CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

JCSP 34 / PCEMI 34

MASTER OF DEFENCE STUDIES RESEARCH PROJECT

The Whole of Government Approach Applied to Canadian National Security

By /par
LCdr/capc B. Henry

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Governments have recognized that the world is undergoing increased levels of instability. They have made changes in their approach to tackling complex issues that span the responsibilities of more than one government department or agency, and are making steps towards increasing the respective levels of interoperability. National security is taking on increased importance in this globalized world, as the traditional boundaries between politics, culture, technology finance, and ecology are disappearing. Additionally, national security threats are no longer simply terrorist or military in nature; they also include natural disasters like earthquakes, hurricanes, floods and forest fires as well as pandemics. The concept of a whole of government approach that integrates, or at least coordinates, the various departments and agencies implicated in national security issues, is essential in facilitating good governance. A coherent and comprehensive whole of government approach reflects an appreciation of the increasingly multidimensional, dynamic, complex and fluid nature of the problem and clearly integrates departments and agencies into a logical, coherent framework.

The purpose of this paper is to examine the efforts undertaken by the Canadian Government towards improving national security through the use of the whole of government approach. The focus is in those areas of national security in which the military has a domestic role to play, with an emphasis on the levels of interoperability between the implicated departments and agencies. The analysis will show that Government initiatives since 9/11 provide the necessary structure and mandate for the various departments and agencies to undertake a whole of government approach. However, in implementation, the initiatives fall short of achieving this goal.

CHAPTER 1: INTRODUCTION

> In the past security was often thought of as largely a military affair. In today's complicated and sometimes bewildering world, security has become a much broader issue. Many of the threats to Canada's security are non-military in nature, and with the changing times have come an understanding that any defence demands the involvement of all elements of society in a way in which security in the Cold War did not.[1]

The global security environment has recently gone through some profound changes. The Cold War came to an end with the collapse of the Soviet Union and the dismantling of the Berlin Wall. The threat of large-scale conventional and state-based wars has dwindled and governments looked to reap a "peace dividend" as many Western nations cut their defence spending and redirected their efforts and funding to social programs and economic growth. Additionally, the world has become an increasingly interwoven place, as we have gone from a Cold War system built around division and walls to a system built around integration and Internet technology. Individuals, corporations and states are able to reach around the world farther, faster and cheaper than ever before as markets, states and technologies become more globalized.[2] While globalization lacks a precise definition, it reflects a widespread perception that the world is rapidly being molded into a shared social space by economic and technological forces and that issues in one area of the world have profound consequences for individuals or communities elsewhere. This changes the traditional boundaries between politics, culture, technology finance, national security and ecology, and increases the breadth, depth and speed of worldwide interconnectedness in all aspects of contemporary social life.[3] The

---

[1] Major General Andy Leslie, "Boots on the Ground: Thoughts on the Future of the Canadian Forces, The 2004 Haycock Lecture," *Canadian Military Journal*, Volume 6, number 4, (Spring 2005), 19.

[2] Thomas L. Friedman, *The Lexus and the Olive Tree*, (New York: Anchor Books, 1999), 8.

[3] David Held, *et al*, *Global Transformations – Politics, Economics and Culture*, (Stanford: Stanford University Press, 1999), 2.

ability to read and understand these connections is important. If you don't see the connections, you don't see the world.[4] However, the speed and scale of social and economic change appear to outstrip the capacity of national governments or citizens to keep up.[5]

Canada has fostered an open society with protected rights and personal freedom of thought and action that is critical to our prosperity and ability to flourish in this increasingly interdependent world. However, this openness was horrifically exploited in the events of September 11, 2001 with an act of terrorism that undermined the core values of our democratic society. This event caused the Canadian Government to undertake actions with a fine balance between the core values of openness, diversity and respect for civil liberties with those of national security.[6] As a result, government will need to assess and effectively deal with a wide range of threats that are primarily ideologically driven, global and networked. More than ever before, every major challenge, from security to the development of social and economic policies, will require the active participation of a wide range of government departments and agencies.

Governments have recognized these increased levels of instability and have made changes in their approach to tackling complex issues that span the responsibilities of more than one government department or agency. A whole of government approach that integrates, or at least coordinates, the departments and agencies implicated in national security issues, is essential in addressing the roots of instability in order to facilitate good governance. National security threats are not always terrorist or military in nature, but

---

[4] Thomas L. Friedman, *The Lexus and the Olive Tree*, (New York: Anchor Books, 1999), 20.

[5] David Held, *et al*, *Global Transformations – Politics, Economics and Culture …*, 1.

[6] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, (Ottawa: PCO, 2004), 3.

also include natural disasters like earthquakes, hurricanes, floods and forest fires as well as pandemics. Therefore, it is not only the military and law enforcement agencies that will need to coordinate their actions and work together, many other departments and agencies will be involved to varying degrees. A coherent and comprehensive whole of government approach reflects an appreciation of the increasingly multidimensional, dynamic, complex and fluid nature of the problem and clearly integrates departments and agencies into a logical, coherent framework.[7]

The purpose of this paper is to examine the efforts undertaken by the Canadian Government towards improving national security in the aftermath of 9/11, through the use of the whole of government approach. The focus will be in those areas of national security in which the military has a domestic role to play. The analysis will demonstrate that the policies outlined in the *National Security Policy* as well as in the *Defence International Policy Statement* provide the necessary guidance and direction for the Government to undertake a whole of government approach, however, in implementation, the Government falls short of achieving this goal. [8] [9] The Government's response to the specific policies will be looked at in detail to outline the relative strengths and weaknesses of the policies, with recommendations provided as to how best to proceed in order to effectively utilize the resources, skills and knowledge of all of the implicated departments and agencies in the whole of government approach to matters of national security. This paper will start with some background information to demonstrate the need

---

[7] Peter Gizewski, "The Future Security Environment: Threats Risks and Responses," *Canadian Institute of International Affairs, International Security Series*, (March 2007), 8.

[8] Department of Foreign Affairs and International Trade, *Canada's International Policy Statement: A Role of Pride and Influence in the World – Overview*, (Ottawa: Department of Foreign Affairs and International Trade, 2005).

[9] Privy Council Office, *Securing an Open Society: Canada's National Security Policy* ….

for a coordinated whole of government approach. The concepts of the whole of government approach will then be examined by exploring the origins and the underlying framework. The dimensions of interoperability, which are measures of the ability of the implicated departments and agencies to work together in an operational setting, will then be studied, as interoperability is critical to the effective and efficient application of the whole of government approach. Next, Canada's application of the whole of government approach towards national security will be considered in detail, with strengths and weaknesses identified and analyzed. Finally, this paper will conclude with some recommendations and a proposed way ahead in order for the Canadian Government to better utilize the whole of government approach in response to threats to national security.

BACKGROUND

Task forces and working groups designed to facilitate interagency coordination have existed for years, but they have usually been ad hoc, limited in authority, and narrow in scope. They were viewed with suspicion by most governmental agencies, as they were considered to be invading on mandates and responsibilities. As a result, such organizations had difficulty breaking down barriers and penetrating information stovepipes. For example, the United States (U.S.) had at least five different terrorist watch lists on 11 September, 2001, and President George W. Bush had previously issued National Security Presidential Directive 1, which replaced 102 interagency working groups with a three-tiered National Security Council system for interagency

coordination.[10] The primary challenge of the whole of government approach is to achieve unity of effort despite the diverse cultures, competing interests and differing priorities of participating organizations.[11]

When adopting the whole of government approach, the various departments and agencies need to be transformed into responsive, adaptive and interoperable organizations capable of providing an integrated response to events that cross departmental boundaries. Although, where necessary or appropriate, their independence must also be maintained, as one of the greatest assets that each organization has is their difference from one another. The purpose of creating each of these individual entities was to get a concentrated focus on the problem from their particular point of view. However, any one organization does not necessarily have all the answers, due to their disparate mandates and expertise. Exposing one organization's specific views and conclusions against conflicting points of view that challenge the processes and outcomes can minimize this weakness. In this manner, multiple perspectives are examined together to create a common understanding rather than introducing multiple independent views.[12] When organized as a whole, it is important to understand how the organizations relate to one another and how they learn to address conflicts, in order to determine just how successful the interdepartmental relations will become. This shared information will help each agency better understand the situation, and will help ensure that each agency is working

---

[10] The White House, *National Security Presidential Directive 1*, (February 2001); available from http://www.fas.org/irp/offdocs/nspd/nspd-1.htm; Internet; accessed 29 February 2008.

[11] Matthew F. Bogdanos, "Joint Interagency Cooperation: The First Step," *Joint Forces Quarterly*, 37; available from http://www.dtic.mil/doctrine/jel/jfq_pubs/0437.pdf; Internet; accessed 29 February 2008.

[12] COL Christopher R Paparone and James A Crupi, "United We Stand, Divided …? Achieving Intelligence Interagency Synergy in Complex Warfare," *American Intelligence Journal*, (Summer 2006), 26-27.

toward the common goal. Leadership in these situations is crucial, as the benefits to this whole of government approach is best achieved when the various departments and agencies are brought together to respond in a collective manner, using their diverse diagnostic tools and perspectives. The challenge for the leader is in their ability to shape a common meaning from a potentially diverse group as opposed to trying to force a pre-conceived position from within their own group. The goal is interdepartmental teamwork and understanding without the "stovepipe" bias inherent in a single organization's approach to problem resolution.

A current example of the implementation of the whole of government approach to solving complex problems can be seen in the conflict resolution activity ongoing in Iraq and Afghanistan. With wars increasingly taking place inside rather than across national borders, they affect whole societies, not just the armed forces. These conflicts devastate economies, damage society, break down social cohesion, destroy traditional cultural patterns, and kill people. Anecdotal evidence suggests that 90 % of the casualties in these conflicts are from within the civilian population. Thus, States have come to realize that new initiatives, processes and methods are required to mitigate the cause of the threat, as well as to manage a coordinated response to the threat. Recognizing the requirement to work in an integrated, joint environment to support the issues surrounding conflict prevention and resolution, the British Department for International Development created the Global Conflict Prevention Pool. This effort combined the resources of their own department with efforts of the Ministry of Defence and the Foreign Commonwealth Office to not only counter global threats but also to achieve integrated solutions to address the root cause of the conflict. Previous to this initiative, each department took

independent responsibility for activity within their own areas of expertise, whereas, this new approach encourages integration, ensuring that each department supported and complemented each other through the use of joint policies to eliminate duplication and increase effectiveness.[13]

Canada has also followed suit, in 2005, instituting its own whole of government approach to foreign policy referred to as the "3D" (diplomacy, defence and development) approach. This approach brought together the Departments of National Defence (DND), Foreign Affairs (DFAIT), and the Canadian International Development Agency (CIDA), in recognizing that issues surrounding global conflict are increasingly interwoven.[14] Military, diplomatic, developmental and law enforcement personnel are working together in a relatively collaborative, cooperative framework to help realize the Afghan National Strategy and thus bring stability, prosperity and good governance to Afghanistan.[15] Ultimately, the objective of the whole of government approach is cooperation and integration in order to provide a comprehensive framework to guide the actions of all participants and thereby maximize the effectiveness across government departments.

While the current spotlight is on the front-line conflicts in Iraq and Afghanistan, where the whole of government approach is on the news on a daily basis, many now realize that this approach can be used for more than just an instrument of foreign policy. The response to Hurricane Katrina in the U.S. highlighted the benefits of having a domestic whole of government organization, with the various agencies involved from the

---

[13] Louise Bell, *The Global Conflict Prevention Pool. A Joint UK Government approach to reducing conflict*, Department for International Development (DFID), Prepared by FCO Creative Services, August 2003, 6.

[14] Department of Foreign Affairs and International Trade, *Canada's International Policy Statement; A Role of Pride and Influence in the World – Diplomacy*…, 10.

[15] Peter Gizewski, "The Future Security Environment: Threats Risks and Responses …, 8.

outset of the emergency. However, it also highlighted the difficulties and dangers in failing to effectively integrate the various government departments and agencies at both the strategic federal levels as well as across multiple levels of government. Having the means to quickly and securely coordinate efforts across agencies is essential. Challenges in communications between the various law enforcement agencies and the firefighters in New York City in the aftermath of 9/11 indicate how all parties involved in terrorist incidents would benefit from shared, secure and durable multi-agency information management and communications.[16] In Canada, the recently released report on the Severe Acute Respiratory Syndrome (SARS) pandemic also indicated that the situation was exacerbated by inadequate coordination and the absence of a sharp focus.[17] These lessons need to be applied at all levels of interdepartmental relationships to prevent similar mishaps in the future and to develop the capacity to quickly assess situations, share information and communicate appropriate action.

---

[16] Fred T. Krawchuk, "Combating Terrorism: A Joint Interagency Approach," *Institute of Land Warfare*, No 05-1 (January 2005), 14.

[17] Archie Campbell, *The SARS Commission Final Report: Spring of Fear*, (Toronto: Ontario Ministry of Health and Long-Term Care, 2006), 17.

CHAPTER 2: WHOLE OF GOVERNMENT APPROACH

> …long-term success depends on the use of all elements of national power: diplomacy, intelligence, covert action, law enforcement, economic policy, foreign aid, public diplomacy, and homeland defense. If we favor one tool while neglecting others, we shall leave ourselves vulnerable and weaken our national effort.[18]

The concept of the whole of government approach is not a new or revolutionary idea. The Committee of Imperial Defence was formed in Great Britain in the late 1800s as an advisory defence planning system instead of creating a Ministry of Defence, as there was political resistance to create a single entity to coordinate defence policy. This committee became the Imperial War Cabinet during both World Wars and included the Dominion Prime Ministers in a consultative discourse regarding the political and military situations being faced.[19] Additionally, in 1951, Prime Minister Winston Churchill placed "overlord" ministers to oversee and coordinate the activities of a number of ministries in order to increase the level of coordination amongst the ministries.[20]

The current reintroduction of this approach "… is the latest manifestation of one of the oldest preoccupations in the field of politics and public administration – the co-ordination of policymaking and administration."[21] One of the reasons for the increased interest stems from some of the negative effects of the New Public Management (NPM) reforms of the 1980s and 90s.[22] NPM was oriented towards providing clear results and

---

[18] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report - Executive Summary*, (Washington, D.C.: Government Printing Office, 2004), 17.

[19] Peter Catterall, *How Imperial was the Committee of Imperial Defence*? (London: Institute of Contemporary British History, 1998); available from http://www.psa.ac.uk/publications/psd/1998/catterall.htm; Internet; accessed 3 April 2008.

[20] David Richards and Dennis Kavanagh, *Can Joined-Up Government be a Reality? A Case Study of the British Labour Government 1997-2000,* Liverpool: University of Liverpool, 2000, 3.

[21] Christopher Pollitt, "Joined-up Government: A Survey," *Political Studies Review*, Vol 1, (2003), 36.

[22] Tom Christensen and Per Laegreid, "The Whole-of-Government Approach to Public Sector Reform," *Public Administration Review*, (November/December 2007), 1059-1060.

increasing efficiency by stipulating specific outcomes for given funding levels. NPM created single-purpose organizations by splitting large bureaucracies into smaller more fragmented ones, which fostered increased competition, both between different public agencies, and between public agencies and private firms. However, by focussing on performance management, single purpose organizations and structural devolution, NPM reforms tended to ignore the problem of horizontal coordination. This increased fragmentation and self-centred authorities made it difficult to coordinate policies, which resulted in government ineffectiveness, departmentalism and vertical stovepipes.[23]

The difficulties encountered in the NPM reforms are not the only reasons for this increased interest in the whole of government approach. The concerns raised by the complex and broad reaching responses required to defend against terrorist attacks, natural disasters and pandemics also underlie the importance of governments working together to avoid contradiction and to share information.[24] There is an emerging interest in the design and implementation of cross-sector collaboration that is focussed on coordinating administrative boundaries and networks.[25]

The literature credits British Prime Minister Tony Blair for introducing the concept of the "joined-up government" approach in 1997, which is considered to be the opposite of departmentalism and vertical silos. [26] [27] Blair introduced this concept to tackle the so-called "wicked" issues that straddled the boundaries of public sector organizations,

---

[23] Tom Christensen and Per Laegreid, "The Whole-of-Government Approach …, 1059-1060.

[24] *Ibid.,* 1060.

[25] *Ibid.,* 1064.

[26] Christopher Pollitt, "Joined-up Government: A Survey …, 34.

[27] David Richards and Martin Smith, "The Tension of Political Control and Administrative Autonomy: From NPM to a Reconstituted Westminster Model," in Autonomy and Control: Coping With Agencies in A Modern State, ed. Tom Christensen and Per Laegreid, (Cheltenham: UK: Edgar Eldar), 189.

administrative levels and policy levels. "Wicked" or complex policy problems usually go beyond the capacity of any one agency to understand or respond to, and there is usually disagreement in the cause of the problem, as well as how best to respond to it. These problems often cross governmental boundaries as well. Wicked problems require innovative, comprehensive and adaptable solutions that can be modified with the benefit of experience and feedback, as the problem is better identified and fleshed out. Issues that fit into this category are terrorism, national security, climate change, healthcare, pandemic influenza and drug trafficking. [28]

The Blair administration's strategy paper, *Modernising Government,* contained keystones of inclusiveness and integration: inclusive in that policies were forward looking, inclusive and fair; and integrated in that policies and programmes were tackled in a joined up way, regardless of the organizational structure of government.[29] Blair also outlined the government's plan to use new technology to develop an information technology (IT) strategy for Government that would establish cross-government coordination frameworks in order to ensure that the government was responsive to the public.[30] Whole of government activities have the potential to span any or all levels of government, and even to include groups outside of government. It is about joining up at the top, but also about joining up at the base, thus enhancing local level integration. The United

---

[28] Commonwealth of Australia, *Tackling Wicked Problems – A Public Policy Perspective*, (Canberra: Australian Public Service Commission, 2007), 1.

[29] Prime Minister and Minister for the Cabinet Office, *Modernising Government*, (London: Stationary Office, 1999), 1; available from http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm; Internet; accessed 26 February 2008.

[30] *Ibid.,* 37.

Kingdom (UK) has been a leader in developing this integrated approach by strengthening the role of central governments.[31]

The UK has been using the terms "joined-up government" as well as the "comprehensive approach" to describe this integrated government approach. Australia and Canada are using the moniker "whole of government," while the U.S. is referring to this as the "interagency process."[32] Because of the structural and political differences of the various national governments, there are differences in the roles of the various departments and agencies, such that each country is pursuing the whole of government approach in slightly different ways. The UK is looking at ministerial and departmental leadership structures, Australia and New Zealand are looking for clarity in their funding mechanisms across the departmental boundaries, and the U.S. is approaching this through government wide information management initiatives.[33]

The Australian Management Advisory Committee's *Connecting Government* report in 2004 defines the whole of government in the Australian Public Service as follows:

> Whole of Government denotes public services agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues. Approaches can be formal or informal. They can focus on policy development, program management and service delivery.[34]

---

[31] Tom Christensen and Per Laegreid, "The Whole-of-Government Approach …, 1061.

[32] Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia's Priority Challenges,* (Canberra: Commonwealth of Australia, 2004); available from http://www.apsc.gov.au/mac/connectinggovernment1.htm; Internet; accessed 26 February 2008, 1.

[33] Peter Elson, Marilyn Struthers and Joel Carlson, *Horizontal Tools and Relationships: An Internal Survey of Government Practices Related to Communities*, (Ottawa: Human Resources and Social Development Canada, 2007); available from http://www.hrsdc.gc.ca/en/cs/sp/sdc/task_force/tfci02/FinalHorizontalityReportJanuary2007_english.pdf; Internet; accessed 3 April 2008, 40.

[34] Management Advisory Committee, *Connecting Government* ….

Canada introduced the whole of government approach in the Treasury Board's annual report to Parliament in 2002 entitled *Canada's Performance 2002.*[35] In this document, federal departments and agencies are clustered into several "horizontal areas" in which the departments and agencies work together towards achieving common goals. These clustered organizations identified common leverage points in which the different federal departments and agencies could plan common strategies and monitor their success in the various efforts. Under the label of horizontal management, the Canadian Government launched whole of government initiatives in the areas of innovation, poverty and climate change.[36] The organizations were clustered in the areas of economic opportunities and innovation, health, the environment and the strength and safety of Canadian communities.[37] Canada initially introduced this approach with the aim of tightening financial management structures and strengthening governance and accountability regimes in order to reinforce the central political capacity with the goal to make subordinate agencies and companies less autonomous.[38]

An example of the success in the whole of government approach in Canada is the delivery of government services to Canadians within the Ministry of Human Resources and Social Development. Albeit within the same federal department, *Service Canada* provides a one-stop gateway that offers single window access to a wide range of

---

[35] Treasury Board of Canada Secretariat, *Canada's Performance 2002,* (Ottawa: Canada Communication Group, 2002), 22.

[36] Herman Bakvis and Luc Juillet, *The Horizontal Challenge: Line Departments, Central Agencies and Leadership*, (Ottawa: Canada School of Public Services, 2004), 7.

[37] Treasury Board of Canada Secretariat, *Canada's Performance 2002 ...,* ToC.

[38] Peter Aucoin, Accountability and Coordination with Independent Foundations: A Canadian Case of Autonomy. In Autonomy and Regulation: Coping with Agencies in the Modern State, ed. Tom Christensen and Per Laegreid, (Cheltenham, UK: Edward Elgar), 2006, 114.

Government of Canada programs and services such as passport services, social insurance number, employment insurance, old age security, and health information. [39] While these services are all within the scope of the Department of Human Resources and Social Development, these services were previously provided through disparate and distinct staffs and facilities. This initiative was aimed at making government more transparent and responsive to citizens, with the goal of Service Canada to improve the delivery of government services by providing Canadians with one stop shopping access to a wide range of personalized government services and benefits. This not only allows the department to effectively utilize their staff and resources in providing a more comprehensive service, it treats the Canadian citizen as a valued customer in the provision of these essential government services. The lessons learned in this endeavour, from the expectations of the customers, through to the configuration of the information services and the handling of privacy concerns, will assist in the application of the whole of government approach to other more complex issues, such as national security, where there are numerous departments and agencies involved.

Australia established a new Cabinet Implementation Unit in 2003 to support their whole of government activities. They took the approach of strengthening the center of their hierarchical structure by establishing new organizational units, such as new cabinet committees, inter-departmental or interagency collaborative units, intergovernmental councils, lead agency approaches, task forces, and integrated technical networks, with the main purpose of getting the various governmental units to work together. In cutting across traditional horizontal structures, they introduced a more coordinated effort to the

[39] Service Canada Website, "People Serving People," http://www.servicecanada.gc.ca/en/home.shtml; Internet; accessed 18 March 2008.

areas of national security, demographics, science, education, environment, rural and regional development, energy and transportation. [40]

However, structural change is not enough to fulfil the goals of these whole of government initiatives. Cultural change is also necessary, as processes and attitudes also need to be adjusted. The various departments and agencies need to identify activities in which the collaborative approach would increase the overall effectiveness of government services to achieve a common goal rather than simply maintaining the "stovepipe" status quo. The whole of government reforms focus on building a strong and unified sense of purpose, trust, value based management and collaboration. It encourages team building and cross-training of members of the participating organizations while improving the self-development of public servants in order to re-establish a common ethic and cohesive culture in the public sector.[41]

In Canada, the Treasury Board identified two challenges in effectively implementing this reform. The first is the lack of a governance structure to provide the leadership on these cross department collaboration efforts, and the second is the vertical nature of government accountability tools.[42] The lack of an interoperable information management capacity across departmental boundaries makes it difficult to effectively utilize procedures and resources across these boundaries and the lack of specialized policy tools for the governance, accountability and coordination of these horizontal initiatives perpetuates the tendency of the civil servants to stay within their departmental "stovepipes." Vertical accountability and the requirement to get ministerial approval to

---

[40] Tom Christensen and Per Laegreid, The Whole-of-Government Approach …, 1061.

[41] *Ibid.,* 1062.

[42] Peter Elson, Marilyn Struthers and Joel Carlson, *Horizontal Tools and Relationships* …, 6.

authorize the expenditure of funds across departmental boundaries means that coordination is required at the political level, which further reinforces the culture of departmentalism as it is considered too hard to battle the bureaucracy.[43]

The whole of government approach is not just to be pursued at the national level. It can be equally effective across levels of government in getting organizations within the municipalities, regions, local governments and civil society organizations to work together. However the simple imposition of top-down direction is not sufficient to make this happen, a cooperative effort across all levels is required.[44] Additionally, the building of a whole of government system is a long-term project that takes time to implement. New skills, changes in organizational culture, the creation of a mechanism to collectively share information, and the building of mutual trust relationships need patience.[45]

The whole of government approach is generally seen as a good thing, in efforts to bring agencies and departments together in an integrated and inclusive manner. However, there are some instances where the "silo" mentality exists for good reason. One example is within the law enforcement community, where the chain of evidence is essential for successful criminal prosecution. In cases like this, there will continue to be the need for well-defined vertical and horizontal organizational boundaries.[46] Additionally, there can be significant disadvantages, including increased implementation costs and the fact that effective collaboration skills are in limited supply. Departments that are horizontally working together in the same policy area may well engage in competition and rivalry

---

[43] Peter Elson, Marilyn Struthers and Joel Carlson, *Horizontal Tools and Relationships* …, 6.

[44] Tom Christensen and Per Laegreid, The Whole-of-Government Approach …, 1063.

[45] *Ibid.,* 1063.

[46] *Ibid.,* 1063.

rather than cooperation. [47] In worst cases collaboration can end poorly—dialogue can turn into conflict, hardened positions and stalemate.[48] Other potential issues, such as accountability and risk management are also of concern in the implementation of joint actions, common standards and shared systems on the one hand, but also vertical accountability for individual agency performance on the other. Whole of government, as a general approach for policymaking and government response is not a panacea that will solve all problems everywhere and every time. It should be used selectively, after careful thought and an estimate of the potential gains versus the cost of implementation. [49] Otherwise, legitimate departmental boundaries would be eliminated and there would be a complete lack of accountability or governmental control. We would return to the construct before the new public management initiative, where we had large bureaucracies with no clear authority or span of control, and the cost of conducting governmental business would increase.

Working more successfully across department and agency boundaries relies on better information sharing and requires structured approaches to the collection, reuse and sharing of data and information. Improving agencies' capability to transfer and exchange information is critical and will require improved interoperability between agencies' information systems. Improvements can be made not just by joining services and information together but also by redesigning and reengineering systems to deliver both better and more efficient services. It may also require agencies to adopt and implement common information policies, standards and protocols. Additionally, common

---

[47] Tom Christensen and Per Laegreid, The Whole-of-Government Approach …, 1063.

[48] Commonwealth of Australia, *Tackling Wicked Problems – A Public Policy Perspective* …, 10.

[49] Tom Christensen and Per Laegreid, The Whole-of-Government Approach …, 1063.

frameworks, policies and standards will need to be flexible enough to respond to the respective organizations' varying business requirements.

The Conference Board of Canada has identified two key principles for the effective governance of a whole of government response. First, leadership and accountability must be clearly defined. Without clear and recognized leadership, responders and the public can experience frustration and confusion. This was apparent in the SARS pandemic in 2003, where there was no identified leader due to uncertain authorities.[50] With leadership comes accountability. The overall leader must work with the leaders within each organization to ensure that all organizations are contributing effectively towards achieving the common goal. How leaders respond to emergencies plays a big part in how the organizations respond to emergencies. Experience is key in this regard.[51] For example, the Federal Emergency Management Agency (FEMA) did not have the right leaders in place to take charge of the scale of the response to Hurricane Katrina.[52]

Additionally, organizations must be able to effectively work together in achieving a common goal. Organizations and individuals require clearly defined mandates that are understood and accepted by all. Roles and responsibilities must be clearly established and aligned and the necessary resources must be made available. All stakeholders must be treated fairly and there must be continuous learning in that observations made during

---

[50] Archie Campbell, *The SARS Commission Final Report: Spring of Fear*, (Toronto: Ontario Ministry of Health and Long-Term Care, 2006), 33.

[51] Andrew Archibald and Trefor Munn-Venn, *A Resilient Canada: Governance for National Security and Public Safety,* (Ottawa: Conference Board of Canada, 2007), 11.

[52] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative – Final Report,* (Washington D.C.: Government Printing Office, 2006), xi.

exercises, training or actual events must be appropriately actioned.[53] Exercises and training are important tools to identify gaps in knowledge, information, responsibilities and procedures. They are also important to build a level of trust between organizations. Exercises help improve the ability of the organizations to cooperate during times of crisis. Exercises need to be widespread, regular and realistic, as the risk in trying to establish the required relationships and structures while responding to a major event are unacceptable.[54]

The following chapter explores the characteristics of interoperability, which provides the frameworks, both technical and operational, in which the departments and agencies can better integrate their resources in order to achieve the common goal, which is the rationale for using the whole of government approach.

[53] Andrew Archibald and Trefor Munn-Venn, *A Resilient Canada…,* ii.

[54] *Ibid.,* 14.

CHAPTER 3: INTEROPERABILITY AND INFORMATION SHARING

> Preventing terrorist activity very much depends on the collection, analysis and dissemination of information and intelligence, and on cooperation between jurisdictions, levels of government and the private sector.[55]

Six Arab nationals took flight lessons although they could barely speak English. They were not doing very well in their training and often disrupted the class. Preferring only Boeing type aircraft, they focused only on flying the plane, with no interest in take-offs or landings. One of them was arrested by the INS in August 2001. Three were stopped for secondary screening by the airport screening services as they went through security on 11 September 2001, but they were allowed to proceed. All these discrete incidents preceded the tragic events of 9/11. The government's single greatest failure in the lead-up to these attacks was the inability of federal agencies to effectively share information about suspected terrorists and their activities. Different agencies had pieces of the puzzle, however, as a whole there were no systems or procedures in place to connect the dots.[56] Richard Clarke, the former White House anti-terrorism advisor writes that is was intelligence failures leading up to the event that allowed this to occur:

> Somewhere in CIA there was information that two known al Qaeda terrorists had come into the US. Somewhere in FBI there was information that strange things had been going on at flight schools in the US. Could we have stopped the September 11 attack? It would be facile to say yes. What is clear is that there were failures in the organizations that we trusted to protect us, failures to get information to the right place at the right time, earlier failures to act boldly to reduce or eliminate the threat.[57]

---

[55] House of Commons, The Government's Response to the *Report of the Special Senate Committee on Security and Intelligency – 1999,* Thursday, December 16,1999; available from http://ww2.ps-sp.gc.ca/publications/Speeches/19991216_e.asp; Internet; accessed 29 March 2008.

[56] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, (Washington, D.C.: Government Printing Office, 2004), 1, 2, 3, 222, 247.

[57] Richard A. Clarke, *Against All Enemies: Inside America's War on Terror,* (New York: Free Press, 2004), 238.

Because of the operational design of today's organizations, there is an increased need to communicate across traditional boundaries. In Canada, the dividing lines between the jurisdictions and mandates of the various government departments as well as the levels of bureaucracy (federal, provincial and municipal) are melding together, thus the sharing of information is becoming much more critical. Information sharing and interoperability are inextricably intertwined not only to communicate between agencies, but also to provide the linkages to predict what could happen and to plan an appropriate response.

Interoperability describes the ability to work together to deliver services in a seamless, uniform and efficient manner across multiple organizations and information technology systems. Promoting interoperability between agencies is critical to achieving whole of government collaboration. The term interoperability however, while seemingly relatively straightforward in principle, is confusingly ambiguous in putting to practice due to the differing understanding of the word. In general terms, the ultimate goal of interoperability is not to ensure that all contributors in a given cooperative venture use the same equipment and systems, but simply that they achieve a more practical level of cooperation.[58] As DND's current *Strategic Capability Planning* document puts it: "The capability to work seamlessly with our most important allies in an operational setting ensures that we can participate effectively in those crises most likely to affect our vital interests."[59]

---

[58] Danford W. Middlemiss and Denis Stairs, "The Canadian Forces and the Doctrine of Interoperability: The Issues," *Policy Matters*, Vol 3 no 7, (June 2002), 11.

[59] Vice Chief of the Defence Staff, "Glossary for Strategic Capability Planning for the CF," *Strategic Capability Planning for the Canadian Forces,* (Ottawa: Department of National Defence, June 2000), 8.

Unfortunately, many of the organizations, like the various intelligence agencies, that are being compelled to collaborate and cooperate have years of tradition in not sharing information. Policies and doctrines, as well as tactics, techniques, and procedures (TTPs) needed to facilitate information sharing and therefore the interoperability requirements, have not been written. Additionally, while technology has grown at an exponential pace, and the technical capabilities to improve this sharing of information have also improved, legacy systems continue to reside throughout organizations as the owners and users refuse to give them up. Individual organizations then use their own funding to buy local technical solutions to meet their immediate needs, without considering the requirement to be interoperable within their own organization, let alone outside of it. Interoperability is further diminished, as these new systems are fielded without consideration for the existing equipment already in service, which the organizations are unwilling to part with.[60]

The ramifications of the lack of interoperability were brought to international attention in the aftermath of Hurricane Katrina. The massive damage to communications infrastructure alone wreaked havoc on the ability of any single agency to coordinate its own relief efforts in the Gulf Coast area. Establishing simple internal operability compounded problems with achieving interoperability with other agencies. National Guard soldiers, responsible to, and equipped by, their respective states, could talk to other soldiers and units from within their state, but they could not talk to soldiers from the other states, as their communications equipment was incompatible. In some cases, missed

[60] Maryann Lawlor, "Leaders Talk Tough About Interoperability," *Signal*, 62, no. 5, (January 2008), 68.

communications delayed disaster relief.[61] The House of Representatives report on the response to Katrina noted that voice radio contact with surrounding parishes or state and Federal agencies was not possible. It created a direct operational impact on the various organizations' ability to maintain control of a rapidly deteriorating situation within the city, carry out rescue efforts and control the evacuation of those who had failed to heed the call for evacuation. Lives were put at risk.[62]

The report also identified breakdowns in advance planning, in delays to system upgrades, as well as problems inherent in command and control with the many agencies and levels of government who were involved in coordinating the response.[63]

As indicated in the previous chapter, one of the key requirements to an effective whole of government approach is the ability for the various government departments and agencies to work together in order to combine their expertise, knowledge, skills and information with one another. A truly interoperable organization is able to maximise the value and reuse potential of information under its control. It is also able to exchange this information effectively with other equally interoperable bodies, allowing new knowledge to be generated from the identification of relationships between previously unrelated sets of data.[64] Enhancing interoperability increases the ability of adaptive human networks to share information, collaboratively analyse problems, and collectively develop and

---

[61] Maryann Lawlor, "Leaders Talk Tough About Interoperability," …, 69.

[62] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *A Failure of Initiative – Final Report,* (Washington D.C.: Government Printing Office, 2006); available from http://katrina.house.gov/full_katrina_report.htm; Internet; accessed 1 March 2008.

[63] *Ibid.*

[64] Paul Miller, "Interoperability. What Is It And Why Should I Want It?" *Ariadne* 24, (June 2000); available from http://www.ariadne.ac.uk/issue24/interoperability/; Internet; accessed 29 February 2008.

execute mutually supporting courses of action to achieve the necessary integrated effects.[65]

The standard definition as used by the North Atlantic Treaty Organization (NATO) allies, including Canada and the United States, holds that interoperability is the "ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together."[66] National and NATO authorities are encouraged to develop, agree upon, and implement concepts, doctrines, procedures and designs which will enable them to achieve and maintain interoperability. This requires the establishment of the necessary levels of compatibility, interchangeability or commonality in operational, procedural, materiel, technical and administrative fields.[67] Interoperability reduces duplication, allows the pooling of resources and produces synergies among member states. It does not necessarily require common equipment, however, the equipment must be able to communicate with other equipment.[68] In this vein NATO has developed standardization agreements (STANAGS), the implementation of which assists nations in achieving the required levels of interoperability to operate within the Alliance.[69] Since its first large-scale maritime exercise in 1952, NATO has worked to encourage standardization. NATO

---

[65] Sandy Babcock, *DND/CF Network Enabled Operations Working Paper*, (Ottawa: DRDC TR 2006-001, January 2006), 13.

[66] Vice Chief of the Defence Staff, "Glossary for Strategic Capability Planning for the CF," *Strategic Capability Planning for the Canadian Forces*, (Ottawa: Department of National Defence, June 2000), 28. See also, North Atlantic Treaty Organization. *NATO Glossary of Terms and Definitions*, AAP-6 (2002).

[67] NATO, *Backgrounder – Interoperability for Joint Operations*, (Brussels: NATO Public Diplomacy Division, 2006); http://www.nato.int/docu/interoperability/html_en/interoperability01.html; Internet; Accessed 3 April 2008.

[68] *Ibid.*

[69] *Ibid.*

maintains many standards, such that militaries maintain levels of interoperability amongst one another, such that when brought together to operate in a common mission, they are able to function together. A multivolume command control and communication (C3) Technical Architecture manual outlines the technical requirements that must be met in order to maintain the requisite level of technical interoperability.[70] Other dynamic mechanisms include the Allied Naval Communications Agency, the Military Agency for Standardization, NATO Communications and Information Systems Agency, and the NATO Standardization Group. These agencies have developed, over a long period of cooperation, systems standards, as well as common procedures and doctrine for using them, if not always common equipment.[71]

The NATO alliance has been active since 1952, with many of these advances in interoperability taking considerable time to mature. NATO continues to promote interoperability and cooperation. In 1994, NATO initiated a Partnership for Peace (PfP) program, in which they invited 23 countries in Central and Eastern Europe to participate in a bilateral agreement with NATO in order to:

> … reduce the risk of conflict arising out of misunderstanding or design and to better manage crises affecting the security of the Allies; to increase mutual understanding and confidence among all European states; and to expand the opportunities for genuine partnership in dealing with common security problems.[72]

Each country jointly developed and agreed upon an Individual Partnership Programme between NATO and themselves, with cooperation focussing on defence matters. Other

---

[70] NATO AdatP-34, *NATO C3 Technical Architecture Manual*; available from http://194.7.80.153/website/home_volumes.asp?menuid=15; Internet; accessed 10 March 08.

[71] Kenneth Gause et al, *U.S. Navy Interoperability with its High-End Allies*, (Alexandria: Center for Strategic Studies, 2000), 7.

[72] NATO, "NATO's Cooperation with Partners," http://www.nato.int/issues/partnership_evolution/index.html; Internet; accessed 16 April 2008.

disciplines, including civil-military relations, education and training, air defence, crisis management, communications and information systems, and civil emergency planning were also included. The military forces of PfP states regularly take part in NATO exercises and training programmes to enhance their interoperability and to ensure that they are capable of actively participating in NATO-led operations. Several of these countries have been, and continue to be, active participants in NATO missions, with significant contributions to the Alliance's operations and missions in the Balkans, Afghanistan, Iraq and Darfur. [73] Ten PfP members have since achieved sufficient interoperability within the NATO alliance and have become full NATO members, and three new countries have been invited to participate in the PfP programme.[74]

NATO has recently adopted the term "operational interoperability," which recognizes that interoperability is not limited to the narrow technical dimension of simply tying systems together to exchange data, but also involves the ability of coalition partners to share information, create a shared understanding of the situation, collaborate on the development and selection of courses of action, communicate these to all forces or units, and allow forces to work together effectively.[75] Table 3.1 below shows both the NATO scale of interoperability alongside the Interoperability Maturity Model ascribed to by the Canadian Department of Public Safety and Emergency Preparedness. This table details a framework by which the level of interoperability between organizations can be measured as a function of capability, including command relationships, doctrine, procedures and information sharing activities. Organizations with an interoperability level of 0 would be

---

[73] NATO, "NATO's Cooperation with Partners," ….

[74] NATO, "Alliance offers partnership to Bosnia and Herzegovina, Montenegro and Serbia," http://www.nato.int/docu/update/2006/11-november/e1129e.htm; Internet; accessed 16 April 2008.

[75] Kenneth Gause et al, *U.S. Navy Interoperability with its High-End Allies* …, 2.

considered completely independent organizations, while those with an interoperability level of 4 would be considered to be fully integrated, and could operate as a single organization.

Table 3.1 – NATO Interoperability Maturity Levels

Level	The NATO scale of interoperability[76]	Interoperability Maturity Model[77]
4	Seamless interoperability across all areas: Command and Control, rules of engagement (ROE), logistics, full intelligence sharing.	Seamless interoperability. Fully automated.
3	Full cooperation in operations and logistics. Combined force for a common mission. Common or comparable ROE mutually agreed upon by a higher command authority. Possible authorization of combined operations with a single operational commander.	Full information access. Not automated.
2	Includes mutual reinforcement of forces, by either temporary attachment or close support. Sharing tactical control allowed. ROE must be close.	Some information sharing. Processes are not automated.
1	Operations are coordinated to optimize operational efficiency for the interests of both parties, via geographic division of areas of operations into zones of national responsibilities or by a functional division of warfare areas according to capabilities, or a combination of the two. Possible exchange of ROE. Common tactical surveillance picture possible.	Basic capability. Processes are not robust and not consistent.
0	Forces operate independently. Exchange of information extends to movement and intentions of forces, operations in progress, and potentially threatening activities of other nations, and includes special-interest maritime traffic.	Informal interaction, Personal contacts via telephone or email.

Source: Kenneth Gause et al, "U.S. Navy Interoperability with its High-End Allies," 41. PSEPC, Public Safety Interoperability Directorate Website.

The experiences outlined above indicate that, while it cannot be expected that Canadian Government departments and agencies will be able to achieve interoperability overnight, I would submit that the NATO standards in concepts, doctrine and technology could form the basis, or at least a departure point, in order to initiate discussions amongst the whole of government agencies in identifying common areas that could be exploited.

[76] Kenneth Gause et al, *U.S. Navy Interoperability with its High-End Allies* …, 41.

[77] Public Safety and Emergency Preparedness Canada, Interoperability Directorate Website; http://www.tbs-sct.gc.ca/im-gi/imday04jourgi/info/ip-pi/page22_e.asp; Internet; accessed 19 March 2008.

Simply stated, interoperability is the effective sharing of information and work processes across technical and organizational boundaries. It is the ability of people, procedures and equipment to effectively operate together. This points to the fact that the concept has technical and organizational dimensions, the presence or absence of which will have a bearing on the level of interoperability that can be realistically achieved.[78] Each of the dimensions of interoperability is further explained in the following sections, where the specific requirements of each, as well as potential difficulties, are presented.

TECHNICAL INTEROPERABILITY

Technical interoperability refers to the technologies, data standards and formats required in order to electronically exchange and process information between systems.[79] Technical interoperability is associated with the hardware and software components, networks and equipment that enable machine-to-machine communication to take place.[80] This kind of interoperability is often centered on communication protocols and the infrastructure needed for those protocols to operate.[81] In many ways this is the most straightforward aspect of maintaining interoperability, as there are often clear right and wrong answers.

A high level of technical interoperability avoids data duplication, processing and storage, which in turn reduces the data processing costs and increases productivity. The

---

[78] National Research Council, *Realizing the Potential of C4I: Fundamental Challenges*, (Washington, DC: National Academy Press, 1999), 1.

[79] University of Oxford, *Information and Communications Technology Strategic Plan*, (March 2007), 90; available from http://www.ict.ox.ac.uk/strategy/plan/ICT_Strategic_Plan_March2007.pdf; Internet; accessed 29 February 2008.

[80] Hans van der Veen and Anthony Wiles, *Achieving Technical Interoperability – The ETSI Approach*, (Cedex, France: European Telecommunications Standard Institute, 2006), 5-6.

[81] *Ibid.,* 5-6.

development of technical standards, shared data centres, compatible or shared networks and other technical resources builds an information infrastructure for government operations, which helps ensure that the departments and agencies that are working together can share and reuse all the available information, not just that resident in their individual organization.[82] In order to facilitate interoperability, growth and maintainability, future networks and systems must be developed with adherence to open standards and architectures. Information technologies need to be used in the development of network centric enterprise services in order to provide modularity, interoperability and the sharing of decision support tools and services.[83] However, all too often, inconsistent data definitions exist, as computer programmers develop their code in isolation, with specific intentions in keeping their code as unique as possible, in order to maintain proprietary control. There are few incentives for developing and adopting standards, and unique definitions help to set that agency's information apart, which makes the dataset unique and thus less likely to be reduced in subsequent budgets because of that uniqueness.[84]

Most of the obstacles to achieving increased levels of interoperability are organizational or political in nature, thus technology should be embraced as the key enabler in order to ease the burden on organizations and their people. An effective

---

[82] Sharon S. Dawes, "Interagency Information Sharing: Expected Benefits, Manageable Risks," *Journal of Policy Analysis and Management*, Vol 15, No 3, 1996, 379.

[83] A. Auger et al, *Decision Support and Knowledge Exploitation Technologies for* C4ISR TM 2004-451, (Ottawa: Defence R&D Canada, 2006, i.

[84] Jeff Waldon, "Interagency Cooperation in Information Management," (Virginia Technical University: Conservation Management Institute); available from http://fwie.fw.vt.edu/WWW/datashar.htm; Internet; accessed 29 February 2008.

technological solution to sharing information will allow the people involved to focus their time and efforts in cooperative analysis.[85]

ORGANIZATIONAL INTEROPERABILITY

Organizational interoperability is the ability of organizations, and the people within them, to effectively communicate and transfer meaningful information between each other even if they are using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Each organization brings its own unique culture, capabilities and operating procedures to the table. In order to increase organizational interoperability each department and agency involved in the venture must realize a benefit from working together. Without effective governance, establishing clear unity of effort, effective leadership and a coordinated response is difficult to accomplish. Public and private sector leaders identified a lack of clarity around governance as the greatest risk to national security. They are concerned about the effective establishment of direction and control and they recognize that a failure in the relationships amongst the implicated organizations could intensify the impact of the event.[86]

---

[85] AFCEA White Paper, "The Need to Share: The U.S. Intelligence Community and Law Enforcement," 2007; available from https://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf; Internet; accessed 29 February 2008.

[86] Andrew Archibald and Trefor Munn-Venn, *A Resilient Canada*…, i.

Organizational interoperability occurs when disparate units agree on a common set of business goals and processes in order to facilitate the exchange of information.[87] Whereas technical interoperability can be seen as the network of systems or equipment, organizational interoperability can be seen to be the network of people. Organizational interoperability depends on successful technical and semantic interoperability.[88] Semantic interoperability is usually associated with the information's meaning and concerns the individual rather than the electronic interpretation. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the information being exchanged.[89] Ensuring semantic interoperability can present significant issues, which become more pronounced as individual resources are made available through the connected gateways, portals or networks. Almost inevitably, each department or agency would use different terms to describe similar concepts, such as author, creator or composer. Even within the military the different services seem to have their own language, which is often at odds with civilian agencies. Something as simple as the daily schedule within civilian agencies is known as the battle rhythm in the army, and the flex in the navy. Identical terms may also mean very different things, such as surveillance, which to the law enforcement community means an active task that has officers dedicated on a 24/7 basis for the purposes of collecting evidence, while in the military community it is the monitoring of the overall situation in a given area using whatever resources are available. Obviously, this introduces confusion and error in

---

[87] University of Oxford, Information and Communications Technology Strategic Plan, (March 2007), 10; available from http://www.ict.ox.ac.uk/strategy/plan/ICT_Strategic_Plan_March2007.pdf; Internet; accessed 29 February 2008.

[88] Hans van der Veen and Anthony Wiles, Achieving Technical Interoperability …, 5.

[89] *Ibid.,* 6.

terminology. [90] The use of common terminology, both within and across organizational and political boundaries, will increase the level of semantic interoperability, and will help alleviate problems as the databases are merged and integrated.

Organizational interoperability provides more comprehensive and accurate information to assist in problem solving, and potentially a coordinated ability to connect the dots. Departments and agencies benefit from cooperative activities that improve the quality, quantity and availability of data. The accuracy and validity of each organization's information can be compared and augmented with that from the other organizations to provide a more comprehensive picture.[91] This would enable the participating organizations to make informed and timely decisions, which, in the case of national security, could eliminate or at least facilitate an accurate and comprehensive response to the threat. However, the decision to make resources more widely available has implications for the organizations concerned. Organizations often blame the lack of information sharing on a lack of time and/or trained personnel. They view collection and management of information as a higher priority than distribution. Techniques for sharing often require a higher level of training and/or knowledge, which they are unwilling to expend extra resources to increase.[92] Additionally, sharing resources is often seen as a loss of control or ownership, and staff may not possess the skills required to support more complex systems as well as this dispersed user community. Changes in processes, as well as extensive staff and user training, are rarely considered when deciding whether or not to

---

[90] Paul Miller, "Interoperability. What is it and Why should I want it?" …, 1.

[91] Sharon S. Dawes, "Interagency Information Sharing: Expected Benefits …, 379.

[92] Jeff Waldon, "Interagency Cooperation in Information Management," …, 1.

release a given resource, but are crucial to ensuring the effective long-term use of any service.[93]

INFORMATION SHARING

As traditional boundaries begin to blur, large organizations increasingly require access to information from a wide range of sources, both in and outside of their own subject area. In many cases, both goals and problems are similar, and there is much to be gained through adopting common solutions wherever feasible. There is clear value in continuing to actively seek partnerships and common solutions across departmental boundaries, to the long-term benefit of the organizations concerned and, more importantly, to the benefit of the end-user, who routinely behaves in a cross-disciplinary manner, and is often hampered by unnecessary institutional barriers.[94]

The decision to share resources is not always freely taken, with the legal requirements of privacy legislation a significant factor in the decision for the dissemination of government-held information. Even in cases where organizations wish to disclose information, there are legal implications to their decision. Additionally, where resources have been compiled from different sources, the intellectual property rights of those providing the background sources also need to be protected. Third party release of information cannot be undertaken without the express permission of the original information source.[95]

---

[93] Paul Miller, "Interoperability. What is it and Why Should I Want It?" …, 1.

[94] *Ibid.,* 1.

[95] *Ibid.,* 1.

Information sharing protocols allow for integrated planning and service delivery. Combining or comparing the information from the various departments and agencies can reveal overlaps, gaps, and potential interactions, which no single organization may identify on their own, Sharing existing data reduces the information collection burden and reduces the potential for error, as common information need only be collected by one of the agencies, and then shared by the rest. Information providers also benefit, as this cuts the number of times that that person or organization needs to provide the same information.[96]

However, there are few direct incentives to freely share information with other agencies or individuals and there are some important disincentives. Often, there is a proprietary attitude towards information as agency budgets are often linked to their ability to provide answers. If information is freely available, the agency may not be able to justify their budget, thus potentially losing jobs.[97] Additionally, there are often concerns regarding actual and/or perceived legal restrictions to sharing information. Some agencies and organizations restrict information sharing citing legal restrictions, licensing agreements or liability concerns for sharing sensitive data.[98]

Information sharing is not the panacea for interdepartmental cooperation. The sharing of information must be justified in that the benefits of sharing this information override the potential risk that the shared information may be used inappropriately. A very current case in point of misuse of available information occurred in the U.S. presidential race, where the passport information of the Democratic contenders was

---

[96] Sharon S. Dawes, "Interagency Information Sharing: Expected Benefits …, 379.

[97] Jeff Waldon, "Interagency Cooperation in Information Management," …, 1.

[98] *Ibid.,* 1.

accessed inappropriately. Safeguards were in place to recognize this breach, and the implicated individuals were immediately fired from their positions. A congressional investigation is being requested to determine whether criminal charges are warranted.[99] Risk mitigation measures have been instituted to safeguard the release of sensitive information; the immediate firing of the employees, and the potential for criminal charges, as opposed to risk avoidance or aversion measures, whereby the information would be overly safeguarded, such that the information is unavailable for sharing by the appropriate departments and agencies, regardless of the benefits this may create. The risk of sharing the information must be balanced against the risk of not being able to connect the dots. The culture of "need to know" must be changed into one with the more open "need to share," with appropriate information security safeguards to protect the integrity of the information.[100] There is no value in having important information if it cannot be shared with others who may need that information or be able to add value.

For information sharing to succeed, there must be a level of trust created. Building this trust requires strong leadership, clear laws and guidelines, and appropriate technology to ensure that the sharing of information serves important purposes and operates consistently with public values. Leaders must consistently and repeatedly enforce the importance of information sharing, and that there is a responsibility to provide this information to other departments and agencies. They must ensure that information-sharing rules are clear, understandable and consistent. Complex, confusing and inconsistent rules inhibit people, as they are more apt to give up if the rules are too

---

[99] CBC News, "Obama wants Congress to Probe Passport Breach," (21 March 2008); available from http://www.cbc.ca/world/story/2008/03/21/obama-passport.html; Internet; accessed 21 March 2008.

[100] Molly M. Peterson, "Homeland Defense Commander Stresses 'Need to Share' Information," *National Journal's Technology Daily*, (December 3, 2002), 1.

hard to follow. Additionally, the construct of data ownership must be eliminated. Information must be seen as a collective resource to be disseminated to the greatest extent possible within the rules. Effective and complete analysis can only be improved with the broader picture that increased information can provide. The perception of the public that this increased sharing of information is being handled correctly can be improved through effective and focused training and education. The right training, with appropriate and effective policies, will better enable the sharing environment, help change the cultures, and increase the confidence that the information is being effectively used.[101]

In order to effectively apply the whole of government approach, success depends on cross-department understanding and interoperability, each participating agency must be able to understand each other and speak the same language. It is easier for the military to operate multi-nationally rather than interagency because language is more common and for the most part, equipment has been purposely built to a "NATO Standard."[102]

AN ORGANIZATIONAL INTEROPERABILITY MATURITY MODEL

The Australian Government has been doing considerable work in defining an organizational interoperability model, much like that conducted by NATO in their scale of interoperability, and shown previously in Table 3.1. The relationships that the organizations being brought together would exhibit at the different interoperability levels

[101] AFCEA White Paper, "The Need to Share: The U.S. Intelligence Community …, 10.

[102] NATO "Backgrounder – Interoperability for Joint Operations…, 1.

are presented in Table 3.2 below, within the attribute categories of preparedness, understanding, command style and ethos. [103]

Table 3.2 – Organizational Interoperability Maturity

Interoperability Maturity	Interoperability Attributes				
		Preparedness	Understanding	Command Style	Ethos
	Unified Level 4	Complete – Normal day-to-day working environment	Shared	Homogenous	Uniform
	Combined Level 3	Detailed doctrine and experience in using it	Shared communications and shared knowledge	One chain of command and interaction with home organization	Shared ethos but with influence from home organization
	Collaborative Level 2	General doctrine in place and some experience	Shared communications and shared knowledge about specific topics	Separate reporting lines of responsibility overlaid with a single command chain	Shared purpose: goals and value systems significantly influenced by home organization
	Ad hoc Level 1	General guidelines	Electronic communications and shared information	Separate reporting lines of responsibility	Shared purpose
	Independent Level 0	No preparedness	Communications via telephone	No interaction	Limited shared purpose

Source: Clark and Jones, "Organizational Interoperability Maturity Model for C2," 10.

The attribute of preparedness refers to the doctrine, experience and training provided to the partner organizations. Understanding refers to the level of information and knowledge sharing that would be undertaken. Command style is a measure of the autonomy of the organization as well as the roles and responsibilities of the partner agencies within the organization. Finally, ethos is a measure of the level of trust, culture, values and goals.

[103] Thea Clark and Richard Jones, *Organisational Interoperability Maturity Model for C2*, (Canberra: Department of Defence, 1999), 10; available from http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/049clark.pdf; Internet; accessed 31 March 2008.

The U.S. Department of Homeland Security (DHS) has also developed a model to demonstrate the relationships between the various interoperability elements. DHS, an overarching federal cabinet level department stood up shortly after 9/11, is responsible for U.S. national security. In their short existence, they have created policies, procedures and doctrine to integrate the previously disparate departments and agencies into one organization. In the area of creating procedures and doctrine, they have formulated an interoperability continuum, which, as shown in Figure 3.1, provides a simple graphical representation of the levels of interoperability, which is very similar to the interoperability maturity model presented above. As can be seen, the areas of leadership and governance, operating procedures, technology, training and exercises, and frequency of usage are all key to maximizing interoperability, with a more integrated approach in each area indicating higher levels of interoperability.

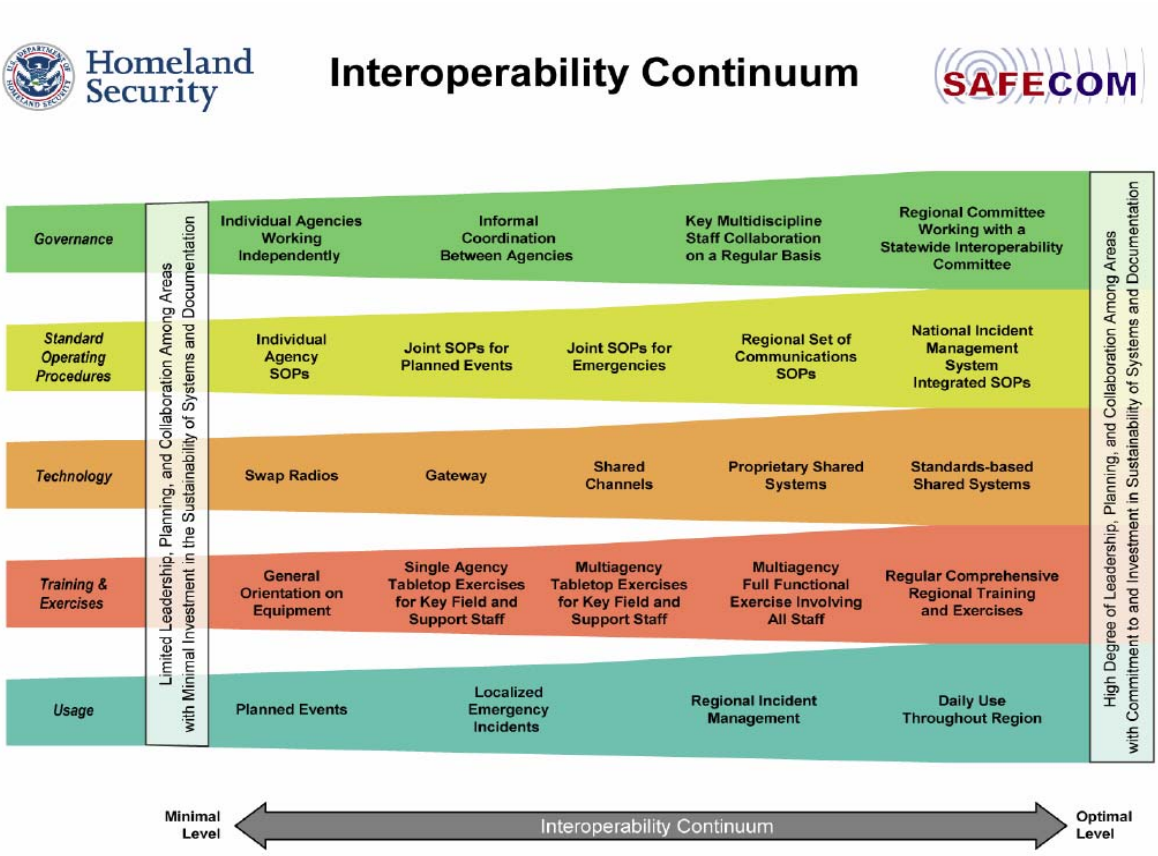

Figure 3.1 – US Department of Homeland Security Interoperability Continuum[104]

Source: SAFECOM, 2006 National Interoperability Baseline Survey

How much interoperability is enough, and which category do we pursue? That depends, as interoperability is highly dependent on the number of departments and agencies involved as well as the mission being undertaken. Different missions have different levels of risk and stress different aspects of interoperability. Where information is to be used and understood the same way, such as tracking aircraft to ensure adequate separation and safe travel around the world, technical systems must be wholly interoperable, as is the case with the Federal Aviation Authority (FAA) in the U.S. and

[104] SAFECOM, *2006 National Interoperability Baseline Survey*, (December 2006); available from http://www.safecomprogram.gov/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf; Internet; accessed 29 February 2008.

NAV Canada here at home. Coalition military operations normally have an integrated Command system, and therefore the highest level of organizational interoperability, however, depending on the participating countries, the level of technical interoperability could be anywhere in the spectrum. In responses to humanitarian crises, like pandemics, fires or floods, where each agency uses different procedures and equipment, a lesser level of technical interoperability may suffice, but there is the requirement for an increase in organizational interoperability to ensure that relief efforts are synchronized.[105]

Canada has embraced the whole of government approach in its response to national security and is working towards achieving the appropriate level of interoperability for the different missions and between the various departments and agencies. The following chapter will examine the policies and procedures enacted by the federal government and will demonstrate that the whole of government approach is being used effectively in some missions, but not as effectively in others.

[105] Kenneth Gause et al, *U.S. Navy Interoperability with its High-End Allies* …, 39.

CHAPTER 4: NATIONAL SECURITY

> There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens.[106]

Up until the tragic events of 9/11, Western states, including Canada, viewed national security in a simplistic fashion. They perceived security in two ways, first as simple criminal activity, handled through intelligence and law enforcement agencies, and secondly as military threats, handled through their respective militaries.[107] However, threats to national security are not always terrorist or military in nature, but also include natural disasters such as earthquakes, hurricanes, floods and forest fires as well as pandemics like the SARS outbreak in 2003. Left unchecked, these threats also have the potential to undermine the security of our free and open society. Traditionally Canada has been a nation that reacts to crises, especially those of a natural nature like the Manitoba floods in 1997 or the ice storm in Quebec and Ontario in 1998. However, this culture of reaction places huge demands on resources as the event is unfolding. If the events are considered unforeseeable, the entire response is reactionary, with the probability of considerably more damage and loss of life than if there were some planning and mitigating measures undertaken in advance.[108] Unforeseeable events however, should be the exception and not the rule. A more proactive coordinated preventative approach will better serve Canada and Canadian citizens and would foster cohesiveness within Government.

---

[106] Privy Council Office, *Securing an Open Society: Canada's National Security Policy …*, vii.

[107] British Columbia Innovation Council, *Port Security Requirements – An Analysis of Industrial Opportunities for Small and Medium Enterprises in Port Security Requirements,* December 2004, 9.

[108] Captain(N) Peter Avis and Iain Grant, "Canadian Maritime Security and the Culture of Prevention," *Canadian Military Journal*, (Winter 2004-2005), 56.

In the Canadian context, national security involves the prevention, pre-emption, deterrence of, and defence against, threats against Canadians, Canadian territory and infrastructure, as well as the management of the consequences of these threats. These security threats span a large geographic area or cross traditional departmental boundaries, such that a national response is normally required, as no one organization, federal, provincial or municipal could adequately address the threat in isolation. To date however, the response has traditionally been handled in an ad hoc manner. Departments and agencies were brought together to respond as the problem escalated, with no consistency in the response mechanism, nor any national planning or coordination activity undertaken.[109] It became very clear after the events of 9/11 that this reactionary response was no longer acceptable, with an integrated whole of government national security framework required, because of the increasingly complex nature of these threats, as well as the number of departments and agencies implicated in the resultant response. The Government of Canada began to adopt a culture of prevention to allow for the preparation, readiness and defence before an event, as well as the response in the aftermath of the event.[110]

Figure 4.1 depicts a classic threat life cycle, in which there is normally a significant period of time during which a threat is incubating and developing event. During this period there may be certain indicators that warn us that a danger exists and that something is about to occur. A reactionary culture waits for the event to occur, and then provides an emergency response action to recover from the event. In a proactive preventative environment, organizations gather, organize and store information in order

[109] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*…, 3.

[110] Captain(N) Peter Avis and Iain Grant, "Canadian Maritime Security …, 57.

to observe what is happening. Preparatory plans would be made, sometimes generic, as to what actions are to be taken, either to prevent an event from occurring, or to mitigate the results of the event, should one occur. With sufficient effort expended in the initial phases of information sharing and threat detection, it is possible to eliminate the threat before it becomes an event, thus negating the emergency response action, as the event is not allowed to occur. Ideally, under the whole of government approach, departments and agencies should be working together from the outset, with the requisite level of interoperability to allow for the effective sharing of information in order to agree on the priority of potential threats and to recognize the warning signs of these threats. The implicated departments and agencies should also be collectively planning for, and exercising their actions to eliminate the threat, and also to exercise the appropriate emergency response to the event. In this way, should an actual threat occur, the problem areas are worked out in advance regarding the roles and responsibilities of the respective agencies, as well as the required levels of interoperability. While it is not always possible to foresee or eliminate every possible threat, this level of preparedness should allow for a consolidated and immediate emergency response from implicated departments and agencies, which have already determined their respective roles and responsibilities, and are already operating in a collaborative environment. This is the culture of prevention that should be embraced.

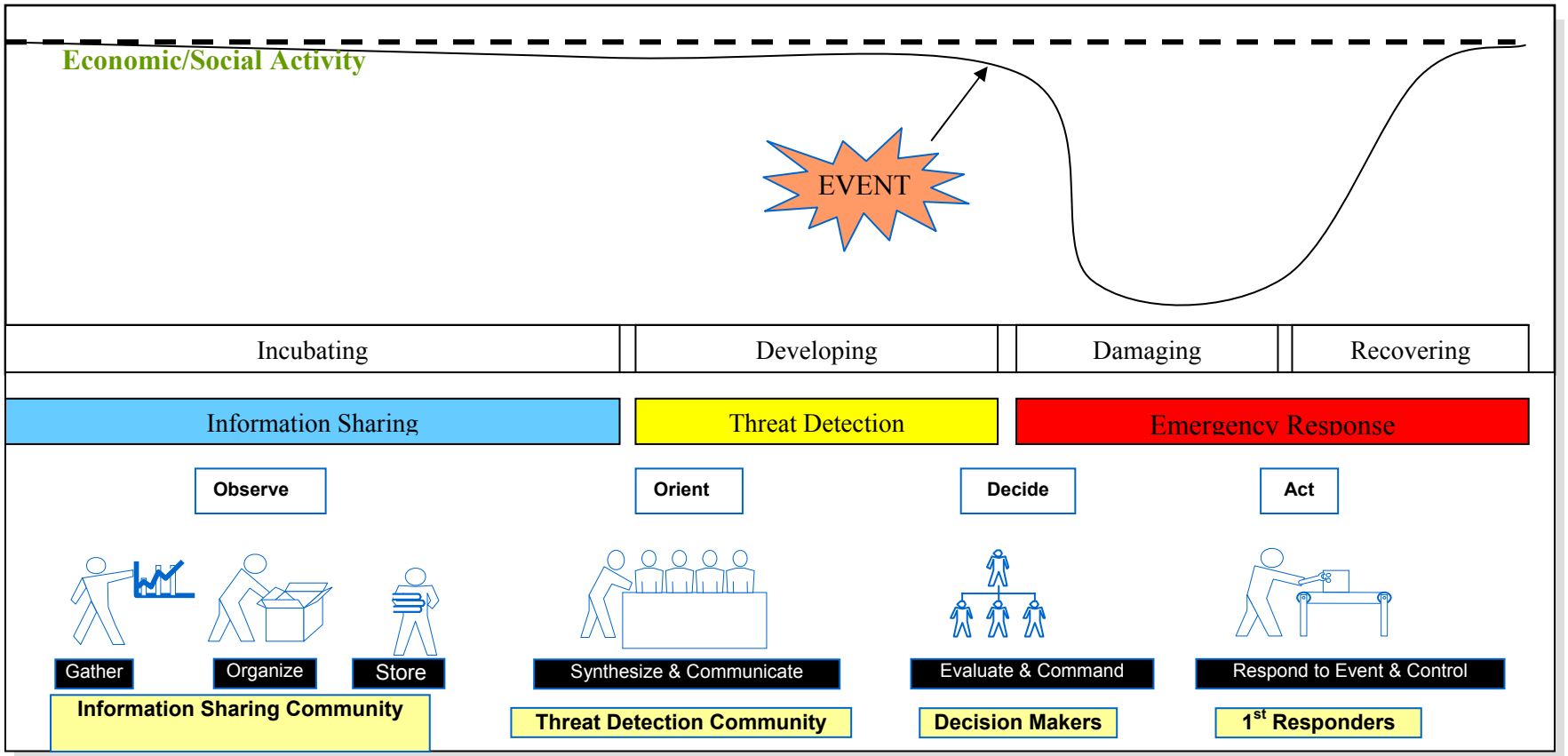

Figure 4.1 - Classic Threat Life Cycle[111]

Source: Aikins, "Interdepartmental Intelligence: The Key Factor for Maritime Security," 5

[111] Greg Aikins "Interdepartmental Intelligence: The Key Factor for Maritime Security," A Presentation to A Conference hosted by the Centre for Foreign Policy Studies, Dalhousie University, (10-12 June 2005); available from http://centreforforeignpolicystudies.dal.ca/pdf/msc2005/msc2005aikens.ppt; Internet; accessed 24 March 2008, 5.

Immediately following the September 11, 2001, terrorist attacks, Deputy Prime Minister John Manley was appointed as the country's lead representative in organizing the government's response to public security and anti-terrorism. An ad hoc Committee of Ministers on Public Security and Anti-Terrorism (PSAT) was formed, with ministerial level representation from the Privy Council Office (PCO), DND, the Solicitor General (Sol Gen), Canada Customs and Revenue Agency (CCRA), Citizenship and Immigration Canada (CIC), Transport Canada (TC), Fisheries and Oceans Canada (DFO), the Canadian Coast Guard (CCG) and the Royal Canadian Mounted Police (RCMP). The PSAT committee conducted hearings and allocated resources to the departments requiring the most urgent security needs in order to guide the government's response to anti-terrorism.[112]

The PSAT Committee created two interdepartmental working groups, including the Interdepartmental Working Group on Aviation Security (IWGAS) as well as the Interdepartmental Marine Security Working Group (IMSWG) to examine the security activities in these two domains, and to recommend improvements as necessary. The federal government has the legislative authority, as provided by sections 91 and 92 of the *Constitution Act*, over the airspace above the country as well as the territorial and inland waterways that are not wholly encompassed within any one province. This includes the ocean approaches to the East, West, and Arctic Coasts of Canada, as well as waters of the Great Lakes and Saint Lawrence Seaway.[113] As such, the federal government mandates

---

[112] Captain(N) Peter Avis, "Surveillance and Canadian Maritime Domestic Security," *Canadian Military Journal*, (Spring 2003), 11.

[113] Department of Justice, *Canadian Constitution Act, 1867*, Sections 91-92; available from http://laws.justice.gc.ca/en/const/c1867_e.html#provincial; Internet; accessed 16 April 2008.

and governs the security actions and activities to protect these areas from terrorist and other threats. Given this mandate and authority, the PSAT Committee, operating at the federal level, was able to recommend several technical, legislative, and regulatory initiatives that will serve to enhance air and marine security. These initiatives will be examined in further detail in the following sections.

AIR SECURITY

The civil air navigation environment has been fairly regulated long before 9/11, due mostly to the requirement to monitor and control aircraft in order to avoid collisions and regulate the airspace overhead. NAV Canada is the privatized capital corporation that coordinates the safe and efficient movement of aircraft in Canadian domestic airspace and international airspace assigned to Canadian control, through the provision of air traffic control, flight information, weather briefings, aeronautical information, airport advisory services, and electronic aids to navigation. [114] The Federal Aviation Authority (FAA) has the same responsibilities in American domestic airspace and international airspace assigned to US control.[115] These two organizations work closely together due to the significant overlapping boundaries as well as the huge volume of aircraft transiting between Canadian controlled to US controlled airspace. Civil regulations require that all aircraft, regardless of size, nationality or purpose (commercial or private) have and utilize a functioning transponder, which is an electronic device that provides, as a minimum the

---

[114] NAV Canada, "Newsroom Backgrounder - Air Traffic Services," http://www.navcanada.ca/NavCanada.asp?Language=EN&Content=ContentDefinitionFiles%5CNewsroom%5CBackgrounders%5Cairtrafficservices.xml; Internet; accessed 3 April 2008.

[115] FAA Website, "FAA Mission," http://www.faa.gov/about/mission/activities/; Internet; accessed 3 April 2008.

aircraft's identification, speed and altitude. This allows for positive identification and control of all aircraft within the controlled airspace, and also, when combined in an information sharing and display computer system, provides the controlling authorities with a graphical representation of all aircraft flying at any particular time. This is known as the air picture.[116] Incidentally, it is this same technology that allows anyone to use any of the online flight tracking programs to see if their flight is arriving on time.[117]

Along with NAV Canada and the FAA, who monitor aircraft for the purposes of safe and efficient aircraft movements, the North American Aerospace Defence Command (NORAD) also monitors and tracks objects in the aerospace environment.

North American Aerospace Defence Command

NORAD is a bi-national military command formally established in 1958 by Canada and the United States to monitor and defend North American airspace during the Cold War. Charged with detecting, deterring and defending against air attacks aimed at North America, NORAD monitors and tracks man-made objects in space and detects, validates and warns of attack against North America by aircraft, missiles or space vehicles. Its mission is to defend the airspace of North America, and to defend the

[116] Transport Canada, "Transport Canada Aeronautical Information Manual," available from http://www.tc.gc.ca/CivilAviation/publications/tp14371/RAC/1-1.htm#1-9; Internet; accessed 3 April 2008, Section 1.9.2.

[117] For example, see the website http://flightaware.com/live/ which provides a visual map of all flights operating under instrument flight rules at a specific snapshot of time. NORAD would have a similar graphical display, with continuous informational updates and would also have access to much more information regarding each flight.

continent. NORAD also provides surveillance and control of Canadian and U.S. airspace.[118]

Prior to 9/11, NORAD focussed on external threats, as the primary threat was the strategic bomber fleet of the former Soviet Union. Exercises were planned and undertaken that envisioned hijacked commercial aircraft, but it was always assumed that the aircraft would be hijacked overseas, not within North America. No one thought that aircraft would be hijacked within North America and then used as guided missiles.[119] The threat of nuclear war and the strategic bomber is still present; however, terrorism now poses a greater threat, with the airspace over the continent and commercial aircraft now watched with greater interest and caution.[120]

The Commander of NORAD is appointed by, and is responsible to, both the Prime Minister of Canada and the President of the United States. Traditionally, the Commander of NORAD is American, and the Deputy Commander is Canadian.[121] NORAD's responsibilities encompass the whole range of activities from initial detection of a threat though to the military response to the threat. This could entail actually firing at and shooting down the threat aircraft, missile or space vehicle. Shoot-down permission requires authority at the Government level, however the Commander of NORAD has the personnel and equipment capable of this task wholly within his Command.

---

[118] Department of National Defence, "NORAD," DND Backgrounder BG–06.011, (May 12, 2006); available from http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1922; Internet; accessed 3 April 2008.

[119] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report,* (Washington, D.C.: Government Printing Office, 2004), 17.

[120] Standing Senate Committee on National Security and Defence, *National Emergencies: Canada's Fragile Front Line*, (Ottawa: Senate, 2004), 7.

[121] Department of National Defence, "NORAD," DND Backgrounder BG–06.011, (May 12, 2006); available from http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1922; Internet; accessed 3 April 2008.

The attacks of 9/11 caught NORAD off guard, as the nature of the attack was completely unexpected. However, once it was determined what was actually transpiring NORAD fighters were alerted and were airborne shortly after the initial strike on the World Trade Center. NORAD officials claim that they would have been able to shoot down United Flight 93, the fourth and final aircraft, before it reached its intended target, the Capital or the White House. Ultimately, this was not required, as the passengers onboard sacrificed their lives and caused the plane to crash in a field in Pennsylvania.[122]

Since 9/11, NORAD has enhanced its tracking capability and vigilance to not only watch over the skies approaching North America, but also the airspace within North America. Working closely with the FAA and NAV Canada, NORAD has a hierarchical and clear bi-national chain of command with the appropriate sensors and weapons to effectively deter, defend and defeat any hostile air threat. Looking back at Tables 3.1 and 3.2, it is evident that this, albeit small, whole of government team encompassing NORAD, FAA and NAV Canada operates within a unified interoperability maturity level, and thus collaboratively has the appropriate mandates and tools to effectively counter threats to North America that approach through the aerospace environment. With a unified command structure, fully automated information sharing mechanism, and a completely integrated command and control system, an immediate air threat can be effectively and completely neutralized. The necessary doctrine exists and planning and exercise activities are regularly conducted to ensure a unified response from all departments and agencies.

---

[122] The National Commission on Terrorist Attacks Upon the United State, *The 9/11 Commission Report,* (Washington D.C.: Government Printing Office, 2004), 62.

Interdepartmental Working Group on Aviation Security

In response to the security breaches that led to the events of 9/11, Transport Canada (TC) was tasked by the PSAT Committee to form and lead the Interdepartmental Working Group on Aviation Security (IWGAS), with representation from the RCMP, Canadian Security Intelligence Service (CSIS) and the Canadian Border Services Agency (CBSA). Their mandate was to enhance aviation safety and security. In this way, with sufficient intelligence and warning, terrorists will no longer be able to get through security and use aircraft in any similar fashion to the actions of 9/11. There was very little information found on the actions of this working group, with the exception of changes to the *Public Safety Act, 2002*, which included provisions under the Aeronautics Act for the creation of a no-fly list as well as the systematic sharing of passenger information, for transportation security reasons only, amongst the IWGAS members.[123]

The classified nature of intelligence activities amongst CSIS, the RCMP and CBSA, means that the only news the public will only hear about the activities of the intelligence community after a success, or failure, in deterring threats. One such example is the August 10, 2006 arrests in the U.K. and the U.S. regarding an alleged terrorist plot to blow up transatlantic aircraft originating from the U.K. using gel-based explosives.[124] The general public was only made aware of this threat due to the complete ban on carry-on luggage. Intelligence community activities at the classified information level make it more difficult for researchers to determine the efficacy of their actions. Transparency and accountability is difficult at best, and, as in the case of the Maher Arar enquiry, may only

---

[123] Transport Canada, "Passenger Protect Program," available from http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm; Internet; accessed 25 March 2008.

[124] CBC News, "Airline Bomb Plot," (10 August 2006) available from http://www.cbc.ca/news/background/ussecurity/airplane-bombplot.html; Internet; accessed April 3 2008.

be investigated after political involvement. However, much of the testimony and information provided to the Arar Commission was still conducted at the classified level, especially as regards to the facts regarding Mr Arar. The Commission was more open regarding the policy review and recommendations for the RCMP's national security activities as a whole.[125]

AIR SECURITY SUMMARY AND RECOMMENDATIONS

The air security of North America, through the actions of NORAD, TC, NAV Canada and the FAA embodies the whole of government approach, and provides North America with an effective detection, deterrent, and defence capability. In order to increase the prevention and mitigation efforts however, the intelligence community needs to maintain their vigilance and continue their efforts in achieving early intelligence and warning so as to defeat the threat before the perpetrator has the opportunity to get themselves, or their weapons on the aircraft in the first place. It is recommended that exercises be planned and conducted that stretch the imagination of the possible and the probable and that the entire aviation security community continues to be involved to ensure that threats are eliminated prior to any requirement to shoot down civilian aircraft.

MARINE SECURITY

Interdepartmental Marine Security Working Group

Unfortunately, organizations involved in marine security are not as advanced in the development and maintenance of a complete appreciation of vessel traffic

---

[125] Dennis R. O'Connor, *A New Review Mechanism for the RCMP's National Security Activities – Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, (Ottawa: Public Works and Government Services Canada, 2006), 611.

approaching or operating within Canadian waterways as the aviation community is in tracking and controlling aircraft traffic. This is due to the myriad of departments and agencies that have mandates in regulating certain aspects of the marine environment. To integrate the efforts of these departments and agencies, the Minister of Transport was given responsibility to form the ad hoc Interdepartmental Marine Security Working Group (IMSWG). With representation from 17 federal departments and agencies, most notably TC, CCG, RCMP, CBSA, DND, and the Department of Justice (DoJ), this group developed a marine security plan that was presented to and approved by Government in December 2002. The foundation of this plan includes efforts towards achieving maritime domain awareness. This includes surveillance of the activities of vessels, cargos and people within the marine zones along with liaison and coordination with the intelligence communities, both domestic and international.[126] An integrated information system, known as the Marine Information Management and Data Exchange (MIMDEX), to allow for the sharing of maritime information was identified and allocated funding.[127]

Maritime Information Management and Data Exchange

The lack of a system for exchanging and sharing relevant information within the marine environment was recognized by IMSWG as a key security deficiency when it commissioned a study in 2002 to examine information exchange requirements between the various departments and agencies with mandates or information holdings related to marine security. The study concluded that organizations involved in maritime security did

[126] Interdepartmental Marine Security Working Group, "Enhancing the Security of Canada's Marine Transportation System – Canada's Marine Transportation System," (Jan. 12, 2004); available from http://www.navy.forces.gc.ca/cms_strat/strat-issues_e.asp?id=301; Internet; accessed 25 March 2008.

[127] Captain(N) Peter Avis, "Surveillance and Canadian Maritime Domestic Security …, 11.

not have the necessary information infrastructure to bring together relevant security information. The study recommended a "one stop shopping" approach to the sharing of information, with the introduction of a networked collaborative intelligence system to fill this gap.[128] The intent was to use existing government information and information networks, and to fuse this information into a common data repository in order to provide a more complete representation of the vessels, cargo and people operating in the marine environment, as well as to facilitate coordinated action and alert departments to potential targets of interest.[129]

Planned to be operational in 2005, MIMDEX was designed to be the government of Canada's interdepartmental and inter-agency information exchange network in order to bring the disparate marine information together from each of the partner agencies into a protected information registry that would collate and fuse marine security information from existing and planned Government of Canada databases.[130] The goal was to develop a shared information network for the collaboration and sharing of vital maritime information using a common and simple graphical representation of this varied information; one which allowed for better anticipation and coordination amongst the government departments and agencies involved in the maritime domain in anticipation of, and in reaction to, potential threats in the maritime domain. Technical interoperability was being approached at the highest level, which required all implicated departments and agencies to look at what information they could provide. The greatest challenge was in

---

[128] Greg Aikins, Network-Centric Operations and Interdepartmental Marine Security," *Canadian Naval Review*, Vol 1 No 3 (Fall 2005), 22.

[129] Interdepartmental Marine Security Working Group, "Enhancing the Security …, 1.

[130] Cdr Steve Peters and LCdr James Salt, "Maritime Security and Coastal Defence – Challenges in the 21st Century," *Soundings*, (May 2006), 9.

determining what information was available to be shared, how much of it needed to be shared, a legal opinion as to how much could be shared, and a networked infrastructure to share the information in a timely manner.[131] To this end, MIMDEX was designed to provide sufficient macro level information based on a rules-based interest flagging system that would provide cumulative indication and warning, but not necessarily attaching specific information to the flag. In this manner, a warning flag could be set on a certain vessel to indicate that there is a potential concern with that vessel, along with amplifying data that would suggest which agency should investigate the vessel further.[132] MIMDEX was designed to be more than a network system that enables information exchange, coordination and communication: it was designed to be a threat anticipation system that helps organizations connect the dots. By networking partners with their information or analysis capability, Canada would move from a very ad hoc and reactive approach to marine security to a network-centric, proactive intelligence and operations posture, where all marine traffic would be graphically represented on an electronic chart, with underlying details on each vessel's characteristics, such as registration, ownership, current cargo, last port of call, next port of call, and a myriad of other details. [133]

Unfortunately the pace of progress has been glacial in the face of legal and bureaucratic stumbling blocks. Privacy laws, the *Charter of Rights and Freedoms*, third party legal constraints and inadequate departmental legal mandates have delayed the development and deployment of MIMDEX despite an urgent public security

---

[131] *Ibid.,* 9.

[132] Gary L. Garnett, "The Coastal Regime and Marine Security Operations Centres," *Canadian Naval Review*, Vol 1 No 3 (Fall 2005), 27.

[133] Greg Aikins, Network-Centric Operations and Interdepartmental Marine Security …, 22.

requirement.[134] Perhaps the approach to achieve seamless and integrated technical interoperability in a direct rather than phased approach was asking too much. However, both the Senate Committee on National Defence and Security (SCONSAD) and the Auditor-General, Sheila Fraser, have criticized this continuing capability gap. The Auditor-General acknowledged that many of Canada's laws prevent the sharing of information within government to protect individuals' rights. However, Sheila Fraser also found that departmental officials would often not even examine the possibility of sharing information, based on the assumption it would contravene the *Privacy Act*.[135] Privacy concerns were often cited as the reasons that agencies did not share information; however officials were unable to provide any legal opinions, specific legislation references or judgments as a basis for that opinion.[136] Additionally, the *Privacy Act* does have accommodations for the sharing of information in different circumstances, including for national security reasons.[137] Sheila Fraser writes "The importance of intelligence in the fight against terrorism cannot be overstated. Coordinating the efforts of the agencies involved is acknowledged as critical to their overall effectiveness."[138] This is why the Senate Committee on National Security and Defence (SCONSAD) specifically

[134] Third party legal constraints prohibit an organization from releasing information they received from one party to a third party, without the permission of the first party. This is one of the biggest issues in the actions of Canadian Officials in relation to Maher Arar.

[135] Auditor General of Canada, *Report of the Auditor General Of Canada to the House of Commons- March 2004*, (Ottawa: Public Works and Government Services Canada, 2004), 23.

[136] Auditor General of Canada, *Report of the Auditor General Of Canada to the House of Commons - March 2004*, (Ottawa: Public Works and Government Services Canada, 2004), 17.

[137] *Ibid.,* 23.

[138] *Ibid.,* 14.

recommended the MIMDEX system for fast tracking.[139] SCONSAD notes that MIMDEX is being designed to allow for interdepartmental cooperation within the legal bounds of the *Privacy Act* and that only legally allowable information from each contributor will be made available through this novel approach of using warning flags.[140]

From an organizational perspective, the ad hoc whole of government approach does not work in this instance, as there is not one overall leader to take ownership and champion the project, due to inadequate legal mandates. The politically risk-averse nature of the various departments and agencies involved will continue to make this a contentious issue, further delaying or even cancelling this project. Strong leadership by the government is required to break down these perceived legal barriers to information sharing.

Marine Security Operations Centres

Another initiative advocated by the IMSWG is the development and stand up of Marine Security Operations Centres (MSOC) on the East Coast, in Halifax, N.S., and the West Coast, in Esquimalt, B.C., to provide marine security for the respective approaches to Canada, Canadian waterways and ports.[141] These operations centres are designed to enhance marine intelligence, surveillance and reconnaissance capabilities by shifting these capabilities from a Navy centric approach to a whole of government approach with the collaborative participation of the other federal departments and agencies implicated in

---

[139] "Canada's Coastlines: The Longest Under-Defended Borders in the World," in *The Report of the Standing Committee on National Security and Defence*, 37th Parliament, 2nd Session, Vol. 1, (October 2003), 153.

[140] Greg Aikins, Network-Centric Operations and Interdepartmental Marine Security …, 22.

[141] The development and implementation of a third MSOC, to operate in the Great Lakes and Saint Lawrence Seaway was recently announced in budget 08.

marine security. The five core partner agencies include DND, RCMP, TC, CCG and CBSA. An interim operational capacity was established in 2005, with full manning and operational capabilities expected in the 2010 – 2011 timeframe, upon the construction of new facilities. While the facility is being designed to house the various departments and agencies in an integrated environment, jurisdictional responsibilities of each of the organizations will not be changed. Because of the diverse mandates of the various agencies, the MSOC will operate under an ad hoc leadership model; if an event occurs, the department or agency with the appropriate jurisdictional regulations will assume command for that operation, with the remaining partners providing services and support as requested.[142] One of the benefits in bringing the agencies into a permanent facility on a full time basis is that they become formal workplaces for long term postings, therefore individual knowledge and experience will not be as readily lost. The long-term goal is to break down inter-agency barriers, develop procedures to effectively work together, and to create information sharing protocols.[143]

However, the key to the successful functioning of the MSOCs is the sharing of information and intelligence by all participating departments and agencies. MIMDEX is expected to be an important component of the integrated marine security information model. This networked capability of this collaborative information environment is designed to link the MSOCs to the marine security partners and to the Government Operations Centre as well as to Canada Command HQ.[144] Without MIMDEX, the MSOCs remain an ad hoc collection of independent departments and agencies, that may

---

[142] Cdr Steve Peters and LCdr James Salt, "Maritime Security and Coastal Defence …, 10.

[143] Eric W. Manchester, "Creation of Marine Security Operations Centres Leads to More Unified Response," *Canadian Sailings,* (14 August 2006), 20-21.

[144] Gary L. Garnett, "The Coastal Regime and Marine Security Operations Centres…, 27.

be co-located in the same facility, but do not have the integrated capacity to fuse the disparate information. At best they could hope to achieve an interoperability maturity model level of 2, which is probably not much better than what the departments and agencies have now have now through ad hoc unofficial agreements, with the only benefit being that they are now co-located. The organizational and physical structures being developed rely heavily on the development and implementation of a highly technical information sharing system, MIMDEX, which may not be created, based on risk-aversion to privacy issues. There is very little hope that the MSOCs will be able to meet their mandate without federal leadership.

Vice Admiral Ron Buck, in a speech to a conference on Maritime Security in 2004, stated that while considerable gaps were being addressed under the auspices of the marine security plan, areas that were not dealt with involve ensuring clarity of mandates, as well as the practical approach towards interdepartmental working relationships.[145] This problem is evident not only in the lack of progress in the MIMDEX project, but also in the framework of the MSOC organization, where there is no direct leader and therefore no ability to achieve a unified interoperability maturity level, regardless of the success of MIMDEX. IMSWG is an excellent conduit to develop ideas and plans in advancing the whole of government approach in the marine security environment, but each department or agency will likely maintain their allegiance and bias within their respective mandates and responsibilities, as there will be no incentive to do otherwise. Dan Middlemiss, an acknowledged expert in the field of marine security told SCONSAD that the IMSWG

[145] Vice Admiral Ron Buck, "Keynote Address: Continental Security from a Maritime Perspective," in *Continental Security and Canada-U.S. Relations: Maritime Perspectives, Challenges and Opportunities*, ed. Robert H. Edwards and Graham Walker, (Centre for Foreign Policy Studies: Dalhousie University, May 2004), 31.

was doing great work, but he pointed out that this group was powerless either to create policy or direct reform. He states: "If we simply rely on the very good work from these interdepartmental groups that are working to find the gaps, they will, and then nothing more will happen because nothing has ever happened again in the past. We need policy."[146] The SCONSAD report emphasized that one of the basic problem with relying on committees composed of a variety of departments and agencies for direction is that each of these departments and agencies has its own legislation and its own mandate, and the security of Canadians is rarely their primary mandate. "Not only is it doubtful that IMSWG will ever create policy, or gain the authority to "direct that things happen," it is doubtful that it *should* create security policy, given unfocused scope of priorities of its members." [147] The National Security Policy, unveiled shortly after the SCONSAD report, helps to address some of these concerns.

National Security Policy

Released in 2004, under Paul Martin's Liberal Government, *Securing an Open Society: Canada's National Security Policy* emphasizes the importance of cooperation among agencies in protecting national security.[148] The document outlines the integrated security system that the Government of Canada is creating, using a co-ordinated whole of government approach with key partners from all levels of government; federal,

---

[146] Danforth Middlemiss, testimony from "Canada's Coastlines: The Longest Under-Defended Borders in the World," in *The Report of the Standing Committee on National Security and Defence*, 37th Parliament, 2nd Session, Vol. 1, (October 2003), 113.

[147] "Canada's Coastlines: The Longest Under-Defended Borders in the World," in *The Report of the Standing Committee on National Security and Defence*, 37th Parliament, 2nd Session, Vol. 1, (October 2003), 113.

[148] Privy Council Office, *Securing an Open Society: Canada's National Security Policy* ….

provincial, territorial and municipal, as well as with the private sector and allies. The policy provides for a dynamic system, designed to continuously evolve to address emerging threats as needed, relying heavily on contributions from all stakeholders.

Canada's National Security Policy identifies three core national security interests: protecting Canada and Canadians at home and abroad; ensuring Canada is not a base for threats to our allies; and, contributing to international security.[149] Within this Policy, the Government provides leadership, resources and frameworks in its desire to demonstrate its commitment to build a fully integrated and effective national security system. It created the Department of Public Safety and Emergency Preparedness Canada (PSEPC), known as the Department of Public Safety (DPS) since 2006, and brought the functions of security, intelligence, policing and enforcement, corrections and crime prevention, border services, immigration enforcement and emergency management together. The RCMP, CSIS, CBSA and the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) are now amalgamated under the direction of a single Minister. It also created the Cabinet Committee on Security, Public Health and Emergencies (CC SPHE) in order to manage national security and intelligence issues as well as to provide the coordinated government wide responses to emergencies. Finally, it created the position of National Security Advisor to the Prime Minister who was charged with improving the coordination and integration of security efforts among government departments and to assist in the development of an integrated policy framework for national security and emergencies.[150]

---

[149] *Ibid.,* 4.

[150] Privy Council Office, *Securing an Open Society: Canada's National Security Policy…,* 9.

Through the framework created by the introduction of a National Security Advisor, the creation of the new federal department of Public Safety and Emergency Preparedness, and the overarching mandate given to the Minister, the NSP provides some of the leadership and authority that the Auditor General and the SCONSAD Committee recognized. The NSP gives PSEPC the mandate to lead the whole of government approach in matters of Canadian national security. Canada now has strategic level leadership that should be able to provide the guidance and direction to the national security portfolio.

MARINE SECURITY SUMMARY AND RECOMMENDATIONS

The government's response to marine security is not as well advanced as that to air security. The aviation transportation system is highly regulated and controlled, which is not the case in the marine environment. This is being partially addressed through the MSOC and MIMDEX initiatives, however, the ad hoc nature of the MSOC and the glacial pace of the MIMDEX project threaten to derail this progress. It is recognized that there are privacy concerns in developing an integrated information sharing system that crosses departmental boundaries, however, it is also recognized that there are methods to mitigate this risk rather than to avoid it. Information sharing protocols between departments are available within the *Privacy Act*, especially in the interest of National Security, and the MIMDEX system is being designed with privacy considerations at the forefront. Not only must the MIMDEX project be allowed to proceed in the development of this integrated information system to provide the technical interoperability required, PSEPC must champion this initiative and provide the leadership to work through the roadblocks too implement this project forthwith. Additionally, in order for the MSOCs to

provide a unified and consistent response to all potential threats, and to operate in a cohesive and coordinated fashion, they must move above the ad hoc leadership style they are using. The whole of government approach brings all implicated departments and agencies with a marine security mandate together into the facility, but unity of effort cannot be achieved without consistent leadership. It is therefore recommended that one departmental agency, either the RCMP, as the federal policing force or DND, as leaders in the marine intelligence, surveillance and reconnaissance fields take command of the MSOC organization. Lead agency status can still be given to any of the other partners on a case-by-case basis for specific operations; however there must be someone in charge to provide overall direction should conflicts arise. As with air security, it is recommended that exercises and training scenarios be planned and conducted that stretch the imagination of the possible and the probable.

EMERGENCY MANAGEMENT

Other measures introduced in the National Security Policy that are relevant to the analysis conducted in this paper are within the areas of emergency management and planning. In order to better respond to emergencies, the government announced the establishment of a new Government Operations Centre (GOC), the review and modernization of the Emergency Preparedness Act, the co-location of federal, provincial and municipal emergency measures centres and the creation of a critical infrastructure protection strategy for Canada.[151] The GOC, under the direction of PSEPC, has been given the mandate to provide strategic level direction and coordination in response to

[151] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*…, 21.

emerging or current threats that affect the national interest, and has been designed as the central node for communications and support within the whole of government response structure.[152] This is particularly important if the emergency is a natural or pandemic emergency. As detailed above, air security and to a certain extent marine security have existing or developing frameworks and response mechanisms to address threats in their respective realms; however responses to natural or pandemic emergencies will involve different organizations, including different levels of government and the private sector, depending on the nature of the threat. These threats, like fires, floods, and hurricanes, are normally managed at the first responder level and escalate to higher-level organizations only if they are beyond the capability of that particular level. The response to these threats is thus ad hoc in nature, as emergency response in Canada is based on the gradual and controlled application of resources to meet the needs and unique requirements of each situation. Under the constitution, emergency management is within the legislative responsibilities of the respective provinces, unless the event has national impact at the outset. Thus, in general, the responsibility to deal with emergencies is placed first on the individual and then on successive levels of government, from the municipal to the provincial and then to the federal level.[153] While each province and territory has a slightly different way of managing emergency responses, their processes is similar in that they each have a tiered response that initiates at the municipal first responder level. However coordination of the tiered response above the provincial level has been lacking,

---

[152] Major Tim Lannan, "Interagency Coordination within the National Security Community: Improving the Response to Terrorism," *Canadian Military Journal*, (Autumn 2004), 49.

[153] Emergency Preparedness Canada, *The Emergency Site Management System: A Doctrine Paper*, (Ottawa: Public Works and Government Services Canada, 1998), 3.

as the federal, provincial, and territorial ministers responsible for emergency management met for the first time in 11 years in January 2005.[154]

The whole of government approach can work very effectively in providing the prevention, mitigation and response actions to these types of emergencies, and the military is better poised today to assist in this endeavour. The Canadian Forces are in a better position to not only respond to emergencies within the domestic environment, as a result of a transformational change to the command and control structure of the CF, they are in a direct position to assist in the planning, preparation for and mitigation of any threats so as to minimize or eliminate the actual event from occurring. The Government's release of its International Policy Statement, with a new Defence Policy Statement, provides the framework for this.

The Role of Pride and Influence in the World – Canada's International Policy Statement

The Government of Canada issued its International Policy Statement in 2005 with clear intentions to embrace the whole of government approach by addressing each of the Defence, Diplomacy, Development and Commerce lines of operations. It was recognized that in the 10 years leading up to this policy statement the issues that dominated the global arena had been transformed and became too complex to be handled in the traditional "silo" methodology of government. Departments and agencies had to become better connected and the system as a whole needed to be more efficient at leveraging

[154] Privy Council Office, *Securing an Open Society: One Year Later,* (Ottawa: PCO, 2005), 17.

assets.[155] A coherent policy that integrates security, development and trade is required. The Defence Policy Statement, a subset of this International Policy Statement, has provided promising guidance and direction for the military to play a strong role in the whole of government approach in the domestic environment, a role the CF previously assisted in only as the department of last resort.

The Role of Pride and Influence in the World – Canada's Defence Policy Statement

The Government called for an effective, responsive and relevant 21st Century Canadian Military, a force able to defend Canada and Canadian interests and values while contributing to international peace and security.[156] This new defence policy presents a vital new vision for the Canadian Forces with a focus on "Canada First" and the protection of Canada and Canadians. The first priority is the defence of Canada, and in this vein the CF created an operational structure with a unified and integrated chain of command at both the national and regional levels. As part of the new Canada First strategy, the CF will work more closely with civil authorities at all levels (federal, provincial and local) to help prevent serious threats from occurring, or to help mitigate the effects of the threat.[157] To this end, General Rick Hillier, the Chief of the Defence Staff (CDS), directed the commencement of an overall transformation of the CF not seen

---

[155] Department of Foreign Affairs and International Trade, *Canada's International Policy Statement: A Role of Pride and Influence in the World – Overview*, (Ottawa: Department of Foreign Affairs and International Trade, 2005), 28.

[156] Department of National Defence, *Canada's International Policy Statement: A Role of Pride and Influence in the World – Defence,* (Ottawa: Department of National Defence, 2005), 2, 11-12, 17, 32.

[157] Department of National Defence, *Canada's International Policy Statement: A Role of Pride and Influence in the World – Defence,* (Ottawa: Department of National Defence, 2005), 18.

since the mid 1960s, when the navy, army and air force were amalgamated.[158] Hillier's vision is of a networked CF, with an effective, capable and integrated infrastructure operating under a 'command centric' umbrella, so that the CF can move from the ad hoc era of crisis-response to the new paradigm of optimized contingency response.[159] The command-centric structure will ensure unity of command in that Commanders at all levels will be operationally focused towards achieving their goal, accountable for clearly assigned authorities and responsibilities. They will also fully understand their commander's intent. This concept of mission command will give commanders the ability to execute operations without direct order, in periods of uncertainty and ambiguity, in order to attain assigned strategic, operational and tactical objectives. [160]

The creation of Canada Command allows the CF to provide relevant, responsive and effective forces and resources from across Canada to wherever a crisis or threat occurs. These forces are relevant in that they have a unified operationally focussed Command structure. They are responsive in that their structure allows them to mobilize and deploy personnel to deal with any crisis, and they are effective by considering Canada as a single operational theatre, with one chain of command.[161] For the first time in CF history, a unified and integrated chain of command at the national and regional

---

[158] Department of National Defence, "Canadian Forces Begin Transformation: Commander of Canada Command and Stand-Up Date Announced," available from www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1691; Internet; accessed 25 March 2008.

[159] Captain Vance White, The Strategic Command Construct," *The Maple Leaf*, Vol 8: No 38, (2 November 2005), 1; available from http://www.forces.gc.ca/site/community/mapleleaf/article_e.asp?id=2024; Internet; Accessed 24 March 2008.

[160] *Ibid.,* 1.

[161] Backgrounder, "Canada Command," (June 28, 2005); available from http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1692; Internet; accessed 10 March 2008

levels has immediate authority to deploy maritime, land and air assets in support of domestic operations.[162]

The Commander of Canada Command is now the direct national operational authority for the defence of Canada and North America. Military forces under his command provide civilian authorities with direct military operational assistance in both routine and contingency scenarios, but they do not replace the civilian authorities. The CF supports the civilian authorities during crises or in operations of national interest that require the special skills or unique capabilities that the CF can provide.[163] The CF has been the force of last resort in domestic operations due to legal and constitutional reasons, however with this new construct and mission focus towards the defence of Canada and Canadians, the CF is poised to play a larger role in domestic security. The CF is organized, trained and equipped to defend Canada and has the capacity to respond to developing domestic emergency and national security situations.[164] The CF has published doctrine and procedures that are followed whenever there is a request for assistance, however, with this new construct under a command organization devoted to supporting domestic operations, Canada Command should become more involved in the planning, training and preparation for these types of situations to ensure that there is an effective whole of government approach, with all implicated agencies involved at the earliest opportunity. Unfortunately the Canadian emergency management framework is reactive

---

[162] Kristin Harold, "Star Top Shuffle Spotlights DND's need for new Home," (28 September 2005); available from http://www.ottawabusinessjournal.com/284348484419516.php; Internet; accessed 10 March 2008.

[163] Department of National Defence, "Canada Command Website," http://www.canadacom.forces.gc.ca/en/index_e.asp; Internet; accessed 10 March 2008.

[164] Department of National Defence, *DCDS Direction for Domestic Operations*, (Ottawa: DND Canada, 2005), 1-1.

in nature, not proactive, thus does not currently support the direct involvement of Canada Command. This framework will be examined in the following section, with recommendations provided in order to make effective use of the resources available from the whole of government.

Emergency Management Framework in Canada

As previously mentioned, emergency response in Canada is based on the gradual and controlled application of resources to meet the needs and unique requirements of each situation. In general, the responsibility to deal with emergencies is placed first on the individual and then on successive levels of government, from the municipal to the provincial and then to the federal level. Disaster response is initiated at the municipal level through the use of first responders (fire, police and paramedic services). Provincial and federal resources may be provided when requested if the resources of the lower level are insufficient to provide an effective response municipality. This is the basis of the Emergency Site Management system employed in Canada, which is an effective mechanism to handle emergencies where the incident is localized and/or there is no extensive or widespread damage.

Based on recent emergencies, however, including the SARS epidemic in 2003, the ice storm in central Canada in 1998, and the Winnipeg floods in 1997, the Canadian emergency management community has recognized the requirement for an overarching whole of government response framework in order to provide a mechanism for emergencies that are clearly of national interest or that require a response from multiple departments or agencies. The challenge is to coordinate between departments and

agencies and across three levels of government. The federal level is responsible to provide funding and planning, the provincial level is responsible to administer the funds and assist in the planning and the municipal level then actually provides the response. Thus developing a national coordinated approach to disaster response is difficult at best.[165] The organizational interoperability challenges are daunting, but must be overcome to ensure an effective emergency response.

In response to the SARS epidemic in 2003, the Standing Senate Committee on Social Affairs, Science and Technology, wrote a report indicating that emergency response procedures need to be better integrated. It noted that while there are considerable resources available at various government levels, it is the lack of "adequate coordination and the absence of a sharp focus in the face of an emergency that is the problem, and it is clear that greater collaboration must be part of the solution."[166] The SARS Commission noted that the response to SARS was "hamstrung by an unwieldy emergency leadership structure with no one clearly in charge."[167]

Emergency management is based on four interdependent risk based functions that follow the classic threat model previously shown in Figure 4.1. The functions are prevention and mitigation, preparedness, response and recovery. As the threat model identifies, if considerable effort is placed on the first two functions, prevention and mitigation as well as preparedness, the threat may be averted entirely or lessened in severity, such that the response and recovery phases are easier to handle, which in turn

---

[165] Standing Senate Committee on National Security and Defence, *National Emergencies: Canada's Fragile Front Lines*, (Ottawa: Senate, 2004), 38.

[166] Standing Senate Committee on Social Affairs, *Science and Technology, Reforming Health Protection and Protection in Canada, Time to Act,* (Ottawa: Senate, 2003), 17.

[167] Archie Campbell, *The SARS Commission Final Report: Spring of Fear*, (Toronto: Ontario Ministry of Health and Long-Term Care, 2006), 33.

could lead to significantly less damage, personal trauma and social, economic and environmental cost.[168] The practical challenge is to provide the appropriate levels of resources to prevention and mitigation efforts such that, if the threat does not materialize, the financial efforts are not considered wasted.

In order to provide this integrated approach in establishing a collaborative security environment, PSEPC was assigned the responsibility to establish and operate a Government Operations Centre (GOC), as well as to develop and implement a National Emergency Response System (NERS). NERS is expected to assist in prevention, mitigation and preparedness by providing the framework in support of incident identification, warning and notification, information sharing, incident analysis, planning and operations coordination. However, this system is still in the planning stage, and, even when fully functional, is only being designed to provide for national policy direction and strategic coordination during an actual emergency. There is no collaborative network in place for planning activities between government departments or agencies.[169] In April 2005, the OAG noted significant problems with the federal response to emergency preparedness, with particular emphasis on the progress of NERS. The report identifies that NERS is key to the effective collaboration between other federal departments and agencies, and that until NERS is fully implemented, the federal response will be fragmented. The report recommends that PSEPC, now DPS, obtain formal agreement from the other federal departments and agencies regarding the construct of NERS, and

---

[168] Public Safety and Emergency Preparedness Canada, *An Emergency Management Framework for Canada*, (Ottawa: Public Safety and Emergency Preparedness Canada, 2007), 4.

[169] Department of National Defence, *DND/CF Network Enabled Operations Working Paper*, (Ottawa: Defence Research and Development Canada, 2006), 20-21.

that the command and control structure governing the federal response to emergencies be formalized.[170]

The GOC is Canada's strategic level headquarters. It is the federal operations centre for the entire country, intended to unite the efforts of all federal departments and agencies during national emergencies. Housed at DPS, it is a resource available to any federal department or agency during a crisis, and is designed to be the hub of a network of operations centres, each run independently by other federal departments and agencies, such as the MSOC, described earlier, the RCMP, Canada Command, Health Canada, and CSIS.[171] However, without NERS, or other networked collaboration systems, communication and coordination between the various ops centres are ad hoc at best. Additionally, without the direct participation of the other departments and agencies, the prevention, mitigation and preparedness activities that form the first two emergency management functions will not get accomplished. This means that the ability to reduce damage, personal trauma and social, economic and environmental costs in the event of a federal emergency are greatly diminished.

Currently then, the federal government maintains a federal operations centre without the ability to collaborate with other federal departments or agencies, who in turn manage their own independent stove-piped operations centres. It is in this area that I suggest that the CF, particularly Canada Command, can play a supporting role. The CF has doctrine in place to support domestic operations, and, by virtue of the inherent flexibility and training of military personnel and units, stands ready to support domestic

---

[170] Office of the Auditor General of Canada, *Report of the Auditor General of Canada - April 2005*, (Ottawa: Public Works and Government Services Canada, 2005), 20.

[171] Public Safety Canada Website, "The Government Operations Centre," http://www.ps-sp.gc.ca/prg/em/goc/index-eng.aspx; Internet; accessed 10 April 2008.

operations whenever the lead civil authorities call upon them.[172] However, an effective application of the whole of government approach would have a governance structure to provide direct liaison between the Canada Command Regional Headquarters and the regional emergency management headquarters of DPS. Additionally, where possible, the provincial emergency management headquarters should also be collocated. In this fashion, the regional headquarters would consist of members of the municipal, provincial and federal emergency management organizations as well as with military members of Canada Command. With its hierarchical command structure, Canada Command also has the command and control (C2) and communications systems to tie into these regional headquarters as well as the GOC so that all levels of government can effectively manage any eventuality. This will allow for synergies, and cooperation and trust to be developed at the earliest possible stage, and any planning and/or exercise activity will involve the full range of support from the outset. The proactive culture of the military, with a focus on extensive training in planning and preparation can assist the more reactionary emergency management organizations plan and prepare for natural disasters or pandemics. Training, education and exercise programs must be initiated that are all-inclusive, with buy in and participation from the municipal, provincial and federal emergency management organizations. Participation at CFC by other government departments, especially in the Operational Planning Process (OPP) would go a long way in meeting this need. Additionally, individuals must be identified, either as liaison officers or participants in the consolidated emergency management operations centres so that exercises and training can be undertaken. This permits the teams to be developed in

[172] Department of National Defence, *DCDS Direction for Domestic Operations,* (Ottawa: J3 Continental, 2005), 1-1.

the early planning stages, which fosters synergies and trust. If we really want to nurture this whole of government approach, it is unproductive for organizations to be cobbled together to support an event, only to have the people return to their normal job back at their department or agency, only to relearn the process and foster the knowledge, teamwork and trust at the next event. Especially in regions where disasters are predictable, there is no excuse not to develop clear governance structures to plan, prepare, exercise and train for such events, like earthquakes in British Columbia, and floods in Manitoba.[173]

EMERGENCY MANAGEMENT SUMMARY AND RECOMMENDATIONS

The emergency management framework in Canada is less than ideal. There is little coordination between the municipal, provincial and federal levels of government as the respective emergency operations centres are not collocated, are not manned on a continuous basis, and do not have any level of technical interoperability between them, with the exception of the telephone system. Without NERS, the emergency preparedness and management system is still very reactionary and isolated. The ability to provide an effective whole of government approach with active participation from the other departments and agencies in the planning and preparation for emergencies is not possible.

It is recommended that leadership within DPS expedite the development and implementation of NERS in order to provide the technical interoperability required for an effective whole of government approach to emergency planning and management. Additionally, in order to break away from the reactionary culture currently inherent in the

---

[173] Andrew Archibald and Trefor Munn-Venn, *A Resilient Canada* …, 18.

municipal, provincial and federal levels of government regarding national emergencies, and to foster a cohesive coordinated and proactive response, it is recommended that the headquarters of the provincial and federal emergency management offices be collocated, and where possible, these be collocated with the regional headquarters of Canada Command. It is also recommended that liaison officers from the various organizations work together in developing plans and mitigation strategies so as to foster the synergies, cooperation and trust necessary to effectively operate in a whole of government framework. Proactive planning, exercises and training will help prevent a natural disaster from becoming a national emergency.

CHAPTER 5: RECOMMENDATIONS AND CONCLUSION

> Major emergencies require extremely close cooperation between the federal government, provinces and territories, communities, first line responders and the private sector. National emergency coordination currently suffers from the absence of both an effective federal-provincial governance regime, and from the absence of commonly agreed standards and priorities for the national emergency management system.[174]

The whole of government approach predates the tragic events of 9/11. Governments were amalgamating departments into more homogenous organizations to reduce autonomy and increase efficiency, with most of the early efforts focussed on grouping departments and agencies with similar mandates, cultures and structure. The main resistance was a diminishing in the control of resources, infrastructure and budgets, that the individual departments and agencies previously exercised.

With the increased instability in the world after 9/11, every major challenge, from security to the development of social and economic policies, required the active participation of the whole of government as these complex issues span the responsibilities of more than one government department or agency. Innovative solutions were required to bring together the disparate organizations that each owned pieces of the puzzle. The primary challenge in bringing these groups together was that, unlike previous whole of government initiatives, these groups did not share mission areas and they had profound differences in culture. This created challenges in achieving unity of effort due to the diverse cultures, competing interests and differing priorities of the participating organizations. Leadership is crucial, as the intent is to bring the skills, knowledge and expertise from within these disparate organizations to achieve a common goal rather than just sharing social space.

---

[174] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*…, 24.

In order to provide an integrated response, the organizations require some level of interoperability. Interoperability describes the ability to work together in a seamless, uniform and efficient manner across multiple organizations and information technology systems. Promoting interoperability between agencies is a key focus to achieving this whole of government collaboration. The ultimate goal of interoperability is to ensure that the organizations involved in the collective venture achieve a practical level of cooperation. Interoperability has two dimensions, technical and organizational. The former is relatively easy to resolve, in that systems and equipment can be modified, designed, or built to satisfy the information management requirements, however the latter is buried deep in culture and tradition, with the lack of effective governance structures seen as the key impediment to achieving unity of effort. Clear leadership and a clear articulation of the mission, roles and responsibilities and accountability frameworks are needed to develop organizational interoperability.

AIR SECURITY

The Canadian Government initiated efforts to strengthen national security shortly after 9/11, with their initial focus on air security. The air security of North America, through the actions of NORAD, TC, NAV Canada and the FAA already embody the whole of government approach, in an arrangement that originated in 1952, long before the attacks of 9/11. There is little new that was required other than increased vigilance towards threats that originated within North American airspace, and the institution of increased information sharing measures between the commercial air carriers and TC,

along with the creation of a no-fly list. One area for improvement is in line with increased vigilance.

The following recommendation is provided to strengthen the whole of government approach to air security:

1. Air security exercises should be planned and conducted that involve the entire aviation security community and that stretch the imagination of the possible and the probable.

MARINE SECURITY

Coordination and collaboration in the marine security environment was not as well established as that in the air environment. Marine traffic is much less regulated, as there are a myriad of agencies with differing mandates within this environment. Two initiatives were undertaken, one to increase technical interoperability, and the second to increase organizational interoperability.

In order to improve the level of technical interoperability, MIMDEX was initiated by DND to amalgamate existing government information and information networks, and to fuse this information into a common data repository in order to provide a more complete representation of the vessels, cargo and people operating in the marine environment, as well as to facilitate coordinated action and alert departments to potential targets of interest. However, the pace of progress is glacial at best due to perceived legal barriers to information sharing. Unless senior governmental leadership steps in as a champion, the politically risk-averse nature of the various departments and agencies involved will continue to make this a contentious issue, further delaying or even cancelling this project.

Organizational interoperability for the marine environment is to be provided through the creation of the MSOC's, which are designed to enhance marine intelligence, surveillance and reconnaissance capabilities through the collaborative participation of DND, RCMP, TC, CCG and CBSA. However, the leadership model being planned for these facilities is ad hoc, with lead agency status assumed for specific operations on a case-by-case basis. However, the degree of organizational interoperability required for this endeavour goes well beyond the level that ad hoc leadership can provide. An ad hoc leadership system is highly personality driven, and can indeed result in strong information sharing and interoperability, but not by doctrine or policy. Thus, it could just as easily result in a lack of interoperability. In order to assure unity of effort, leadership must be provided through a hierarchical directive approach, with the associated doctrine detailing the roles and responsibilities of the various organizations.

The following recommendations are provided to strengthen the whole of government approach to marine security:

1. The Canadian Government should set an overarching marine security policy in line with the National Security Policy. The MSOCs need strengthened mandates and responsibilities to become a NORAD-like entity, responsible not only for deterrence and defence, but also to initiate the response action.

2. The development and implementation of MIMDEX should be expedited and the associated legislative review intensified to resolve the perceived legal barriers.

3. Overall Command of the MSOCs should be delegated to one departmental agency, either the RCMP, as the federal policing force, or DND, as leaders in the marine intelligence, surveillance and reconnaissance fields take command of the MSOC organization. Lead agency status can still be given to any of the other partners on a case-by-case basis for specific operations; however there must be someone in charge to provide overall direction should conflicts arise.

4. Marine security exercises should be planned and conducted that involve the entire marine security community and that stretch the imagination of the possible and the probable.

EMERGENCY MANAGEMENT

Emergency response in Canada is based on the gradual and controlled application of resources to meet the needs and unique requirements of each situation. In general, the responsibility to deal with emergencies is placed first on the individual and then on successive levels of government, from the municipal to the provincial and then to the federal level. Based on recent emergencies however, including the SARS epidemic, the ice storm and the Winnipeg floods, the Canadian emergency management community recognized the requirement for an overarching whole of government response framework in order to provide a mechanism to plan, prepare for and respond to emergencies that are clearly of national interest or that require a response from multiple departments or agencies. In order to provide this integrated approach, PSEPC was assigned the responsibility to establish and operate the GOC, as well as to develop and implement NERS.

Like MIMDEX in the marine environment, NERS is designed to provide the technical interoperability to support emergency management between the various operations centres. NERS is key to the effective collaboration between other federal departments and agencies, and is currently in the developmental stage, thus until is fully implemented, the federal response will be fragmented.

The GOC, as Canada's strategic level headquarters, is intended to provide organizational interoperability by uniting the efforts of all federal departments and agencies during national emergencies. It is designed to be the hub of a network of

operations centres, each run independently by other federal departments and agencies, such as the MSOC, the RCMP, Canada Command, Health Canada, and CSIS, as well as the emergency management operations centres stood up by the municipal and provincial governments, once an event has occurred. This reactionary culture is insufficient to provide the level of security required in today's complex environment. Emergency management must become proactive, with a nucleus of departments and agencies integrated into an organization that is planning and preparing for such emergency situations. Canada Command, the CF organization tasked with providing military support to domestic operations, can play a leadership role in this proactive approach.

The following recommendations are provided to strengthen the whole of government approach to emergency management:

1. The approach to emergency management should become more proactive. Canada Command can provide the experience, skills and knowledge in creating and developing plans to prepare for and manage emergency situations. Their status as the department of last resort status, only to be brought in after all other resources are exhausted, must be changed.

2. The development and implementation of NERS should be expedited in order to provide the technical interoperability required for an effective whole of government approach to emergency planning and management.

3. Training, education and exercise programs should be initiated that are all inclusive. Organizations must be stood up where personnel can work together as a unit, planning and preparing for events, rather than being cobbled together to respond to a crisis and then return to their normal jobs, only to have to relearn the process during the next crisis. Liaison positions between government departments will help establish some of the synergies, as roles and responsibilities, as well as expectations can be determined early.

4. Emergency exercises should be planned and conducted that involve the entire emergency management community and that stretches the imagination of the possible and the probable.

It has been almost seven years since 9/11, and while the Government has been making progress, the speed makes one wonder where national security lies in the priority list. Additionally, there are instances where it appears that the Government's interest in maintaining a whole of government approach is waning. In early April 2008, the government quietly stopped providing biannual classified briefings to municipal, provincial and non-governmental energy industry operators, even though this was considered to be "the most sophisticated example of the public-private collaboration the federal government insists is essential for national security."[175] Senator Kenny, the Chair of SCONSAD recently summed up his concerns regarding the steady decline in spending and apparent lack of interest on national security initiatives when he hinted that it might take a terrorist attack on Canadian soil for the Government to take notice. "Until there's a big, bad event, there are no votes in it."[176]

The analysis conducted for this paper though, demonstrates that the Government is making headway in applying the whole of government approach towards national security. Both the National Security Policy and the International Policy Statement have outlined strong initiatives, which, when implemented will go a long way to filling the current gaps in our national security. These initiatives, however, require significant increases in technical and organizational interoperability, that cannot be expected to happen overnight. Let us hope that DPS provides the leadership to continue to expedite these initiatives in order to ensure an event as described by Senator Kenny does not occur.

---

[175] Ian MacLeod, "The State of Emergency," *Ottawa Citizen*, 12 April 2008, 1; available from http://www.canada.com/ottawacitizen/news/story.html?id=3dd3d47a-24a8-4b03-86d8-9c31b1d1f849&k=88593; Internet; accessed 12 April 2008.

[176] Jan Ravensbergen, "Senator slams security spending," *Ottawa Citizen*, 18 April 2008, 1; available from http://www.canada.com/ottawacitizen/news/story.html?id=b0a94213-289f-4790-8990-505b66cd7ce9; Internet; accessed 18 April 2008

BIBLIOGRAPHY

AFCEA White Paper. "The Need to Share: The U.S. Intelligence Community and Law Enforcement." 2007; available from https://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf; Internet; accessed 29 February 2008.

Aikins, Greg. "Interdepartmental Intelligence: The Key Factor for Maritime Security." A Presentation to A Conference hosted by the Centre for Foreign Policy Studies, Dalhousie University. (10-12 June 2005); available from http://centreforforeignpolicystudies.dal.ca/pdf/msc2005/msc2005aikens.ppt; Internet; accessed 24 March 2008.

———. Network-Centric Operations and Interdepartmental Marine Security." *Canadian Naval Review*, Vol 1 No 3 (Fall 2005).

Archibald, Andrew and Trefor Munn-Venn. *Building Resilience: Leadership and Accountability*. Ottawa: Conference Board of Canada. March 2008.

Archibald, Andrew and Trefor Munn-Venn. *A Resilient Canada: Governance for National Security and Public Safety.* Ottawa: Conference Board of Canada. November 2007.

Aucoin Peter. "Accountability and Coordination with Independent Foundations: A Canadian Case of Autonomy." In Autonomy and Regulation: Coping with Agencies in the Modern State, edited by Tom Christensen and Per Lægreid, Cheltenham, UK: Edward Elgar 2006.

Aucoin, Peter. "Beyond the 'New" in Public Management Reform in Canada: Catching the Next Wave." Chap. 3 in *The Handbook of Canadian Public Administration,* edited by Christopher Dunn, 37-52. Montreal: Oxford University Press, 2002.

Aucoin, Peter and Mark D. Jarvis. *Modernizing Government Accountability: A Framework for Reform.* Ottawa: Canada School of Public Service, 2005.

Auf der Heide, Erik. *Disaster Response: Principles of Preparation and Coordination*. [book on-line]; available from http://orgmail2.coe-dmha.org/dr/static.htm; Internet; accessed 22 March 2008.

Auger A., D. Gouin and J. Roy. *Decision Support and Knowledge Exploitation Technologies for* C4ISR TM 2004-451. Ottawa: Defence R&D Canada, 2006.

Australia. Attorney-General. *Communications Legislation Amendment (Information Sharing and Datacasting) Bill 2007*. Canberra: Australian Public Service Commission, 2007; available from http://www.comlaw.gov.au/comlaw/Legislation/Bills1.nsf/0/404BE354484D50CACA257300001086F3?OpenDocument; Internet; accessed 3 April 2008.

———. Commonwealth of Australia. *Tackling Wicked Problems – A Public Policy Perspective*. Canberra: Australian Public Service Commission, 2007.

———. Government Information Management Office. *Australian Government Information Interoperability Framework.* Canberra: Australian Public Service Commission, 2006; available from http://www.agimo.gov.au/publications/2006/may/iif; Internet; accessed 3 April 2008.

———. Management Advisory Committee. *Connecting Government: Whole of Government Responses to Australia's Priority Challenges.* Canberra: Australian Public Service Commission, 2004; available from http://www.apsc.gov.au/mac/connectinggovernment1.htm; Internet; accessed 26 February 2008.

———. State Services Authority. *Joined Up Government. A Review of National and International Experiences*. Melbourne: State Government of Victoria. 2007.

Avis, Captain(N) Peter. "Surveillance and Canadian Maritime Domestic Security." *Canadian Military Journal*, (Spring 2003).

Avis, Captain(N) Peter and Iain Grant. "Canadian Maritime Security and the Culture of Prevention." *Canadian Military Journal*, (Winter 2004-2005).

Babcock, Sandy. *DND/CF Network Enabled Operations Working Paper*. Ottawa: DRDC TR 2006-001, January 2006.

Bakvis, Herman and Luc Juillet. *The Horizontal Challenge: Line Departments, Central Agencies and Leadership*. Ottawa: Canada School of Public Services, 2004.

Barr, Col David. "The Kananaskis G8 Summit: A Case Study in Interagency Cooperation." *Canadian Military Journal*, Winter 2003-2004.

Bearne, Susanna, Olga Oliker, Kevin A. O'Brien, and Andrew Rathmell. *Technical Report on National Security Decision-Making Structures and Security Sector Reform*. Santa Monica: Rand Corporation, 2005 available from http://www.rand.org/pubs/technical_reports/2005/RAND_TR289.sum.pdf; Internet; accessed 3 April 2008.

Bell, Louise. *The Global Conflict Prevention Pool. A Joint UK Government Approach to Reducing Conflict*. Department for International Development. Prepared by FCO Creative Services. August 2003.

Bogdanos, Matthew F. "Joint Interagency Cooperation: The First Step." *Joint Forces Quarterly*, 37; available from http://www.dtic.mil/doctrine/jel/jfq_pubs/0437.pdf; Internet; accessed 29 February 2008.

British Columbia Innovation Council. *Port Security Requirements – An Analysis of Industrial Opportunities for Small and Medium Enterprises in Port Security Requirements.* December 2004.

Brook, Douglas A. and Cynthia L. King. "Civil Service Reform as National Security: The Homeland Security Act of 2002." *Public Administration Review*, 67. 3. (May/Jun 2007).

Buck, Vice Admiral Ron. "Keynote Address: Continental Security from a Maritime Perspective." in *Continental Security and Canada-U.S. Relations: Maritime Perspectives, Challenges and Opportunities*. edited by Robert H. Edwards and Graham Walker. Centre for Foreign Policy Studies: Dalhousie University, May 2004.

Canada. Auditor General of Canada. *Report of the Auditor General Of Canada to the House of Commons- March 2004*. Ottawa: Public Works and Government Services Canada, 2004.

———. Department of Foreign Affairs and International Trade. *Canada's International Policy Statement: A Role of Pride and Influence in the World – Overview*. Ottawa: Department of Foreign Affairs and International Trade, 2005.

———. Department of National Defence. B-GG-005/004/AF-000 *Canadian Forces Operations*. Ottawa: DND Canada, 2000.

———. Department of National Defence. Backgrounder. "Canada Command." (June 28, 2005); available from http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1692; Internet; accessed 10 March 2008.

———. Department of National Defence. "Canada Command Website." http://www.canadacom.forces.gc.ca/en/index_e.asp; Internet; accessed 10 March 2008.

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

———. Department of National Defence. "Canadian Forces Begin Transformation: Commander of Canada Command and Stand-Up Date Announced." (June 28, 2005); available from www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1691; Internet; accessed 25 March 2008.

———. Department of National Defence. *DCDS Direction for Domestic Operations.* Ottawa: J3 Continental, 2005.

———. Department of National Defence. *DND/CF Network Enabled Operations Working Paper.* Ottawa: Defence Research and Development Canada, 2006.

———. Department of National Defence. *Marine Security Operations Centres Scope Statement*. Project no. 00000806, File no. 30000806-326 Amdt 1. 22 June 2005; available from http://www.msoc-cosm.gc.ca/document/background/docs/msoc_project_scope_22jun05_e.pdf; Internet accessed 12 April 2008.

———. Department of National Defence. Backgrounder, "NORAD." (12 May 2006), http://www.forces.gc.ca/site/newsroom/view_news_e.asp?id=1922; Internet; accessed 3 April 2008.

———. Department of Justice. *Canadian Constitution Act, 1867;* available from http://laws.justice.gc.ca/en/const/c1867_e.html#provincial; Internet; accessed 16 April 2008.

———. Emergency Preparedness Canada. *The Emergency Site Management System: A Doctrine Paper.* Ottawa: Public Works and Government Services Canada, 1998.

———. House of Commons. The Government's Response to the *Report of the Special Senate Committee on Security and Intelligency – 1999.* Thursday, December 16,1999; available from http://ww2.ps-sp.gc.ca/publications/Speeches/19991216_e.asp; Internet; accessed 29 March 2008.

———. Office of the Auditor General of Canada. *Report of the Auditor General of Canada - April 2005*. Ottawa: Public Works and Government Services Canada, 2005.

———. Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Ottawa: PCO, 2004.

———. Privy Council Office. *Securing an Open Society: One Year Later.* Ottawa: PCO, 2005.

———. Public Safety Canada Website. "The Government Operations Centre." http://www.ps-sp.gc.ca/prg/em/goc/index-eng.aspx; Internet; accessed 10 April 2008.

———. Public Safety and Emergency Preparedness Canada "Emergency Management Organizations." Canada. http://getprepared.ca/who/emo_e.asp; Internet; accessed 10 April 2008.

———. Public Safety and Emergency Preparedness Canada. Introduction of the Emergency Management Act. Canada. http://www.publicsafety.gc.ca/media/bk/2005/bk20051117-en.asp; Internet; accessed 10 April 2008.

———. Public Safety and Emergency Preparedness Canada. Interoperability Directorate Website; http://www.tbs-sct.gc.ca/im-gi/imday04jourgi/info/ip-pi/page22_e.asp; Internet; accessed 19 March 2008.

———. Public Safety and Emergency Preparedness Canada "What we do." http://www.ps-sp.gc.ca/abt/wwd/index-en.asp; Internet; accessed 10 April 2008.

———. School of Policy Studies, Queens University. *Canada Without Armed Forces?* edited Douglas L. Bland, Kingston: McGill-Queen's University Press, 2004.

———. Service Canada Website. "People Serving People." http://www.servicecanada.gc.ca/en/home.shtml; Internet; accessed 18 March 2008.

———. Standing Senate Committee on National Security and Defence. *Canadian Security Guide Book, 2005 Edition, An Update of Security Problems in Search of Solutions, A Report of the Standing Senate Committee on National Security and Defence*. Ottawa: The Standing Committee on National Security and Defence, December 2004.

———. Standing Senate Committee on National Security and Defence. *Canadian Security and Military Preparedness, Report of the Standing Committee on National Security and Defence*. Ottawa: The Standing Senate Committee on National Security and Defence, February 2002.

———. Standing Senate Committee on National Security and Defence. "Canada's Coastlines: The Longest Under-Defended Borders in the World." in *The Report of the Standing Committee on National Security and Defence*. 37th Parliament, 2nd Session, Vol. 1, October 2003.

———. Standing Senate Committee on National Security and Defence. *National Emergencies: Canada's Fragile Front Lines, An Upgrade Strategy, Report of the Standing Committee on National Security and Defence*. Ottawa: The Standing Committee on National Security and Defence, March 2004.

———. Standing Senate Committee on Social Affairs. *Science and Technology, Reforming Health Protection and Protection in Canada, Time to Act.* Ottawa: Senate, 2003.

———. Transport Canada. "Passenger Protect Program." http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm; Internet; accessed 25 March 2008.

———. Transport Canada. "Transport Canada Aeronautical Information Manual." available from http://www.tc.gc.ca/CivilAviation/publications/tp14371/RAC/1-1.htm#1-9; Internet; accessed 3 April 2008.

———. Treasury Board. *Canada's Performance 2002 – Annual Report to Parliament*. Ottawa: Treasury Board of Canada Secretariat, 2002.

———. Vice Chief of the Defence Staff. "Glossary for Strategic Capability Planning for the CF." *Strategic Capability Planning for the Canadian Forces*. Ottawa: Department of National Defence, June 2000.

CBC News. "Obama wants Congress to Probe Passport Breach." 21 March 2008; available from http://www.cbc.ca/world/story/2008/03/21/obama-passport.html; Internet; accessed 21 March 2008.

———. "Airline Bomb Plot." 10 August 2006; available from http://www.cbc.ca/news/background/ussecurity/airplane-bombplot.html; Internet; accessed April 3 2008.

Christensen, Tom, and Per Lægreid. *The Whole of Government Approach – Regulation, Performance, and Public-Sector Reform.* Oslo: Stein Rokkan Centre for Social Studies, 2006

Christensen, Tom, and Per Lægreid. "The Whole of Government Approach to Public Sector Reform." *Public Administration Review*. (November/December 2007).

Campbell, Archie. *The SARS Commission Final Report: Spring of Fear*. Toronto: Ontario Ministry of Health and Long-Term Care, 2006.

———. The SARS Commission Interim Report: SARS and Public Health in Ontario. Toronto: Government of Ontario, 2004.

Catterall, Peter. *How Imperial was the Committee of Imperial Defence*? London: Institute of Contemporary British History; available from http://www.psa.ac.uk/publications/psd/1998/catterall.htm; Internet; accessed 3 April 2008.

Christensen, Tom and Per Laegreid. "The Whole-of-Government Approach to Public Sector Reform." *Public Administration Review*, (November/December 2007).

Clark, Thea and Richard Jones. *Organisational Interoperability Maturity Model for C2*. Canberra: Department of Defence, 1999; available from http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/049clark.pdf; Internet; accessed 31 March 2008.

Clarke, Richard A. *Against All Enemies: Inside America's War on Terror.* New York: Free Press, 2004.

Dawes, Sharon S. "Interagency Information Sharing: Expected Benefits, Manageable Risks." *Journal of Policy Analysis and Management*, Vol 15, No 3, (1996).

Elson, Peter. Marilyn Struthers, and Joel Carlson. *Horizontal Tools and Relationships: An Internal Survey of Government Practices Related to Communities*. Ottawa: Human Resources and Social Development Canada, 2007; available from http://www.hrsdc.gc.ca/en/cs/sp/sdc/task_force/tfci02/FinalHorizontalityReportJanuary2007_english.pdf; Internet; accessed 3 April 2008.

FAA Website. "FAA Mission." http://www.faa.gov/about/mission/activities/; Internet; accessed 3 April 2008.

Fitz-Gerald, Ann M. "Addressing the Security-Development Nexus: Implications for Joined-Up Government." *Policy Matters* 5, no. 5 (2004): 24.

Friedman, Thomas L. *The Lexus and the Olive Tree*. New York: Anchor Books, 1999.

Garnett, Gary L. "The Coastal Regime and Marine Security Operations Centres." *Canadian Naval Review*, Vol 1 No 3 (Fall 2005).

Gause, Kenneth, Catherine Lea, Daniel Whiteneck, and Eric Thompson. *U.S. Navy Interoperability with its High-End Allies*. Alexandria: Center for Strategic Studies, 2000.

Gizewski, Peter. "The Future Security Environment: Threats Risks and Responses." *Canadian Institute of International Affairs, International Security Series*, March 2007.

Gow, Iain. *A Canadian Model of Public Administration*. Ottawa: Canada School of Public Service, 2004.

Granatstien, J. L. *Whose War is it? How Canada can Survive in the Post-9/11 World*. Toronto: Harper Collins Publisher Ltd, 2007.

Grubbs, Joseph W. "Can Agencies Work Together? Collaboration in Public and Nonprofit Organizations." *Public Administration Review* 60, no. 3 (May/June 2000).

Halligan, John and Jill Adams. "Security, Capacity and Post-Market Reforms: Public Management Change in 2003." *Australian Journal of Public Administration*, 63, 1, (March 2004).

Harold, Kristin. "Star Top Shuffle Spotlights DND's need for new Home." (28 September 2005); http://www.ottawabusinessjournal.com/284348484419516.php; Internet; accessed 10 March 2008.

Held, David, Anthony McGrew, David Goldblatt, and Jonathan Perraton. *Global Transformations – Politics, Economics and Culture*. Stanford: Stanford University Press, 1999.

Humpage, Louise. "Experimenting with a 'Whole of Government' Approach: Indigenous Capacity Building in New Zealand and Australia." *Policy Studies*, 26, 1, (2005).

Interdepartmental Marine Security Working Group. "Enhancing the Security of Canada's Marine Transportation System – Canada's Marine Transportation System." Jan. 12, 2004; available from http://www.navy.forces.gc.ca/cms_strat/strat-issues_e.asp?id=301; Internet; accessed 25 March 2008.

Krawchuk, Fred T. "Combating Terrorism: A Joint Interagency Approach." *Institute of Land Warfare*, No 05-1 (January 2005).

Kuban, R. *The Emergency Site Management (ESM) System: A Doctrine Paper*. Ottawa: Emergency Preparedness Canada, 1998; available from http://www.pegasusemc.com/pdf/esmdoct.pdf; Internet; accessed 3 April 2008.

Kuban, R. H. MacKenzie-Carey, and A. P. Gagnon. *Disaster Response Systems in Canada*. London: Institute for Catastrophic Loss Reduction, 2001; available from http://www.iclr.org/pdf/research%20paper%2016%20-%20paper%204%20ron%20kuban.pdf; Internet; accessed 3 April 2008.

Johnson, Bev. *Strategies for Successful Joined Up Government Initiatives*. Perth: John Curtin Institute of Public Policy, 2005.

Lannan, Major Tim. "Interagency Coordination within the National Security Community: Improving the Response to Terrorism." *Canadian Military Journal*. (Autumn 2004).

Lawlor, Maryann. "Leaders Talk Tough About Interoperability." *Signal*, 62, no. 5, (January 2008).

Leslie, Major General Andy. "Boots on the Ground: Thoughts on the Future of the Canadian Forces, The 2004 Haycock Lecture." *Canadian Military Journal*. Volume 6, number 4, (Spring 2005).

MacLeod, Ian. "The State of Emergency." *Ottawa Citizen*, 12 April 2008; available from http://www.canada.com/ottawacitizen/news/story.html?id=3dd3d47a-24a8-4b03-86d8-9c31b1d1f849&k=88593; Internet; accessed 12 April 2008.

Maloney, Sean M. "Domestic Operations: The Canadian Approach." *Parameters* 27, no. 3 (Autumn, 1997): 135

Manchester, Eric W. "Creation of Marine Security Operations Centres Leads to More Unified Response." *Canadian Sailings,* (14 August 2006).

McDonough, Frank. *Climbing Up the Ladder to a Whole of Government Status*. International Council for Internet Technology, 2006; available from http://www.ica-it.org/docs/Whole_of_Government_Status.pdf; Internet; accessed 3 April 2008.

Middlemiss, Danforth. testimony from "Canada's Coastlines: The Longest Under-Defended Borders in the World." in *The Report of the Standing Committee on National Security and Defence*. 37th Parliament, 2nd Session, Vol. 1, October 2003.

Middlemiss, Danford W. and Denis Stairs. "The Canadian Forces and the Doctrine of Interoperability: The Issues." *Policy Matters*, Vol 3 no 7, (June 2002).

Miller, Paul. "Interoperability. What Is It And Why Should I Want It?" *Ariadne* 24, (June 2000); available from http://www.ariadne.ac.uk/issue24/interoperability/; Internet; accessed 29 February 2008.

NATO. *AdatP-34. NATO C3 Technical Architecture Manual*. available from http://194.7.80.153/website/home_volumes.asp?menuid=15; Internet; accessed 10 March 08.

———. "Alliance offers partnership to Bosnia and Herzegovina, Montenegro and Serbia." http://www.nato.int/docu/update/2006/11-november/e1129e.htm; Internet; accessed 16 April 2008.

———. *Backgrounder – Interoperability for Joint Operations*. Brussels: NATO Public Diplomacy Division, 2006; available from

http://www.nato.int/docu/interoperability/html_en/interoperability01.html; Internet; Accessed 3 April 2008.

———. *NATO Glossary of Terms.* Brussels, Belgium: NATO Standardization Agency.

———. *NATO Handbook.* Brussels, Belgium: NATO Office of Information and Press, 2001.

———. "NATO's Cooperation with Partners." http://www.nato.int/issues/partnership_evolution/index.html; Internet; accessed 16 April 2008.

NAV Canada. "Newsroom Backgrounder - Air Traffic Services." http://www.navcanada.ca/NavCanada.asp?Language=EN&Content=ContentDefinitionFiles%5CNewsroom%5CBackgrounders%5Cairtrafficservices.xml; Internet; accessed 3 April 2008.

O'Connor, Dennis R. *A New Review Mechanism for the RCMP's National Security Activities – Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*. Ottawa: Public Works and Government Services Canada, 2006.

Organization for Economic Co-operation and Development. "Public Sector Modernisation: The Way Forward." *OECD Observer*, (November 2005); available from http://www.oecd.org/dataoecd/40/33/35654629.pdf; Internet; accessed 3 April 2008.

Paparone, COL Christopher R. and James A Crupi. "United We Stand, Divided …? Achieving Intelligence Interagency Synergy in Complex Warfare." *American Intelligence Journal*, (Summer 2006).

Peters, Cdr Steve and LCdr James Salt. "Maritime Security and Coastal Defence – Challenges in the 21st Century." *Soundings*, (May 2006).

Peterson, Molly M. "Homeland Defense Commander Stresses 'Need to Share' Information." *National Journal's Technology Daily*, (December 3, 2002). 1.

Pollitt, Christopher. Joined-up Government: A Survey. *Political Studies Review*, Vol 1, (2003).

Ravensbergen, Jan. "Senator slams security spending." *Ottawa Citizen*, 18 April 2008; available from http://www.canada.com/ottawacitizen/news/story.html?id=b0a94213-289f-4790-8990-505b66cd7ce9; Internet; accessed 18 April 2008.

Richards, David and Dennis Kavanagh. *Can Joined-Up Government be a Reality? A Case Study of the British Labour Government 1997-2000.* Liverpool: University of Liverpool, 2000.

Richards, David and Martin Smith. "The Tension of Political Control and Administrative Autonomy: From NPM to a Reconstituted Westminster Model." in Autonomy and Control: Coping With Agencies in A Modern State, edited Tom Christensen and Per Lægreid, Cheltenham: UK: Edgar Eldar.

SAFECOM. *2006 National Interoperability Baseline Survey*. December 2006; available from http://www.safecomprogram.gov/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf; Internet; accessed 29 February 2008.

Segal, Hugh D. "National Security, The Public Interest and How We Govern: A Time For Innovation." *Canadian Military Journal*. Volume 2, number 2, Summer 2001. 1-4. Available from http://www.journal.forces.gc.ca/engraph/vol2/no2/pdf/39-42_e.pdf; Internet: accessed 3 April 2008.

United Kingdom. Cabinet Office. *Transformational Government Enabled by Technology*. London: Stationary Office, 2005.

———. *The Global Conflict Prevention Pool: A Joint UK Government Approach to Reducing Conflict*. London: Foreign and Commonwealth Office, 2003.

———. Ministry of Defence. *The Comprehensive Approach*. Joint Discussion Note 4/05, January 2006; available from http://www.mod.uk/NR/rdonlyres/BEE7F0A4-C1DA-45F8-9FDC-7FBD25750EE3/0/dcdc21_jdn4_05.pdf; Internet; accessed 26 March 2008.

———. Prime Minister and Minister for the Cabinet Office. *Modernising Government*. London: Stationary Office, 1999; available from http://www.archive.official-documents.co.uk/document/cm43/4310/4310.htm; Internet; accessed 26 February 2008.

United States. Department of Homeland Security. *The Federal Response to Hurrican Katrina Lessons Learned*. Washington: Government of the United States, 2006.

———. Joint Chiefs of Staff. *Joint Publication 3-16: Joint Doctrine for Multinational Operations*. Washington, D.C.: U.S. Government Printing Office, February 1999.

_____. US Joint Forces Command. "Joint Interagency Coordination Group (JIACG)." http://www.jfcom.mil/about/fact_jiacg.htm; Internet; accessed 5 April 2006.

———. The Joint Warfighting Center. "Doctrinal Implications of the Joint Interagency Coordination Group (JIACG)." *Joint Doctrine Series*, Pamphlet 6, 27 June 2004.

———. The National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Washington, D.C.: Government Printing Office, 2004.

———. National Research Council. *Realizing the Potential of C4I: Fundamental Challenges*. Washington, DC: National Academy Press, 1999.

———. Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. *A Failure of Initiative – Final Report.* Washington D.C.: Government Printing Office, 2006.

———. Senate Committee on Homeland Security and Governmental Affairs. *Hurricane Katrina: A Nation Still Unprepared*. Washington, D.C.: United States Senate, 2006.

———. US Coast Guard. National Plan to Achieve Maritime Domain Awareness for the National Maritime Security Strategy. October 2005,1-33; available from http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf; Internet Accessed 20 March 2007.

———. The White House. *National Security Presidential Directive 1*. February 2001; available from http://www.fas.org/irp/offdocs/nspd/nspd-1.htm; Internet; accessed 29 February 2008.

———. The White House. *The National Strategy of the United States of America.* Washington, D.C.: U.S. Government Printing Office, September 2002.

University of Oxford. *Information and Communications Technology Strategic Plan*. March 2007; available from http://www.ict.ox.ac.uk/strategy/plan/ICT_Strategic_Plan_March2007.pdf; Internet; accessed 29 February 2008.

van der Veen, Hans and Anthony Wiles. *Achieving Technical Interoperability – The ETSI Approach*. Cedex, France: European Telecommunications Standard Institute, 2006.

Van Gramberg, Bernadine. Julian Teicher, and Juan Rusailh. *Reinventing Government in Australia: Whole of Government in a Federation.* Melbourne: Victoria University, 2005.

Waldon, Jeff. "Interagency Cooperation in Information Management." Virginia Technical University: Conservation Management Institute; available from http://fwie.fw.vt.edu/WWW/datashar.htm; Internet; accessed 29 February 2008.

White, Captain Vance. "The Strategic Command Construct." *The Maple Leaf*, Vol 8: No 38, (2 November 2005); available from http://www.forces.gc.ca/site/community/mapleleaf/article_e.asp?id=2024; Internet; Accessed 24 March 2008.