Hussein, Mark MacDonald, and Doug Williams. "Measuring and Ensuring Excellence in Government Science and Technology: Canadian Practices." *The Council* (2001).

Sampson, B. "Robots to the rescue." *Professional Engineering* 21, no. 15 (2008): 35.

SAP. "The Canadian Department Of National Defence Completes First Major Implementation Of The SAP-Based Materiel Acquisition And Support Information System (MASIS)." *SAP Customer Success Story.* The Canadian Navy, 2005.

Savitch, Hank and Grigoriy Ardashev. "Does terror have an urban future?" Urban Studies 38, no. 13 (2001): 2515-2533.

Shearer, David. "Outsourcing War." *Foreign Policy* 112, Fall 1998.

Schilling, William. *Nontraditional Warfare: Twenty-first-century Threats and Response*. Washington, D.C., 2002.

Steger, Manfred B. "Ideology." Blackwell Publishing Ltd, 2002.

The Diplomat. "South Korea and the Trilateral Dilemma." last accessed 28 June 2014. http://thediplomat.com/2014/06/south-korea-and-the-trilateral-dilemma/.

The White House. "We The People, Your Voice In Our Government." Last accessed 9 June 2014, https://petitions.whitehouse.gov/.

"Undersea Defence Technology." *Sea Technology* 54, no. 5 (May 2013): 45-47.

United States. Department of Defense. *Defense Technology Development: Management Process Can Be Strengthened for New Technology Transition Programs.* GAO-05-480. GAO Reports 1, 2005.

United States. Department of Defense. Homeland Security Subcommittee Hearing. "Jihadist Use of Social Media - How to Prevent Terrorism and Preserve Innovation." Last accessed 9 June 2014. http://homeland.house.gov/hearing/subcommittee-hearing-jihadist-use-social-media-how-prevent-terrorism-and-preserve-innovation.

United States. Department of Defense. Report to Congress "Insurgents Weaknesses and Vulnerabilities," Report on Progress Toward Security and Stability in Afghanistan and United States Plan for Sustaining the Afghanistan National Security Forces. April 2010.

United States. Department of Defense. *Strategy for Homeland Defense and Civil Support.* Washington: D.C, June 2005.

United States. Department of Defence. U.S. Pacific Fleet. Leading America's Rebalance to the Pacific. "RIMPAC." Last accessed 21 June 2014. http://www.cpf.navy.mil/rimpac/2014/.

United States. United States Army. *Adapting Our Aim: A Balanced Army for a Balanced Strategy.* Washington, DC: Government Printing Office, 2009.

van Creveld, Martin. *Technology and War: From 2000 BC to the Present.* The Free Press: New York, 1991.

Vandroff, Mark and Kimble, Robert. "Navy Raises the Bar." *Defense AT&L* 42, no. 5 (2013): 17-19.

Vespalcová, Vendula. "Justifying Ballistic Missile Defence: Technology, Security and Culture." *Defense & Strategy* no. 2 (2011): 145-147.

Wayne, ER and Kim Hua. "Reliability Growth Planning and Analysis of a Combat System: Using Duane Model and Crow Extended Reliability Growth Model." *Defence Science and Technology Agency DSTA Horizons* (2007): 97.

Weitz, Richard. "US Missile Defense." *World Affairs* 176, no. 2 (2013): 80-87.

Withington, Tom. "Flying Off the Shelves: Naval Applications for Civilian Technology." *Naval Forces* 32, no. 6 (2011): 55.