National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# INFORMATION SHARING IN THE MARINE SECURITY OPERATIONS CENTRES: TENSION BETWEEN EFFECTIVENESS AND CONTROL

Major Norman A. Sproll

**JCSP 37**

**Master of Defence Studies**

**Disclaimer**

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

**PCEMI 37**

**Maîtrise en études de la défense**

**Avertissement**

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

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 37 - PCEMI 37

MASTER OF DEFENCE STUDIES - MAÎTRISE EN ÉTUDES DE LA DÉFENSE

# INFORMATION SHARING IN THE MARINE SECURITY OPERATIONS CENTRES: TENSION BETWEEN EFFECTIVENESS AND CONTROL

By Maj Norman A. Sproll

29 April 2011



Word Count: 19 206



Compte de mots : 19 206

**TABLE OF CONTENTS**

## ABSTRACT

In 2004, the Government of Canada published its national security policy which included the creation of two Canadian Forces (CF) led Marine Security Operations Centres (MSOCs), on the Atlantic and Pacific coasts, to network all the government agencies involved in maritime security into a single framework to respond to national security threats thereby enhancing the security of the marine transportation sector. This study uses the CF risk management process to examine the operations of these MSOCs. The risk assessment process shows that MSOC operations are faced with three main risks. Because the MSOCs rely on network enabled operations in which information must be freely available to all participants to achieve the required enhancements to marine security, there is a high risk of mission failure due to inadequate information exchange by the partner agencies. In any situation where personal information is open to sharing, there is a danger that due to poorly controlled sharing of information, personal information may be wrongfully disclosed and therefore MSOC operations face a high risk of causing harm to individuals who may be the subject of MSOC monitoring. These two high level risks conflict, causing tensions between operational effectiveness and information control. Finally, there is a moderate risk of mission degradation or inappropriate employment of the CF due to misunderstandings regarding the role of the MSOC. Changes to the role, governance, procedures and/or structure of the MSOCs can be made to mitigate these risks. This examination shows that the optimum configuration for the MSOCs is to view them as independent systems directed by a board of governors drawn from senior, regional leaders from each of the core partner agencies and designated as investigative bodies. These systems will require thorough and effective information control regimes that should include an independent review mechanism. The systems approach to structuring the MSOCs will maximise the effectiveness and thereby fully realise the goals for which they were created while protecting the safety and liberty of Canadians.

# CHAPTER 1 – INTRODUCTION

## The Inception of the Marine Security Operations Centres

The events of 9/11 caused many countries of the Western world to re-evaluate their security posture and counterterrorism approaches. More specifically, in the months immediately following the 9/11 attack Canada endeavoured to absorb the lessons observed by the United States' National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) and ensure that the nation was not vulnerable to similar attacks and could assist allied countries, and in particular our neighbour to the South, in defending against comparable threats. Amongst numerous observations and lessons, the 9/11 Commission identified a requirement to integrate intelligence collection and analysis and enhance information sharing to ensure that there were no governmental seams that terrorists could exploit. The Commission also noted that there needed to be greater integration between intelligence and operational elements so that governments could respond effectively to terrorist threats.[1] In addition to these lessons, the Government of Canada determined that there was a need, amongst many others, to enhance the security of the transportation sector.[2] The government's efforts to close gaps in Canada's security culminated in the publication of the National Security Policy (NSP) in 2004.

A major component of the NSP intended to enhance transportation security in the marine environment was the creation of "networked marine security operations centres"[3] (MSOCs) under the direction of the Canadian Forces (CF). The NSP foresaw that the Royal Canadian Mounted Police (RCMP), the Customs and Border Services Agency (CBSA), Transport Canada, and the

---

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton And Company, 2004), 401 to 410.

[2] Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Government of Canada, 2004), 11, 35 to 39

[3] *Ibid.*, ix.

Canadian Coast Guard (CCG) would be the core partners in the MSOCs. The NSP directed that the MSOCs would "have the authority and capacity, through interagency staffing, to bring to bear all civilian and military resources necessary to detect, assess, and respond to a marine security threat."[4] The following year saw the establishment of two MSOCs, on the Atlantic and Pacific coasts, established with an interim operational capability.[5]

Since 9/11 and the reforms that it inspired, there has been an increased tension between the requirements of national security and individual rights to privacy and the openness and transparency of government.[6] In the last decade, there have been a number of controversies related to the government's collection and employment of information. One of the most significant was the case of Maher Arar which led to the convening of the Commission of Inquiry into the Actions of Canadian Officials related to Maher Arar led by Justice Dennis O'Connor (the O'Connor Commission) and which in the end resulted in strong criticisms of some of Canada's national security agencies.[7] This backlash against enhanced security measures has impacted on the MSOCs. Within the government there has been considerable debate as to the structure, governance, and information sharing capabilities of the MSOCs and how these issues relate to the legislative and regulatory controls on how the government collects, handles, stores and employs information.[8] Some of the core partners remain unsure whether they can fully participate in the

---

[4] *Ibid.,* 38.

[5] Privy Council Office, *Securing an Open Society: One Year Later - Progress Report on the Implementation of Canada's National Security Policy* (Ottawa: Government of Canada, 2005), 34 to 35.

[6] Jeffery Roy, "Security, Sovereignty, and Continental Interoperability: Canada's Elusive Balance," *Social Science Computer Review* 23, no. 4 (Winter 2005), 463.

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

[8] LCdr Paul Gravel, *The Canadian Forces and Inter-Departmental Cooperation Toward Domestic Security: Tear Down those Walls!* (Toronto: Canadian Forces College Joint Command and Staff Programme New Horizons Paper, 2009), 15.

MSOCs under their existing mandates.[9] This debate is increasingly impacting the operations of the MSOCs and their development toward full operational capability. If carried to its extreme, this debate over the control of information and mission effectiveness of the MSOCs, could have serious implications for maritime security in Canada. The aim of this paper is to examine the tension between the requirement to exchange information to achieve operational effectiveness and the need to control the sharing of information to protect the safety and privacy of individuals subjected to the monitoring activities of the MSOCs. This tension arises from the need to enhance the effectiveness of maritime security operations by fully implementing network enabled operations through the free sharing of information, including personal information, which conflicts with the need to control the collection, retention, handling, and exchange of personal information so as to protect the safety and liberty of individuals who may be the subject of government monitoring. This paper will undertake a risk assessment process to determine the level of risk associated with these activities. This examination will investigate the causes of the issues and discuss controls and/or alternate courses of action that might be implemented to mitigate the risks and achieve as best possible mission effectiveness and control of information. Ultimately, this study will show that the optimum configuration for the MSOCs to achieve mission effectiveness while safeguarding individuals is to view them as two separate systems each directed by a decision making group of senior leaders from the core partners and designated as investigative bodies but with strong and effective information control measures in place including an independent review mechanism.

**Scope**

The NSP directed the establishment of two CF led MSOCs, one on the east coast and one on the west coast. Subsequent to the publication of the NSP, a third MSOC was created under RCMP leadership to cover the Great Lakes and St Lawrence Seaway (GLSLS). This CF College

[9] Fisheries and Oceans Canada, *Canadian Coast Guard: Maritime Security Framework* (Ottawa: Maritime Security, Canadian Coast Guard, Fisheries and Oceans Canada, 2010), 3 to 8.

examination deals only with the CF led MSOCs. Due to treaty restrictions and an operating environment in which military resources are not required to detect and respond to most threats, there is substantially less involvement of the CF in the operation of the GLSLS MSOC. As a result, the GLSLS MSOC is much more law enforcement focussed and does not involve the type of CF operations or military authority issues under consideration in this paper. Any reference to an MSOC or the MSOCs collectively in this paper is refer to only the two CF led MSOCs unless the GLSLS MSOC is specifically named.

**Methodology**

Military operations are complex and dynamic undertakings that are fraught with risks that must be mitigated or accepted. MSOC led operations to respond to a national security threat in the maritime environment are particularly complex activities, as will be described more fully later in this paper, and as such are subject to unique and complicated risks. Within the CF there is an established doctrine and process for managing these risks as outlined in the CF joint doctrine manual Risk Management for CF Operations. As this process provides an accepted and practical methodology processing and planning risk management, this examination of risks faced by the MSOCs in their operations will be based on this methodology. This methodology is particularly applicable for this purpose as it is tailored for use in evaluating CF operations and it ensures that key aspect of risk analysis are considered without being dependent on complex calculations based on factors that cannot be adequately quantified. [10]

The CF risk management process assists decision-makers in understanding the risks they face and how these risks may be mitigated. It aids in evaluating course of action options and permits decision-makers to balance risks against mission effectiveness. As legal risks can play a

[10] Department of National Defence, *B-GJ-005-502/FP-000 Risk Management for CF Operations* (Ottawa: Department of National Defence, 2007), i.

major part in domestic operations, including the MSOCs activities, it is important to note that under CF doctrine, risk management does not sanction or justify violating the law.[11]

Risk management involves two separate activities, risk assessment and risk mitigation. In this methodology, the risk is defined as the chance of injury or loss expressed in terms of probability and severity. Probability is a likelihood that a real or potential condition can cause injury or loss or lead to mission degradation. Severity is the expected consequence of a real or potential condition in terms of degree of injury, loss, or other mission impinging factors.[12]

The full CF risk management methodology consists of 14 steps. However many of the later steps of the process deal with making risks decisions and implementing controls and these issues lie outside the scope of this paper. Therefore this analysis will proceed along the first seven steps of the CF risk management process as follows:

- Step 1 – analyze mission;
- Step 2 – list real or potential conditions that can cause injury, loss, or mission degradation;
- Step 3 – list causes;
- Step 4 – assess severity;
- Step 5 – assess probability;
- Step 6 – complete risk assessment;

[11] *Ibid.*, 1-1 to 2-1.

[12] *Ibid.*, 1-2.

- Step 7 – develop possible controls.[13]

In this paper, Chapter 2 will analyse the MSOCs mission and the operational environment simply to identify and list the risk conditions that may cause concern. This chapter will argue that the on-the-water response to a maritime threat to the nation is a complex undertaking requiring a whole-of government approach. This discussion will note that the whole-of-government approach requires an exchange of information between government organisations requiring a balancing in the extent to which information is shared or withheld. Ultimately, the nature of the maritime response to a threat gives rise to risk conditions wherein too little information may be shared jeopardising mission effectiveness, conditions in which too much information may be shared in violation of legislation and law, or conditions such that the role of the MSOCs may not be clear creating dangers with respect to CF authorities or gaps between response functions.

Chapter 3 will examine the causes of these risk conditions and identify possible mitigation strategies. This chapter will separately examine the first the need for greater information sharing to achieve mission effectiveness, then the requirement for the regulations to control information sharing to ensure the privacy of individuals, and finally possible misunderstandings with respect to the role of the MSOCs. This analysis will identify the causes of the risk conditions to include the need to share more information, including personal information, to implement network enabled operations with a view to enhancing operational effectiveness; the need to control and restrict information collection, handling and exchange to protect individuals from the misuse of their personal information or its inadvertent disclosure to those who might use personal information against them; and confusion regarding the role of the MSOCs as it evolved in order to put policy into practise. The analysis will also identify the variables in role, governance, structure and procedures that may be altered to change the existing arrangements. These variables will be

[13] *Ibid*., 3-1 to 3-5.

considered in terms of possible risk mitigation measures that could be implemented to reduce the risks faced in the course of MSOC operations.

Chapter 4 will conclude the risk assessment process. In this chapter, the possible impacts of the identified risk conditions will be evaluated to assess the possible severity of the risk, and evaluate the probability that these conditions might come to fruition. This chapter will determine the level of risk caused by the conditions identified earlier by comparing the severity of the risk to its probability in accordance with the CF risk management procedure. The analysis will identify that the greatest danger in MSOC operations is the high risk of too much information sharing leading to injury to individuals, followed by the high risk of mission failure due to inadequate exchange of information, and the moderate risk of mission degradation or misemployment of CF elements due to confusion regarding the role of the MSOCs. The assessed levels of risk indicate the significance of mitigating each specific risk and establishes a priority scheme by indicating which risks are more threatening.

Finally, in Chapter 5 this examination will discuss possible changes that could be implemented to mitigate the risks identified earlier. Possible measures to mitigate these risks will be discussed in terms of possible changes to the role to include law enforcement tasks, changes to governance to permit a freer sharing of information, changes to procedures to better control the exchange of information and changes to structure of the MSOCs to close gaps between the intelligence and operations functions within maritime security operations. In conclusion, this analysis will recommend a set of changes to governance and structure that will optimise mission effectiveness without endangering the privacy of individuals.

## CHAPTER 2 – THE MSOC MISSION AND POTENTIAL RISK CONDITIONS

### Step 1 – Analysing the Mission

The Government of Canada's aim in establishing the MSOCs was to enhance transportation security in the maritime realm. To understand how the MSOCs might achieve this enhancement and the role information sharing plays in this respect, it is necessary to understand the threat environment, the government's approach to responding to national security threats and the part that the MSOCs play in this effort. In responding to a maritime national security threat the CF operate within the overall government policy and procedure framework which Public Safety Canada has entitled Canada's Counterterrorism Arrangements[14] and must comply with the legislative direction that frame these arrangements. Prior to 9/11, there was no coherent federal government policy on homeland security and the government approach was extremely fragmented.[15] The publication of the NSP in 2004 made progress in developing an overall policy, but responsibilities, authorities, and competencies remain fragmented and dispersed through several departments.

In Canada, responses to terror threats are governed by several key principles including:

- Terrorist incidents are criminal offenses;
- The rule of law will be maintained;
- Every effort will be made to seek a peaceful resolution to a terrorist incident.[16]

The lead minister for dealing with a terrorist incident is a Minister of Public Safety and under the Security Offenses Act, the RCMP is charged as the lead agency for responding to terrorist

---

[14] Public Safety Canada, *An Overview of Canada's Counter-Terrorism Arrangements* (Ottawa: Government of Canada, 2003), 63.

[15] Colonel J. J. Selbie, "Homeland Security: A Canadian Perspective" (Carlisle Barrack: U.S. Army War College, 2001), 19.

[16] Public Safety Canada, *An Overview of Canada's Counter-Terrorism Arrangements*, 1-1.

incidents.[17] However, depending on the nature of the threat or incident, particularly if the threat includes an element of nuclear, biological, chemical, radioactive, or explosive weapons, these leads may need to involve as many as 14 other government departments or agencies not to mention numerous provincial and municipal authorities. The federal organisations involved include regulatory agencies such as Transport Canada, or the Canadian Coast Guard who enforce Canadian laws and regulations and may prosecute violators but are not authorised to use force; law enforcement agencies, primarily the RCMP and CBSA, who enforce our laws and regulations, may prosecute violators, and are authorised to use force if necessary; and the CF, Canada's defence and security organisation, which is authorised to use military force to thwart a threat but is not normally involved in enforcement and prosecution.[18]

Consequence management is defined as measures to mitigate the damage, loss, hardship, and suffering caused by acts of terrorism. In Canada, consequence management is the responsibility of provincial or municipal authorities. It is likely however, that federal organizations will be called upon to assist provincial and territorial authorities with consequence management.[19]

Within the Canadian counterterrorism arrangements, the CF is a resource of last resort to resolve the issue with military force. The employment of the CF in this respect is guided by the CF Armed Assistance Directions[20], National Counter-Terrorism Plan[21] and Section 273.6 of the National Defence Act (NDA) which spells out the rules regarding CF assistance to law enforcement agencies. These directions specifically state that CF armed assistance will only be

---

[17] Parliament of Canada, *Security Offences Act. 1984, c. 21, s. 56. Consolidated* (Ottawa: Department of Justice, 2011), 2.

[18] Public Safety Canada, *An Overview of Canada's Counter-Terrorism Arrangements*, 3-4 to 3-14.

[19] *Ibid*., ii.

[20] *Ibid*., 5-2.

[21] Department of National Defence, "National Defence and the Canadian Forces - JTF2: National Counter-Terrorism Plan," http://www.jtf2.forces.gc.ca/ct/index-eng.asp (accessed 27 February 2011).

engaged when it is determined that an incident is beyond the means of the RCMP to deal with. Other than armed assistance, the CF may also be employed in a supporting role to provide technical advice; chemical, biological, nuclear, or radioactive (CBRN) response; or assist in consequence management.[22] In all cases, the police response to the incident remains under police management and the CF activities are limited to those areas of their specialized authorities and competencies.

While the Canada's Counterterrorism Arrangements and NSP direction does not discriminate specifically by the environment in which a terrorist incident is occurring, in practical operational terms, it is useful to consider the distinction in responses in the land, air, and maritime environments. There are both similarities and differences in how responses to terrorist incidents in the different environments may evolve and several inferences can be made by observing these differences. Further, the differences will highlight how Canada's Counterterrorism Arrangements must be tailored to meet the requirements of each specific environment and in the case of the MSOCs, especially the maritime environment.

The land of domain is the environment in which Canadian law enforcement agencies are most effective. In the context of national security threats, land environment responses include those dealing with aircraft that have yet to take off and those that have been forced to land. Law enforcement agencies have proven to be fully capable of managing a wide range of problems in the land environment without external support. Additionally in the land environment, law enforcement agencies at various levels of government are ubiquitous and provide presence and surveillance over most of the populated regions of the country where the risk of security incidents are greatest. Law enforcement agencies are able to effectively respond to most land-based threats with little or no support from the CF. This allows the CF to remain largely in a supporting role

[22] Public Safety Canada, *An Overview of Canada's Counter-Terrorism Arrangements*, 3-8.

only taking an active, leading role, in the most extreme circumstances. However, it should be noted that dealing with national scale threats in the land environment remains a complex issue involving numerous federal and provincial/territorial organisations. To deal with this complexity and ensure the passage of information, the RCMP, as the lead agency for responding to national security threats, has created five Integrated Security Enforcement Teams (INSETs) in the largest Canadian population centres to network and integrate the efforts of the numerous agencies involved including municipal and provincial police forces, provincial counterterrorism organisations, and other federal intelligence, regulatory and law enforcement agencies.[23] Under RCMP leadership, the INSETs employ investigators from local law enforcement agencies and analysts from other agencies to conduct national security investigations and respond to specific threats. These INSETs have been effective in the sharing of information related to security threats and as a venue for coordinating the activities of the numerous organisations that may have a role in responding to a threat or incident. For example, the O-INSET based in Toronto alone in 2003 worked on more than 1100 files, and a dozen projects; and responded to nine minor crises such as a specific threat to an El Al flight arriving in Toronto.[24] O-INSET was also central to coordinating the investigation and successfully concluding the arrest of the "Toronto 18" who were plotting terrorist attacks in Ontario. It is in this land environment that Canada's Counterterrorism Arrangements have evolved to deal with security threats most effectively; however, as will be discussed below, challenges remain in dealing with other environments.

Dealing with a national security threat in the air environment, that is a threat related to an airborne aircraft, presents several challenges that are not an issue in the land environment. In the

---

[23] Royal Canadian Mounted Police, "Royal Canadian Mounted Police Website: Integrated National Security Enforcement Teams," http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm (accessed 16 January 2011).

[24] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 102 to 107.

first instance, surveillance of North American airspace is less complicated than surveillance in the land environment in that it involves fewer organisations and these organisations have an established network to exchange information and share situation awareness. Monitoring and controlling the air space over North America is conducted by two national civil aviation authorities and the North American Air Defense Command (NORAD).[25] NORAD has established close ties and interlinked networks with the civil authorities who will be the first to identify possible threats and through them monitors routine events, but does not take an active role in day-to-day regulatory activities. The most pressing challenge in responding to an air based threat is the limited means and methods available to resolve the threat. Law enforcement and regulatory agencies have no integral means of engaging a threat aircraft in the air. Unlike land threats, if an airborne threat is identified by civil authorities, they have no choice but to call upon NORAD to respond due to a complete lack of civilian means to respond. Once called, NORAD command and control structures initiate action to further identify the threat, and verify hostile intent, and in doing so work as information fusion and coordination centres in their own right. They are intricately connected with law enforcement in civil air authorities through the exchange of liaison officers and/or virtual connections and rapidly exchanged all available information with these agencies to develop the necessary air domain awareness to respond to the threat.[26] If, based on the air domain awareness available, the threat aircraft is determined to have hostile intent; NORAD takes action to resolve the threat. Again, the problem of limited methods to resolve the threat manifests itself. Ideally, NORAD will endeavour to communicate with the hostile aircraft and use the threat of military force to compel the aircraft to land. If this is not successful,

---

[25] Adam J. Hebert, "Noble Eagle without End," *Air Force Magazine,* February 2005, 44 to 47, http://www.norad.mil/News/2007/061907.html (accessed 06 February 2011).

[26] Otto Kreisher, "The Years of Noble Eagle," *Air Force Magazine,* 19 June 2007, 51 to 52, http://www.norad.mil/News/2007/061907.html (accessed 06 February 2011).

NORAD instructs its military resources to use military force to neutralise the threat.[27] Once a threat is neutralised, the situation is returned to the control of civil authorities to lead the clean-up and/or resolve any law enforcement issues. NORAD or other military resources may be involved in the final resolution of the action but only in a supportive role under civil direction.

Responding to national security threats in the maritime environment incorporates many of the worst aspects of the other two environments. Like the land environment, in the maritime environment there is a complex arrangement of responsibilities, authorities, and competencies between the various involved agencies. In 2006, in the renewal of the NORAD agreement between the United States and Canada, NORAD was given an added task of providing maritime warning for the continent. In a reviewing NORAD's progress on undertaking this responsibility, its commander noted the extreme complexity of arrangements for maritime warning and response. In particular, the commander observed the complexity of the task because the security threats are closely related to criminal threats. Further, he noted the plethora of players in the maritime domain and the fact that few are military organisations creating a significant challenge in creating a network to develop the necessary levels of information exchange. Finally, the commander remarked that warning is not sufficient, but that action must follow and that there remains a divide between the warning function and the operational response.[28] Therefore, like the land environment, there is a requirement for extensive integration and coordination between the organisations involved.

Like the air environment, in the marine environment civil authorities have limited capability to detect and respond to events on the water, particularly given the vast ocean area and coastline

---

[27] Hebert, *Noble Eagle without End*, 46 to 47.

[28] General Victor Renuart, *Remarks by General Victor Renuart Commander of NORAD and NORTHCOM to the Heritage Foundation* (Colorado Springs: United States Northern Command, 2008), 3 to 4.

that requires monitoring. This results in a situation where no one organization can complete its mission on its own and all the agencies in the maritime domain must work together to resolve any incident, regardless of whether it represents a law enforcement issue or national security threat.[29] Few law enforcement agencies have the capability to work on the water and what capabilities do exist are very limited, usually restricted to the lake and river operations. The Canadian Coast Guard has extensive capabilities to operate on the ocean, but their mandate is limited to safety and regulatory activities. Even surveillance of Canada's three oceans is limited by the resources available within the Coast Guard, the Department of Transport, Environment Canada, and the CF. To effectively monitor Canada's waters and conduct any type of law enforcement or national security response requires all the agencies of the government to work together and regularly involves employment of the CF and civil resources to complete these operations. To work together to monitor Canada's oceans and coast, the national security partners need to freely share information derived from their separate collection efforts so that multiple assets do not need to collect on the same areas.[30]

Like the land environment, in the sea environment there a more options for resolving a threat with minimum use of force and minimum collateral damage. However, unlike the land environment where the necessary capabilities are largely available within law enforcement agencies, in the maritime environment the required capabilities are embedded with several organisations including several important capabilities that are only available within the CF and the Department of National Defence (DND). The CF and DND must provide:

- Long range, high endurance air patrols;

---

[29] Privy Council Office, *Securing an Open Society: One Year Later - Progress Report on the Implementation of Canada's National Security Policy*, 35.

[30] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)* (Ottawa: Government of Canada, 2007), 5 to 6.

- Long range seaborne search capabilities;
- Monitoring of potential threat electronic emissions;
- Mobile command and control capable of leading complex responses on the water;
- High speed manoeuvre on the seas;
- CBRN reconnaissance and response;
- The authority to board threat vessels outside of Canada's territorial waters;
- Special forces capability to board an aggressively defended ship; and
- In the extreme case, the ability to disable or sink a threat vessel.

This leads to a circumstance where a response to a national security threat must be truly a whole-of-government operation in which the CF will play a very prominent role. The lack of capabilities within law enforcement agencies and the availability of the required capabilities within the CF led to the NSP assigning lead for on-the-water response to national security threats to the CF, despite other legislation and direction giving the RCMP the lead role in other areas.

The necessary whole-of-government nature of responses to national security threats in the maritime environment adds complexity to the problem which will be exacerbated as leadership of operations to resolve the threat will likely evolve over time. Initial monitoring and surveillance may be a law enforcement or regulatory agency led activity. As the operation develops, leadership may shift as the nature of the threat is clarified; regulatory agencies will lead where a safety, environmental or medical threat is identified; law enforcement agencies will lead if the threat is criminal in nature; and if an on-the-water response is required, the lead role will shift to the CF in keeping with the NSP. Once a situation is resolved, leadership will need to shift again during close-out of the operation so that law enforcement and regulatory agencies can gather the

materials necessary for prosecution of security offences and provincial authorities can execute consequence management if necessary. The need to shift leadership during operations to respond to national security threats requires a high degree of interagency integration and cooperation to ensure that the operations flow seamlessly and that all threats are accounted for and defeated. To effectively engage all the government departments and ensure the smooth conduct of operations so that the involved agencies have the capacity to fill their roles in a timely and useful manner, especially the leadership role as it transitions from one agency to another, requires that information must be shared openly and quickly. Failure to share information could jeopardise threat detection and effective response. These are the same lessons identified by the 9/11 Commission in reviewing the circumstances surrounding the attack on New York as discussed previously. This is the first risk condition that is evident in this analysis.

While the need for all the government organisations involved in detecting and responding to maritime security threats to share information is evident from the nature of the response arrangements described above, there is a danger that information may be shared to freely. Canada is an open and democratic society that values the ability of individuals to conduct there lives without being monitored or interfered with by the government. Since 9/11, there have been four cases where overly free sharing of information by government agencies aimed at improving threat detection and response resulted in the rendition of individuals and their subsequent interrogation.[31] Canada's laws and regulations are aimed at preventing such violations of an individual's rights to privacy and liberty. While these laws and regulations may be seen as an impediment to the free sharing of information needed to respond to security threats they are important to protect individuals. Thus the need to freely share of information to best deal with a

[31] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Reporting the Events Relating to Maher Arar: Analysis and Recommendations*, 267.

national security threat gives rise to a second risk condition, the threat of too openly sharing information.

The MSOCs play and important part in managing the complexity of the CF role in responding to national security threats in the maritime environment and enhancing the effectiveness of government responses. In the first instance, the MSOCs helped to coordinate the efforts to detect and monitor possible threats, especially CF involvement in this effort. By early involvement in any government response, the MSOCs help the CF prepare and execute its leadership of any on-the-water response to these threats as mandated in the NSP. Finally, because they are structured as interagency teams aimed at providing all the involved agencies with a common understanding of the threat and response requirements, they are well-suited to assist other government departments in executing their own operations.[32] In developing the methods and procedures for supporting an on-the-water response as a whole-of-government effort, the MSOCs have also become adept at assisting in the coordination of other CF support to law enforcement and humanitarian relief operations even though this is not their primary mandate. Due to the close relationship between national security threats and criminal activities as identified by the O'Connor Commission,[33] often the MSOCs find themselves dealing extensively with criminal threats as well as national security threats. Further, because the MSOCs are the primary facility available for interagency information sharing, law enforcement and regulatory agencies often use the MSOCs to discuss and share information regarding their own particular interests. The close relationship between criminal and national security threats, the use of the MSOCs for law enforcement and regulatory agency information exchange and the employment of the MSOCs to assist CF support to law enforcement and humanitarian aid tasks all give rise to a potential

---

[32] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*, 1 to 2.

[33] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 570 to 572.

confusion with respect to the mandate and role of the MSOCs. These circumstances set the conditions wherein the MSOCs can be misused to support or coordinate tasks for which they lack adequate authority. This creates a third risk condition needs to be prevented or mitigated. [34]

**Step 2 - Potential Conditions That Can Cause Injury, Loss, or Mission Degradation**

In reviewing and summarizing the analysis of the MSOC mission as described above, it becomes evident that there are three main risk conditions that can cause injury, loss, or mission degradation. These real or potential conditions are:

- There is a possibility that the sharing of information is impeded to such extent as to jeopardise the mission;
- There is a possibility that information is too extensively shared, inadvertently disclosed, or otherwise handled in contravention of law and regulation so as to endanger the privacy and freedom of individuals.
- Because law enforcement and regulatory agencies do not have a separate integration and coordination facility to manage their own mandated responsibilities, the MSOCs are often engaged as a law enforcement and regulatory coordination and information fusion function. This is beyond the NSP mandate for the MSOCs and requires additional authorisations;

Within these three broad risk conditions, there are several specific factors which could impact on the actual probability and severity of the associated risk. The specific factors, their influences and causes are the subject of the next step in the risk assessment process.

---

[34] LCdr James Salt, *The Whole-of-Government Approach to Maritime Information Sharing: Reality Or Fiction?* (Toronto: Canadian Forces College Joint Command and Staff Programme New Horizons Paper, 2008), 11 to 12.

# CHAPTER 3 – ANALYSIS OF THE CAUSES OF THE RISK CONDITIONS

## Step 3 – The Causes of Risk Conditions

The next step in the CF risk management process is to analyse the causes of the risk conditions identified. In this chapter, the need for greater information sharing, the danger of excessive information sharing, and potential confusion with respect to role and mandate of the MSOCs will be examined separately. This examination will highlight the specific requirements for information sharing and risks that might arise if these requirements are not met. Further, the analysis will discuss the risks that too much information sharing creates and the laws and regulations that prevent aim to prevent these risks. The evolving role of the MSOCs will also be reviewed to note how law enforcement requirements for information sharing create a situation where the MSOCs are engaged inappropriately in activities outside their mandates. The discussion will also note where there are opportunities to change existing arrangements to better balance mission effectiveness against the control of information while more closely achieving the MSOCs' role as laid out in the NSP.

## The Need for Greater Information Sharing

As stated previously, the MSOCs were created to enhance the government's response to national security threats in the maritime environment by improving information sharing to detect and assess threats; and improve the coordinated response of the multiple Government of Canada agencies involved in maritime security. The CF achieve this effect through the implementation of network enabled operations to enhance the effectiveness and efficiency of on-the-water responses to security threats and achieve the integration of intelligence and operations functions desired to overcome the failings that contributed to the 9/11 crisis. The following analysis demonstrates that network enabled operations achieve their effectiveness by exploiting improved information sharing to achieve information superiority, self synchronisation, and supporting reachback,

reachforward and emergent leadership. If a failure in information sharing impedes achievement of these effects, the situation causes a risk condition wherein mission success is jeopardised.

Network enabled operations is the CF term used to describe operations aimed at achieving operational advantages through the use of networks to link sensors, decision-makers, and operational elements. The Canadian concept is derived from similar Allied concepts such as the United States' network-centric warfare and the United Kingdom's network enabled capabilities.[35] In the Canadian context, network enabled operations has coevolved and least partially absorbed the joint, interagency, multinational, and public (JIMP) framework of conducting operations. Unique to the Canadian concept of network enabled operations is the focus on the human dimensions of these operations by encapsulating the social networks developed by organizations and individuals working in a theatre of operations and the flow of information on these social networks rather than just dedicated command and control systems.[36]

Derived from its origins in U.S. network centric warfare theory, the Canadian network enabled operations concept accepts four basic tenets:

- A robustly networked organization improves information sharing;
- Information sharing and collaboration enhance the quality of information and situational awareness;
- Shared situational awareness enables self synchronization and emergent leadership by the most appropriate individual or organisation;

---

[35] Michael H. Thomson and Barbara D. Adams, *Network Enabled Operations: A Canadian Perspective* (Guelph: Humansystems Incorporated, 2005), 3 to 4.

[36] *Ibid*., 6 to 7.

- Shared situational awareness and self synchronization increases mission effectiveness.[37]

The aim of establishing the MSOCs as interagency teams was to implement network enabled operations in the domestic maritime environment to enhance partner agencies access to each other's information, thereby increasing all the agencies situational awareness and permitting them to synchronize their operations. In short, the MSOCs intend to achieve the benefits available to network enabled operations. Specifically they are trying to achieve the benefits of network enabled operations which include:

- Information superiority which generates the ability of all MSOC partners to obtain and employ the relevant information required to conduct their operations while denying the same to the potential threat;

- Self synchronisation permits partner agencies to synchronise their efforts to be mutually supporting and more efficiently and expeditiously achieve shared goals;[38]

- Force agility which enables partner agencies to respond flexibly with the resources required when they are required making the response force more robust, resilient, responsive, flexible, innovative, and adaptable;[39]

- Reachback enables partners to reach into the full capabilities of their parent organisations and harness all the capabilities required to resolve an issue;[40]

---

[37] *Ibid*., 6.

[38] David S. Alberts and others, *Understanding Information Age Warfare* (Washington: Command and Control Research Program, 2001), 205 to 227.

[39] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command, Control in the Information Age* (Washington: Command and Control Research Program, 2003), 128.

[40] Thomson and Adams, *Network Enabled Operations: A Canadian Perspective*, 11.

- Reachforward permits the parent agencies of MSOC partners to obtain timely situational awareness and enhance their ability to direct and support participating partners;[41]

- Effects-based operations enable MSOC partners to determine desired outcomes of operations and harness a broad range of military and non-military capabilities to achieve those outcomes.[42]

- Emergent leadership allows transition of leadership roles so that the most appropriate leader, either an individual or an organisation, is able to emerge and direct the overall effort.[43]

While the concept of network enabled operations normally envisions physically dispersed operational entities well connected by high capacity communications and advanced information systems, the MSOCs by necessity utilise more traditional means to achieve shared situational awareness. Network enabled operations requires robust and rich information exchange, reach to all participants in an activity, and high quality interaction between the members.[44] Because the core members of the MSOCs do not possess a robust common information systems network, and likely never will due to privacy law concerns and security compartmentalisation of information systems employed by the Government of Canada, the network enabled operations are achieved through the creation of purely human networks of interagency teams at a shared physical facility with connection to individual partner agency information systems. Working physically co-located provides for a high quality interaction and the rich information exchange amongst the members present in the MSOCs which is desirable for effective operations. Because, as foreseen in the

---

[41] *Ibid*.

[42] *Ibid*.

[43] Alberts and Hayes, *Power to the Edge: Command, Control in the Information Age*, 179 to 185.

[44] *Ibid*., 74 to 82.

MSOC concept of operations, interagency members have access to their individual agency networks, they can reach into agency data stores to extract information relevant to their roles and projects.[45] Making all MSOC products available to partner agency networks enables them to be viewed and used by agency partners not located within the MSOCs. The sharing of information between networks means agency members inside and outside the MSOCs can collaborate on topics of mutual interest, MSOC agency representatives can reach and consult subject matter experts within their specific agencies, and leaders in departmental headquarters in Ottawa can obtain a shared situational awareness on their own agency networks. Most significantly, the MSOC members are closely linked to their own agency operations centres or offices so that threats detected and clarified by the MSOCs can be responded to by all the partner agencies and each agency has adequate situational awareness to enable coordinated response. However, the extended information exchange to include more dispersed components of the partner organisations will occur at a slower pace as MSOC members will need to manually exchange information between systems.[46]

As the operational environment has become more complex and threats have broadened to include more than just adversarial military forces, the CF has come to need a more flexible and more holistic response. As noted by the O'Connor Commission, due to globalisation, the availability of ubiquitous secure communications, the overlap between criminal and security threats and the emergence of new threats and techniques, responding to domestic national security threats is now more than ever before a whole-of-government endeavour requiring the efforts of several government departments and agencies to meet and defeat threats and/or manage the

---

[45] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*, 4 to 5.

[46] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*, 4 to 5.

consequences.[47] Network enabled operations have come to be widely seen as the most effective means to exercise the necessary command and control of the complex operations required to respond to national security threats.

The first goal of the MSOCs is to attain information superiority over their potential adversaries. As described in the MSOC concept of operations, the MSOCs are relatively small interagency teams working together on a permanent basis and performing two main operational functions; surveillance planning and task coordination; and intelligence activities and tasks including threat assessment.[48] The creation of small, interagency working teams has the added benefit of optimizing the knowledge worker environment. Experience has shown that knowledge workers are more effective in an environment with minimal structures, minimal supervision, maximum difficulties as challenges, and working within trusted networks to process information into actionable intelligence.[49] The small interagency work teams of the MSOCs provide the optimum conditions for developing an effective trusted network. This method of interaction is important to overcome potential problems in information sharing related to trust amongst MSOC partners.

The MSOCs construct is efficient in its use of information collection resources. As discussed previously, no single government department has the resources necessary to conduct surveillance of Canada's coasts. Coordinating all the departments' resources provides maximum coverage with the limited resources available. The effectiveness of this approach can only be achieved if the separate agencies pool the results of their surveillance into a common database so that each

---

[47] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 116 to 117.

[48] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*, 7 to 9.

[49] Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (Danvers: World Scientific Publishing Co. Pte. Ltd., 2007), 194 to 195.

department can rely on the others to provide the coverage it needs. If information from each contributor is not available to the others, the potential advantages of coordinating information collection are never achieved.

The effectiveness of the MSOCs is also enhanced through the use of interagency expertise in the processing of information. In a more traditional naval usage, network enabled operations "allowed naval units prosecuting a contact to post acoustic and other sources of information for viewing and collaborative assessment by other units."[50] Employed within the MSOC context, network enabled operations ensures that expertise from partner agencies will permit the MSOCs to review the information from different perspectives to be able to situate any new information in the most appropriate context. This is particularly important given that the information being collected and assessed in the modern domestic maritime environment is generally related to civil entities and therefore should be viewed from a civil perspective. Further, the reachback of the network enabled environment will be an important capability in detecting and defining threats. Through sharing information on partner agency networks, MSOC members will be able to engage external participants in reviewing results of collection and consult subject matter experts within their own organisations. Diversity of views is the key to identifying threats.[51] By engaging interagency analysis, the MSOCs are in a better position to achieve information superiority. However, this necessitates robust information exchanges so that all the MSOC members can review the information from their particular perspective. Sharing the information just within the MSOC is not sufficient either. Members must be able to share the information fully within their own departments so that they can involve other investigators and analysts who may be working on related projects and can consult subject matter experts to receive additional input.

---

[50] Allan English, Richard Gimblett and Howard G. Coombs, *Networked Operations and Transformation: Context and Canadian Contributions* (Montreal: McGill-Queen's University Press, 2007), 46.

[51] Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, 192.

In detecting and assessing threats, the failure to share information will, at minimum result, in highly redundant information collection as each area will need to be monitored by each department separately to achieve their separate departmental mandates. At worst, coupled with an overall lack of surveillance resources, failure to share information after collection will result in a possible threat not being detected. Alternative approaches to threat detection and definition are very expensive and inefficient. To achieve the same degree of detection as the MSOCs, each partner agency would need the full range of information collection resources within its own inventory. Further, to establish a similar degree of interagency review of collected information would require the extensive exchange of investigators and analysts between agencies so that each agency was able to review the information it collected from the perspective of its partners. Redundant subject matter experts would have to exist in every department so that each department had access to their expertise separately on their own departmental networks. It is unlikely that Canada could afford to achieve the levels of redundancy necessary to achieve the MSOCs effects without actually sharing information between departments. Of note also, in the process deconflicting interagency information collection and conducting interagency threat assessments, the MSOCs must become involved in the tracking and monitoring not just national security threats, but also law enforcement and regulatory agency subjects of interest. This creates a potential conflict with respect to role that will be discussed in greater depth later.

Since the core partners of the MSOCs represent the primary government agencies capable of responding to a national security threat, the MSOCs become an important venue for supporting the coordination of a response to such a threat. While the NSP designates the CF as a lead for them on-the-water response to a national security threat, DND relies on the cooperation of other government departments to fulfill their part of the responses. An important component of the MSOC function is to provide common situational awareness to the operations staffs of the partner

agencies.[52] The participation of members from all the core agencies and their access to their regional departmental operations staff through individual agency networks provides a means for ensuring that the operational staffs have a common understanding of the situation and are able to direct their own resources to respond. The MSOCs go further in this direction by supporting the operation of interagency decision making groups (DMGs) which enable the regional leaders of the core agencies to gather, receive a complete briefing on the threats identified and defined by the MSOCs, and determine the most appropriate response to a security threat. The DMGs also conduct local coordination of proposed operations.[53] The MSOC concept of operations notes that the DMGs may have to involve higher level authorities on certain occasions to enable the employment of certain resources, but this is not seen as a routine situation and will slow the decision making and operations coordination process. Issues related to the impact of including Ottawa based authorities in the decision making process will be discussed further below. By bringing the core agencies of the MSOCs together in a single DMG, the CF achieves several benefits of network enabled operations, especially through enhancing force agility and the capacity for self synchronization.

The MSOCs and closely associated DMGs provide venues for determining the availability of government assets, voluntary assignment of those assets to complete necessary tasks, and synchronization of the assets and task completion. Self synchronization is an important capability to ensure timely responses to threats. By sharing a common maritime picture and an overall awareness of all the government resources available to meet a problem, the MSOCs and DMGs put individual agencies in a strong position to undertake the initial steps of responses on their own authority. Voluntary tasking and coordination of responses by other government agencies is

---

[52] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*, 4.

[53] *Ibid*., 12.

particularly useful because it enhances timeliness and effectiveness of the response by allowing them to begin the preparations to respond even while the Ottawa based central headquarters of each partner organisation begins to consider the problem. The inclusion of all the partner agencies in a collective decision making process means that the all departmental capabilities are available for consideration as tools to achieve governmental aims and the operation can be tailored to more effectively meet the effect desired by the government. A shared understanding of the situation also permits the partner agencies to undertake any the necessary risk management measures by permitting individual organisations to respond on their own initiative.

The reachforward capabilities of the networked environment additionally reduce the time required for the central headquarters of each agency to comprehend and approve the intentions and efforts of the local authorities. Since situation awareness information can be hosted on partner agency networks, the leadership in Ottawa can develop an understanding of the situation from their own resources and be fully prepared to discuss proposed measures before meeting in Ottawa to make final decisions. There is no requirement for a group briefing to detail the situation and fewer requirements to query local partners about the particulars of the situation.

As discussed previously, the leadership role for responding to maritime threats will evolve as the operation progresses from warning, to response, to resolution. This need to transition leadership of an operation is a form of emergent leadership that is supported through network enabled operations. Through their close relationship with the DMG, the MSOCs are able to provide timely notice of changes in the situation requiring different operational responses. Actual determination of the lead agency will be conducted by the DMG which will also specify the timing and circumstances for the change in leadership and conduct detailed handover coordination. By providing a high degree of situational awareness to individual partner agencies, the MSOCs are able to ensure that complex interactions and transitions in leadership are supported by a common understanding of the situation reducing the time required to handover

control between lead agencies. The ability to transition leadership during an operation will also make the forces involved in the operation more agile and responsive to changes in the situation. Reachforward will ensure that authorities in Ottawa are quickly apprised of the new situation and, if necessary, can more quickly approve changes to the plan.

In 2009 and 2010, the MSOCs successfully played a central role in the resolution of two security and law enforcement concerns. The first involved the movement of illegal migrants to Canada on a ship named the Ocean Lady in 2009, and the second was a similar situation involving a ship named the Sun Sea in 2010.[54] These operations were entitled Operation POSEIDON 1-09[55] and Operation POSEIDON 1-10[56] respectively. In both cases, the initial identification of a potential issue of concern was done by law enforcement agencies. These agencies notified the Pacific MSOC of the potential threat posed by these movements and nominated the ships in question as vessels of interest to the MSOC. The MSOC was successful in engaging the full breadth of interagency collection resources to monitor these ships right from there port of origin all the way into Canadian territorial waters. At the time of each event, the MSOC conducted a full review of the threat posed by these illegal migrant movements and assessed that it was unlikely that either vessel was national security threat. The MSOC provided sufficient, timely situational awareness to engage the DMG which determined that the RCMP and Immigration Canada should be the lead agencies for resolving the issue. In each case, while CF resources tracked and monitored the vessels, an RCMP boarding party embarked on a CF frigate and set out

---

[54] Department of National Defence, "Canada Command: Operations General," Department of National Defence, http://www.canadacom.forces.gc.ca/daily/archive-opgen-eng.asp (accessed 12 April 2011).

[55] Department of National Defence, "Land Forces Knowledge Management System: Op POSEIDON 1-09," Department of National Defence, DND Intranet http://kms.kingston.mil.ca/kms/CentralInstance.aspx?Type=Rotation&Id=586 (accessed 16 April 2011).

[56] Department of National Defence, "Land Forces Knowledge Management System: Op POSEIDON 1-10," Department of National Defence, DND Intranet http://kms.kingston.mil.ca/kms/CentralInstance.aspx?Type=Rotation&Id=587 (accessed 16 April 2011).

to intercept the track of interest. In each case, the frigate intercepted the migrant vessel just inside Canadian territorial waters where the RCMP legal mandate is in effect. Both vessels were boarded without opposition by RCMP teams. In the case of the Sun Sea, a CF prize crew took control of the ship and sailed it to a designated anchorage and provided medical support to the migrants. The CF also provided a patrol craft to follow behind the Sun Sea and rescue any passengers that fell overboard. In the case of the Ocean Lady, the RCMP provided two vessels to play this role.[57]

These examples show how the MSOCs, in partnership with the DMGs, can be effective in supporting interagency operations off of the Canadian coast. The CF led MSOCs initially took the lead in tracking and monitoring the vessels of interest and assessing what threat they posed. Once the situation was clear, the DMGs were involved to develop an interagency plan that achieved the effects desired by the government. Several resources from different agencies were involved in the execution of each operation and there efforts were synchronised without major issue. During the course of events, the lead role was transferred to the RCMP and later to CBSA without a problem. While both operations were successful in achieving the government's aims, the after action review of Operation POSEIDON 1-10 did raise concerns regarding a lack of information sharing by some of the partner agencies as the CF found that they were engaged in the operations planning and coordination process very late. [58]

All the advantages of employing a network enabled operations framework rely on rich information sharing by the partner agencies. One alternative to sharing information within the MSOCs is for the separate partners to try to return to planning and conducting operations

---

[57] Department of National Defence, *Canada Command: Operations General*.

[58] Department of National Defence, "Land Forces Knowledge Management System: 2010-0026-J2 INT Op POSEIDON After Action Review," Department of National Defence, DND Intranet http://kms.kingston.mil.ca/kms/CentralInstance.aspx?Type=Feedback&Id=227 (accessed 16 April 2011).

independently. While this would obviate the necessity of sharing information, it would impede the effectiveness of the operation. Reverting to an independent agency approach to responding to threats would undo the enhancements to transportation security sought within the NSP. If one agency tried to truly go-it-alone, there would be a severe limit on the available response options. If a single agency tried to plan the operation to include capabilities within other agencies, there would likely be a lag in planning as the decision makers engaged their peers in other departments to find out what capabilities were available, and how they could be used. Planning the operation as a group activity within a DMG supported by and MSOC is a more efficient and effective approach to planning response to security threats but it will require substantial information sharing.

The other alternative to sharing information regionally within the MSOCs is to centrally manage the effort by the Ottawa based headquarters of the partner agencies. To centrally direct and coordinate the response will likely reduce the effectiveness of the response as coordination will take more time and participating agencies would likely fulfill a specific direction rather respond proactively to meeting new developments in this situation as they arise. Government departments normally operate independently of one another within the Government of Canada, and interdepartmental activities are normally coordinated at the deputy minister level. To coordinate the response to a national threat centrally from Ottawa would require the departments to move their situational awareness information to Ottawa for consideration by a high level central DMG. This DMG would first have to review the available information and compare each others information holdings to make sense of the situation. Even if this effort was supported by a central information fusion capability, it would take time to move the information to Ottawa and develop a shared situational awareness there. Further, it would not resolve the fundamental issue that at some point the separate organisations have to share their information freely to develop a shared understanding of the situation.

Once the central DMG made its decision with respect to how to respond to a national security threat, then instructions would need to be transmitted to the local responders. So that regional subordinates can understand any instructions received and respond effectively, the shared situational awareness would also need to be transmitted to them. Any perturbation in the execution of the operation would need to be identified to the central DMG for resolution. The result would be a reduction in the timeliness and agility of the response and possible local disconnects as circumstances not foreseen by the central authorities might separate the interaction of local partners. While central decision making by Ottawa authorities could achieve a fair degree of synchronisation; it can not match the regional MSOC/DMG combination in terms of agility and timeliness and some gaps in synchronisation would likely continue.

The MSOCs employ information sharing to implement network enabled operations to achieve the enhancement to transportation security desired by the NSP. Information must be shared as freely as possible to ensure that no threat is able to pass undetected. As outlined above, this creates a risk condition wherein inadequate sharing of information can result in mission failure. CF leadership seeking to derive ever increasing effectiveness from the MSOCs remain very concerned that impediments to information sharing will undermine the capabilities of the MSOCs. Possible failure to share necessary information is specifically identified as a challenge in Contingency Plan POSEIDON to respond to a maritime national security threat.[59] When this contingency plan was actually put into effect to conduct operations in 2009 and 2010, limitations in information sharing were identified as a weakness in the execution of the plan.

Within the CF the community, some leaders are concerned that the MSOCs do not have sufficient information to develop full "maritime domain awareness". In the maritime domain

---

[59] Department of National Defence, "Land Forces Knowledge Management System: JTFP Contingency Plan POSEIDON Information Brief," Department of National Defence, DND Intranet http://kms.kingston.mil.ca/kms/FileView.aspx?Id=3248&UniqueParameter=634387305394488546 (accessed 16 April 2011).

there is a belief that to develop a full appreciation of the potential marine threats, the MSOCs need to obtain and assess what the Privacy Act has deemed personal information.[60] In the view of those focussed on maximizing the effectiveness of MSOCs, the controls on the sharing of information are seen as impediments to achieving full effectiveness creating a tension between mission effectiveness and information control. The Privacy Act and the controls on collecting, storing and handling personal information are often cited as the greatest impediments to maximising the effectiveness of information sharing within the MSOCs.[61] The important role that these controls play in protecting individuals and the risks attendant on excessively sharing information is the subject of the next section.

**The Need to Control the Sharing of Information**

As integration and interoperability have become the guiding principles in the national security realm since 9/11, government misuse of information and the openness of national security operations have been ongoing concerns in the public domain. The government employs legislative instruments amplified by government regulations and procedures to prevent such error and abuse and the harm to individual that can result. The MSOCs define themselves as information fusion centers. As part of the revamped national security regime established in the post-9/11 environment, the MSOCs are required to comply with all of the legal instruments related to information handling to prevent error and abuse which could cause harm to individuals. The manner in which the MSOCs comply with these controls can affect the structure and governance of the MSOCs and their effectiveness in achieving their mandates. In the following discussion, the information control regulations in place in Canada will be analysed to show their

---

[60] Parliament of Canada, *Privacy Act 1980-81-82-83, c. 111, Sch. II "1". Consolidated,* (Ottawa: Department of Justice, 2010), 2.

[61] Salt, *The Whole-of-Government Approach to Maritime Information Sharing: Reality Or Fiction?*, 18 to 20.

impact on information sharing in the MSOCs noting where they limit the sharing of information and achieving further enhancements in operational effectiveness. The analysis will also consider what scope exists to alter the existing concept of operations to enable increased information sharing. Finally, the discussion will consider the harm that may be caused if information is shared too freely.

In general, the Privacy Act[62] provides protection to personal information. Outside these protections it can be understood that government agencies have the authority to collect, process, store, and use information where there is responsibility for an action based on the information. Therefore, since the CF is responsible for on-the-water responses to a national security threat, it has the authority to collect, process, store, and use information related to that threat. The existing MSOCs concept of operations provides guidance and direction on these matters. Currently, the MSOCs do not have any standing responsibility to support law enforcement activities. As such, the MSOCs have no standing authority to handle information related to law enforcement although such authorities may exist during the finite periods where the MSOCs are acting in a support to law enforcement role under Section 273.6 of the NDA.[63] The information that the MSOCs may use is proscribed by their role.

Under their current concept of operations, the MSOCs collect information and monitor vessels to assess the threat posed by a vessel of interest. Normally, the specific threat posed by a vessel of interest will initially be unclear. Once sufficient information is obtained, the MSOCs evaluate whether the vessel of interest is a national security concern or law enforcement concern. If it is a national security concern, it is fully within the mandate of the MSOCs to continue to track and monitor the vessel. If it is determined that the vessel is a law enforcement concern, the

---

[62] Parliament of Canada, *Privacy Act 1980-81-82-83, c. 111, Sch. II "1". Consolidated*

[63] Parliament of Canada, *National Defence Act. R.S., c. N-4, s. 1. Consolidated* (Ottawa: Department of Justice, 2011), 212 to 217

authorities laid out in Section 273.6 of the NDA should be engaged to enable the MSOCs to continue to track and monitor the vessel. This is of particular concern if CF resources are employed to collect the information which the MSOCs employ to maintain their tracking and further define the threat. In the examples of the responses to the approach of the Ocean Lady and Sun Sea discussed above, the authorities to act in support of law enforcement were engaged in accordance with Section 273.6 of the NDA. Whether monitoring national security threats within their own mandate or tracking law enforcement concerns in support of other agencies, the MSOCs are not law enforcement agencies and as such do not collect what has been designated as personal information under the Privacy Act.

Under the Privacy Act, information related to a person's identity; employment; financial status; education and training; their personal activities and habits; their relationships; and any criminal or terrorist related history are all considered private. The same is true of detailed information related to corporations and other business arrangements. However, in many cases such information is highly useful in assessing and confirming or denying the existence of a threat. For example, hypothetically, if an MSOC is tracking a vessel which is making an unscheduled deviation from its course, information related to a senior crew member's association with a weapons smuggling organisation would be useful in assessing the threat posed by the deviating vessel. Alternatively, if the hypothetical vessel was operated by a group with an interest in harp seals, the threat could be discounted. Personal information of this nature is also useful in assessing the reliability and credibility of human sources of information. Personal information can help analysts understand a person's motivations for providing information and may indicate whether they are in a position to obtain the information in the first place. Finally, personal information can aid in placing information collected by other means into the correct context and as such help in making sense of what other sensors and sources are providing. For all these reasons, the access to personal information by the MSOCs could be of value to these units. Under

the Privacy Act, the collection and handling of such personal information is restricted to certain elements within the government.

In addition to information voluntarily shared by an individual or corporate entity, the Privacy Act acknowledges that there are "investigative bodies" that need to collect personal information for law enforcement and intelligence assessment purposes.[64] Investigative bodies of the Canadian Government are specifically identified as such by an Order in Council.[65] At this time, the CF as a whole is not considered to be an investigative body and the MSOCs do not fall into this category either. The Privacy Act provides designated investigative bodies guidance on the collection, handling, storage and disposal of personal information. It provides limited guidance on the sharing of such information but it can be surmised that if any sharing does occur, it should only be between designated investigative bodies and not with other organisations that do not have this role. In reviewing the RCMP's current national security activities, the O'Connor Commission noted that direction and policy on the sharing of information were not extensive. The Commission further noted that the RCMP generally used "consistent use disclosure" to substantiate the exchange of information between law enforcement agencies which lends credence to the view that personal information can only be shared between similar investigative bodies.[66] Since the MSOCs are not investigative bodies they are not permitted to handle personal information. The limitation on sharing personal information places a restraint on the extent to which information can be shared within the MSOCs and therefore effectively limits the mission effectiveness that can be achieved through network enabled operations.

---

[64] Parliament of Canada, *Privacy Act 1980-81-82-83, c. 111, Sch. II "1". Consolidated*, 4.

[65] *Ibid*., 44.

[66] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 112 to 115.

Since the risk of mission failure due to inadequate information sharing is high, as will be detailed in Chapter 4, it might be beneficial to increase information sharing within the MSOCs to maximise the effectiveness of the MSOCs' networked enabled operations. To achieve this will require the MSOCs to gain greater access to personal information, and this change will have an impact on their structure and operations. Amongst other requirements, to fully fulfill and support the collection and handling of personal information, the MSOCs would need to be designated as investigative bodies by an Order in Council in keeping with Privacy Act. Further, the MSOCs would need to be established as registered personal information databanks related to intelligence activities. The MSOCs' procedures would need to be amended to record personal data in keeping with personal databank standards and additional staff would be required to maintain the databank to this standard as well as maintain necessary records and registration with the Government of Canada.[67] While these are not insurmountable problems in themselves, it is unlikely that the government will take this step as this would appear to make the CF involved directly in domestic law enforcement. Because the collection and handling of personal information is required to further enhance the effectiveness of the MSOCs and mitigate the risk of mission failure, a change in governance might be in order to achieve this. If this approach to enhancing information exchange is taken, the MSOCs could be placed under the direction of a law enforcement agency which has already been designated as an investigative body, most likely the RCMP, or established as independent agencies. These options will be discussed more fully in Chapter 5 as possible mitigations to existing concerns that information sharing is not sufficient to maximise the effectiveness of the MSOCs.

Beyond the letter of the Privacy Act, the MSOC staffs should also consider recent interpretations of the law by commissions of inquiry into national security matters. In particular, the O'Connor Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher

[67] Parliament of Canada, *Privacy Act 1980-81-82-83, c. 111, Sch. II "1". Consolidated*, 10 to 11.

Arar made several observations related to interagency activities which could impact the MSOCs. While these observations were not directly related to National Defence or the MSOCs and are not binding, failure to take them into consideration could have consequences for the CF in the future.

In its investigations into the circumstances surrounding the Arar affair, the O'Connor Commission highlighted what it thought were great failures in interagency information sharing. Of particular note, the O'Connor Commission found that an investigative team within the RCMP was sharing information too freely. The sharing of unverified database contents and raw reporting by this team was strongly criticized. Another observed failure was sharing of information at the working level without sufficient direction and oversight by centralized information sharing control centres. The O'Connor Commission recommended that all such sharing of unverified information should be prohibited.[68]

The enhanced information sharing that would be required by security and law enforcement agencies to increase the effectiveness of the MSOCs can be seen to enable the free sharing of information abjured by the O'Connor Commission. While network enable operation theories see such free sharing as beneficial, as previously discussed, it does run counter to the spirit of the Privacy Act, against the recommendations of the O'Connor Commission, and puts at risk the privacy and safety of individuals. As such, the unregulated sharing of unverified information should be avoided as routine activity. The O'Connor Commission recommended that information could be shared at the national or operational level but that it needed to be carefully screened for relevancy; accuracy and reliability; and privacy concerns. The Commission further recommended that such sharing should be directed and overseen by central agencies. Additionally, the O'Connor Commission recommended that all organisations dealing with national security matters and the exchange of information related to national security should be subject to independent

[68] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Reporting the Events Relating to Maher Arar: Analysis and Recommendations*, 331 to 343.

review by an external agency with the requisite expertise and full access to the internal workings of the agency under review. Finally, the Commission recommended that these procedures be applied by all government departments.[69]

If fully applied, the recommendations of the O'Connor Commission will have an impact on the free sharing of information within the MSOCs. Procedures for screening and national oversight could slow the exchange of information and make members extremely cautious about what they share. Additionally, screening for relevancy and reliability is counter to network enabled operations concepts which would see information being freely available so that the user, not the provider, would determine its relevancy and could compare the information with other information available to determine its accuracy and reliability.

In addition to regulating how information is shared within the MSOCs, the MSOCs need to regulate how information flows out to their partner agencies. In keeping with the recommendations of the O'Connor Commission, on a routine basis the MSOCs should implement the screening and oversight measures recommended by the Commission. Raw reporting should not be shared. Rather, the MSOCs should release only fully developed, finished products whose format and content have been established in advance. The MSOCs require a set of policies and procedures for carefully checking the contents of the reports for accuracy and veracity before release. These policies and procedures will need to be authorised by the central authorities who establish overall release of information policy for the CF and these elements will need to monitor and oversee information sharing by the MSOCs with external elements. All these arrangements should be subject to independent review which would require the establishment of a review body and its supporting staff.

---

[69] *Ibid*., 331 to 343.

Full implementation of the O'Connor Commission recommendations will likely significantly impact information sharing within the MSOCs and their external sharing of information with partner entities. Implementing the recommendations will impact MSOC policies and procedures, and may create requirements for additional staff to handle the additional workload. Overall, it is assessed that implementation of the Commissions recommendations will impede the richness and speed of information exchange and therefore have an impact on the effectiveness of the MSOCs as information fusion centres.

The Maher Arar case investigated by the O'Connor Commission does highlight the dangers of the free information sharing that could result if the Privacy Act regulations and the recommendations of the commission are not applied. The MSOCs and their partner agencies are complex entities and if they do not carefully adhere to information control regulations, the flow of information can often be unpredictable. While generally it is rare and exceptional that a government officer will intend to cause harm to an individual, unpredictable results from the improper sharing of information can more commonly result in serious injury as is demonstrated by the Arar case. At minimum, an improper exchange of information could lead to close scrutiny of the inner working of government agencies by boards or commissions of inquiry, public censure of the government or one of its constituent organisations, and a loss of confidence in the government. In more serious instances, elements of partner agencies not fully aware of the source and/or reliability of the information could be motivated to take action based on an incomplete understanding of the situation. Alternatively, information that is shared to freely without appropriate caveats and restrictions can become the impetus of inappropriate responses even by those who are authorised to handle such information but receive the information without fully understanding its reliability and accuracy. If information is shared inappropriately, government agencies could be motivated to undertake actions that could severely impact the lives of individuals. They could be falsely arrested, denied entry into the country, forced to leave the

country, or in the extreme case, be subjected to violence or military force.[70] In other circumstances, information that is shared too freely could be inadvertently released to the wrong people. If wrongfully leaked to a third party; private individuals, foreign governments and/or business interests could use the information against the victim. If information is leaked to a third party, the subject of the information could be made the victim of criminal activity, refused employment, publically embarrassed, or suffer financial consequences. Wrongful disclosure could also lead to a situation where sources of information could be compromised. Compromised sources will no longer be able to provide the timely, reliable information. Worse yet, human sources of information could become the subject of intimidation or the victims of violence. The consequences of improper information sharing are serious and as such the risk condition wherein serious harm can befall individuals due to excessive information sharing must be considered carefully even if it may impinge on achieving enhanced operational effectiveness.

**Potential Confusion With Respect to the MSOC Role**

While at first glance the role assigned to the MSOCs in the NSP is simple and straightforward, challenges have arisen in the implementation of the initial operating capability that have caused the role to evolve. The following study will examine the role assigned by the NSP and its subsequent evolution to highlight problem areas in the assigned role caused by conflicts between the MSOC role and partner agency mandates. The examination will also consider mission areas that are not adequately addressed in the current construct. The discussion will identify where there are possible changes that may be considered in the risk mitigation strategies evaluated in Chapter 5. Finally, this analysis will examine the potential consequences of the risk condition wherein law enforcement agencies incorrectly employ the MSOCs to fill law enforcement requirements.

---

[70] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 570 to 572.

The CF MSOCs are part of the Government of Canada's response to the 9/11 attacks and revised assessment of threats to North American continental security and their stated purpose is to lead on-the-water responses to national security threats. The need for the MSOCs was first articulated in *Securing an Open Society: Canada's National Security Policy* (NSP). In this articulation of the purpose and function of the MSOCs, the Government stated ". . . Marine Security Operations Centres will have the authority and capacity . . . to bring to bear all civilian and military resources necessary to detect, assess, and respond to maritime security threat."[71] Implied in this role are both the intelligence and operations coordination function intimately connected as recommended by the 9/11 Commission. Since the publication of the NSP, the role has evolved to focus on intelligence fusion and support to the operations coordination function. Specifically, the role identified by the five partner agencies is:

- CF MSOC Mission: "The Marine Security Operations Centres' mission is to generate maritime situational awareness by combining knowledge and skill sets of the government agencies engaged in, or in support of, marine security. It will accomplish this through collection, integration and analysis of the information sources of these agencies, thereby assisting in the detection, assessment and support of a coordinated response to a marine security threat or incident."[72]

- RCMP's Description of the MSOC Role: "The primary purpose of an MSOC is to produce actionable intelligence, concentrating on national security, organized crime and

[71] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, 38 to 39.

[72] Department of National Defence, *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*, 4.

other criminality and to communicate the information to the appropriate jurisdiction in a timely fashion."[73]

- Canadian Coast Guard MSOC Role: "The MSOC is a joint facility that brings together all of the government entities responsible for the marine areas of Canada . . . It provides a single secure location where the representatives from those bureaucracies can collect, share and assess information regarding potential threats to Canadian security and enhance their common awareness of any situation."[74]

- Transport Canada MSOC Role: ". . . to detect, assess, prevent and respond to a direct or indirect marine security threat."[75]
- CBSA has not publically published a defined role for the MSOCs.

The reasons for the change in role are two fold. First, each core partner agency already has an existing operations centre or office that runs its day-to-day operations. It would be a violation of departmental mandates to subordinate these entities to a CF led MSOC. Second, interagency coordination to respond to a national security threat normally is conducted by executive level departmental leaders within the DMG. This executive level of leadership must be engaged to commit departmental resources to and interagency operation. This DMG could not be subordinated to the MSOCs which are led by officers who hold the Navy rank of Commander and therefore do not hold sufficient rank to have executive level leaders subordinate to them. Instead, the compromise role was implemented for the MSOCs wherein they perform the intelligence function to support an external DMG. This approach causes a divide between the intelligence and

[73] Royal Canadian Mounted Police, "Marine Security Operations Centres," Government of Canada, http://www.rcmp-grc.gc.ca/mari-port/msoc-cosm-eng.htm (accessed 04 February 2011).

[74] Canadian Coast Guard, "Canadian Coast Guard: Maritimes Region," Canadian Coast Guard, http://www.ccg-gcc.gc.ca/e0003796 (accessed 15 April 2011).

[75] Transport Canada, "Transportation Security," Government of Canada, http://www.tc.gc.ca/eng/policy/report-aca-anre2006-4b_security-eng-1551.htm (accessed 05 February 2011)

operations coordination function but this is somewhat mitigated by close association between MSOCs and the DMGs. Mitigation strategies that can bring together the intelligence and operations functions into a single entity would better implement the lessons learned from the 9/11 attack and more closely adhere to the intent of the NSP as will be discussed in Chapter 5.

The RCMP description of the role of the MSOCs also raises the issue of possible misemployment of the CF led MSOCs, specifically their use to produce intelligence on organised crime and criminality. The NSP provides specific direction regarding responsibilities in the maritime domain identifying three areas of activity. The NSP designates the Minister of Transport as lead for marine safety and security policy. The Minister of Public Safety is lead for enforcement and policing. The Minister of National Defence (MND) is responsible for responding to maritime security threats. In outlining these responsibilities, the NSP clearly makes a distinction between law enforcement and response to security threats. While the NSP does not specifically define marine threats, it does indicate the national threats are ". . . those that have the potential to undermine the security of the state or society. . ."[76] and require a national response due to the lack of capacity at lower levels. The NSP also indicates that ". . . while most criminal offences, for example, may threaten personal security, they do not generally have the same capacity to undermine the security of the state or society as the activities such as terrorism or some forms of organized crime."[77] The NSP therefore clearly lays out three broad areas for government action and assigns lead departments for each area.

All three areas of activity require interagency coordination and participation, but only two interagency mechanisms are currently in existence. The Ministry of Transport is chair of the Interdepartmental Marine Security Working Group which coordinates interagency development of marine security policy and regulation. The NSP directed the CF to establish the MSOCs as

---

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

[77] *Ibid*.

interagency centres to assess, detect, and respond to marine security threats. As such, the MSOCs provide the necessary interagency coordination to fulfill the MND's needs for whole-of-government coordination to meet his component of the delegated security responsibilities. As it currently stands, the Minister of Public Safety has no standing facility to coordinate interagency activity in support of executing his responsibilities for maritime law enforcement and policing as designated in the NSP. Absent a standing resource such as a coordination centre, working group, or enforcement team, law enforcement and regulatory authorities must currently rely on other means to fulfill there interagency coordination requirements in support of their marine law enforcement role. This situation leads law enforcement and regulatory agencies to rely heavily on the MSOCs to assist them in interagency coordination as indicated by the RCMP's description of the MSOCs' role. This reliance is evident in the MSOC performance of the collection management function to deconflict maritime surveillance and efficiently achieve information collection in pursuit of all the partner agency mandates. The need for a interagency information sharing and coordination facility creates a risk condition wherein the CF led MSOCs are employed to support law enforcement activities outside of their authority. It also can result in some confusion regarding the true role and purpose of the CF led MSOCs.

In accordance with the direction provided with the NSP, the MSOCs are currently aimed at addressing only national security threats, not law enforcement issues, and contribute to coordinating an on-the-water response to such threats within the mandate given to the MND within the NSP. The CF can play a supporting role in law enforcement and regulatory operations under the authority of Section 273.6 of the NDA, however this is not intended to be a routine occurrence and there is no standing authority to conduct such support.[78] CF direction instructs that authority to support law enforcement operations is normally to be granted on a case by case basis. These measures help ensure that the CF remains a resource of last resort in domestic

[78] Parliament of Canada, *National Defence Act. R.S., c. N-4, s. 1. Consolidated*, 212 to 217.

operations and minimise the risk that military force will be used inappropriately against Canadians. In some cases, such as support to fisheries patrols and counter drug operations, memoranda of understanding (MOUs) have been established between the CF and the other involved ministries to authorise this support on a more routine and responsive basis.[79] Besides the operations covered by the existing MOUs, the minister has also delegated some powers to authorise support to provincial and municipal police down to operational commanders where such support does not involve potential public confrontation.[80] As MSOC support to law enforcement is operational support where the CF will not be directly in contact with any disturbance of the peace, the MND could delegate authority to authorise such support, where it is not covered by an existing MOU, to operational commanders, similar to the arrangements in place to support provincial and municipal police. In the case of the MSOCs, in the transformed CF structure, the operational commander is commander Canada Command. Commander Canada Command could also delegate these powers further down to the regional command, rear admiral, level.

Ideally, from a departmental mandate perspective, the national security and law enforcement activities should have separate interagency information sharing and coordination facilities, but this would be inefficient and cumbersome. As noted previously, the resources to conduct surveillance of Canada's extensive ocean areas are limited. They are too limited to be shared efficiently between two separate information sharing centres. Sharing collection resources between two centres would also create an additional requirement for another layer of interagency coordination. In addition, the creation of two centres for interagency information sharing would lead to a further requirement for information sharing and coordination between the two centres as tracks of interest may be of indeterminate threat, a national security threat, a law enforcement

---

[79] Department of National Defence, *Canada Command Direction for Domestic Operations: Interim Version V1* (Ottawa: Department of National Defence, 2006), 11-3.

[80] *Ibid*., 11-4 to 11-5.

threat, or both, and the assessment of their status may change at any time as more information becomes available. From an efficiency perspective, it makes sense for there to be a single information sharing and collection coordination centre that supports both the national security and law enforcement roles. The MSOCs are able to fulfill this requirement if they are given a law enforcement role in addition to their national security role and authority is provided to conduct intelligence and collection coordination functions in support of law enforcement authorities.

As stated previously, the power to authorise operations in support of law enforcement agencies in cases where no direct involvement with a public disturbance is foreseen could be delegated to the commander of Canada Command or lower to the regional joint task force level. CF regulations intend that this power is normally exercised on a case by case basis. To facilitate the performance of the intelligence and coordination roles within the MSOCs in support of law enforcement on an ongoing basis, it is feasible for regional commanders to be delegated the power to authorise specific and limited intelligence and collection coordination activities. If the MSOCs are given a law enforcement role to achieve efficiencies in the intelligence and collection coordination functions, it would not be unreasonable delegate the power to authorise activities not covered by an existing MOU to the regional joint task force commanders overseeing the MSOCs who should be part of the DMG. The close connection between the MSOCs and the DMGs ensures that authorisations would be quick and responsive to changes in the situation. The speed and responsiveness of the authorisations would at minimum match the speed and responsiveness of the coordination of operational responses to the threat. This level of responsiveness can not be assured if the DMG must communicate with commander Canada Command each time the MSOCs are required to monitor a track of interest that represents a criminal threat. The seniority, knowledge, and experience of the CF representative on the DMG provide confidence that this power will only be exercised when it is necessary and reasonable to do so. Alternatively, a comprehensive MOU covering all the operations and functions of the MSOCs can be negotiated

between the core partners, but this will be a long and laborious process. The delegation of the power to authorise MSOC to conduct intelligence and collection coordination functions in support of law enforcement or the creation of an MOU to detail their operations are possible mitigations to the risk condition that the MSOCs may be employed outside their current authorities to support law enforcement agencies and will be considered further a possible risk mitigation measure in Chapter 5.

**Summary**

Within the MSOC construct, there exists tension between the need to share information to maximise effectiveness and the need to control information in accordance with Canadian law to protect the liberties and safety of individuals and additional tension related to the role of the MSOCs due to the requirement for the MSOCs to meet both national security and law enforcement roles while closing gaps between intelligence and operations. Increased information sharing is needed to achieve information superiority over potential national security threats; and enable self synchronisation, agile response, and flexible leadership. However, increased information sharing could increase the risk of misunderstanding the information shared causing harm to individuals, or the inadvertent compromise of a source of information jeopardising the usefulness and potentially the safety of that source. There is also a risk that there are gaps between intelligence and operations coordination that, as the 9/11 Commission observed, might have a detrimental impact on responding to national security threats. Finally, there is a risk that the CF led MSOCs, which currently have strictly a national security role, may be used inappropriately on an ongoing basis to support law enforcement activities. As these risk conditions are grave concerns, it is incumbent on the government to implement mitigation measures. To prioritise and judge the importance of the risk conditions that must be mitigated, this analysis will first determine the level of risk posed by the three risk condition discussed.

## CHAPTER 4 – RISK ASSESSMENT

Within the CF risk management process, risk is defined as the chance of injury or loss, including mission failure, expressed in terms of the severity of potential harm and probability that the injury or loss will occur. Risk is assessed to aid decision makers in understanding the risks they face and prioritise mitigation measures.[81] This examination of the MSOC construct has identified that there are risks of inadequate information exchange to implement network enabled operations contributing to mission failure, too much information sharing leading to misuse of the information or inadvertent disclosure to third parties potentially causing injury to individuals, or confusion with respect to the role of the MSOCs creating potential gaps that could degrade mission effectiveness or lead to the inappropriate employment of CF resources. This chapter continues this analysis by assessing first the severity and then the probability of these risks separately. Subsequently the severity and probability will be compared to determine the risk levels faced in MSOC operations. The aim is to fully understand the relative level of risk presented by each risk in the conduct of MSOC operations and prioritise the requirements for mitigation measures. The final assessment will show that there is significant risk in balancing the need to share information to achieve mission success with the need to control the flow of information to ensure that the lives and liberties of individuals are safeguarded.

**Step 4 – Assessing Severity**

To assess the level of risk faced in MSOC operations, it is necessary to first evaluate the potential severity of the risk of mission failure due to inadequate information sharing; personal injury due to poorly controlled information sharing; or degradation of mission effectiveness or loss of political support due to inappropriate employment of the CF. The CF risk management process classifies the severity of risk in four broad categories as follows:

---

[81] Department of National Defence, *B-GJ-005-502/FP-000 Risk Management for CF Operations*, 1-1 to 2-1.

- Catastrophic: These are risks that can lead to the loss of the ability to achieve the mission, may result in death or permanent disability, or result in loss of political support.

- Critical: Critical risks are those risks that can significantly degrade mission capability, lead to personal disability, or damage political support.

- Marginal: Risks that can lead to mission degradation, have a minor impact on political support, or result in injury to individuals are defined to be marginal risks.

- Negligible: Negligible risks are those that have little or no impact on mission effectiveness, no adverse affects on political support, or result in minor injury requiring limited remediation action.[82]

Applying the classification above, it is evident that the severity of the risk of MSOC mission failure would be catastrophic. Experience has shown that terrorist attacks can cause significant causalities including numerous deaths and normally even more injuries. To name just two examples, the 9/11 attacks resulted in thousands of casualties and Air India Flight 182 bombing led to hundreds being killed. Any risk that may result in death or permanent disability must be assessed as catastrophic in the CF risk classification system.

The severity of the risk of excessive information sharing in the MSOCs is catastrophic. As noted by the O'Connor Commission, the police powers of law enforcement agencies can lead to false arrests; detention; search and seizure; refusal of entry into Canada; refusal of employment; and restrictions on the use of transportation.[83] If the CF is involved, the inadvertent misuse of military force could result in death or serious injury. If information is wrongfully

[82] *Ibid*., A-1.

[83] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, 570 to 572.

leaked to a third party, the subject of the information could suffer loss of employment, loss of reputation, or they could become the victim of blackmail or other crimes or suffer financial penalties such as refusal of loans or refusal of banking services. Compromised sources could be subject to intimidation or violence, possibly including death. Under these circumstances, the results of improper information sharing would be catastrophic.

The final risk under consideration, the danger of role confusion leading to gaps that could degrade mission effectiveness or misemployment of CF resources is marginal. As noted in the analysis of the causes of this risk, the close association between the MSOCs and the DMGs has mitigated the remaining separation between the intelligence and operations function so that mission effectiveness may be degraded by the separation but not significantly so. Additionally, the potential for the CF to be misused, without the appropriate authority in support of law enforcement activities could lead to inquiries into the conduct of MSOC operations, public censure of the government and could cause minor damage to political support for the government, no government has fallen because of a situation where not all the legal authorities to enable interagency operations have been completed correctly. The fact that risk of inappropriate employment of the CF could lead to minor damage to political support for the government by definition means that the severity of this risk is marginal.

The potential injuries or losses that could result from inadequate information sharing, poorly controlled information sharing or confusion in the MSOCs' role are severe, but they are only part of the calculation of the level of risk. It is a mistake to consider only the severity of outcomes in evaluating risk in that a severe outcome that is unlikely to occur is still a minor risk. Judging the probability that these risk conditions may present themselves during MSOC operations is a necessary step in the risk assessment process.

**Step 5 – Assessing Probability**

Assessing the probability that the inadequate sharing of information within the MSOCs will result in mission failure; that weak control of information by the MSOCs will cause personal injury; or that confusion with respect to MSOCs' role will lead to mission degradation or misapplication of CF resources entails categorising the probability of these conditions arising into one of the five measures of probability detailed in the CF risk management process. The five measures defined by the CF are:

- Frequent: The risk condition is expected to occur continuously during an operation.
- Likely: The risk condition is expected to transpire at a high rate but experienced intermittently.
- Occasional: The condition arises sporadically or sometimes.
- Seldom: The risk conditions happen rarely and as isolated incidents.
- Unlikely: The conditions occur only very rarely but are not impossible.[84]

Employing the measures of probability from the CF risk management process, the probability of risk of mission failure due to inadequate information sharing within the MSOCs is categorised as seldom. Although terrorist attacks have occurred in Canada, they occur rarely. While threats have been identified within the last decade, the existing counterterrorism arrangements have been adequate to thwart them. Canada has not suffered a successful terrorist attack since the Air India Flight 182 bombing of 1985. Since the Air India attacks, there have been no successful threats of multiple, coordinated attacks.[85] As terrorist threats to Canada only develop occasionally and are

---

[84] Department of National Defence, *B-GJ-005-502/FP-000 Risk Management for CF Operations*, A-2.

[85] Integrated Threat Assessment Centre, "Terrorism in Canada," Integrated Threat Assessment Centre, http://www.itac-ciem.gc.ca/thrt/cnd-eng.asp (accessed 16 April 2011).

rarely successful, particularly in the last decade, they can be characterised as seldom under the risk management lexicon.

The probability of risk of personal injury due to poor control of information exchange in MSOC operations is characterised as occasional. Government agencies generally do not intentionally cause harm to individuals, however errors do occur from time to time due to the complexity of government operations. The absence of greater public concern indicates that in general, the existing review and remediation measures are generally successful in identifying and correcting situations where errors occur. The notable exceptions are the cases investigated by the O'Connor Commission, and the cases of Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, three additional Muslim-Canadians interrogated by Middle-Eastern authorities probably based on information provided by Canadian officials, investigated by the Iacobucci Commission, all of which occurred in the last decade.[86] While these might represent relatively rare cases in the history of Canadian intelligence and law enforcement activities, that they all occurred in the first half of the last decade raises the concern that these issues have become more frequent since 9/11. Since the release of the O'Connor and Iacobucci commission reports, the government has taken steps to prevent a reoccurrence of these events which have lead to reduction in their incidence in the latter half of the last decade. As cases of poorly controlled information exchange occurred sporadically in the aftermath of the 9/11 attacks, the probability of risk in this area is judged to be occasional as defined by the CF risk management process.

The risk of confusion regarding the role of the MSOCs causing gaps in mission execution or misemployment of CF resources is the final risk to be evaluated for probability and is assessed as occasional. The state where the intelligence function is separated from the operations

[86] Canadian Broadcasting Corporation, "In Depth Maher Arar: The Cases of Almaki, Nureddin and El Maati," Canadian Broadcasting Corporation, http://www.cbc.ca/news/background/arar/torture-claims.htm (accessed 16 April 2011).

coordination function is an ongoing problem that could result in mission degradation, albeit limited degradation due to the close relationship between the MSOCs and DMGs. Additionally, the core partner interest in employing the MSOCs to meet their day-to-day requirements for interagency coordination in support of their separate mandates and the efforts to derive efficiency in collection efforts by employing all available collection assets to achieve all the core partners mandates leads to a high rate of situations wherein CF resources are collecting information in support of other departmental mandates. While it is acknowledge that several MOUs exist to authorise some of these activities, there are areas of activity where specific authorisation by higher authorities is required under the NDA. It is likely that sometimes, the required authorisations lag behind the necessary activity which means the results of the collection cannot be used for the effects desired. Given that the issue occurs at a high rate and causes problems sometimes, the assessed probability, in the lexicon of the risk management process, is occasional.

**Step 6 - Completing Risk Assessment**

As indicated previously, the risk assessment process is completed by comparing the severity of the risk to the probability that the dangerous situation may develop. This comparison is done using Table 1 to cross index the severity with the probability to determine the risk level. The terms used to describe the risk level are:

- Extremely High Risk: If the risk condition develops during an operation, the operation will fail with severe consequences.
- High Risk: If the risk situation occurs during an operation it will likely result in severe mission degradation.
- Moderate Risk: If this risk occurs during an operation mission degradation will occur. It is unlikely in this event that catastrophic loss will result.

- Low Risk: Expected losses will have minimal impact on achieving the mission.[87]

**Table 1: Risk Assessment Matrix**

| Severity | Probability | | | | |
|---|---|---|---|---|---|
| | **Frequent** | **Likely** | **Occasional** | **Seldom** | **Unlikely** |
| **Catastrophic** | Extreme | Extreme | High | High | Moderate |
| **Critical** | Extreme | High | High | Moderate | Low |
| **Marginal** | High | Moderate | Moderate | Low | Low |
| **Negligible** | Moderate | Low | Low | Low | Low |

Source: Canadian Forces, "B-GJ-005-502/FP-000 Risk Management For CF Operations," A-1

Conducting the assessment of risk process outlined, we can see that the risk of mission failure due to inadequate information sharing is high, the risk associated with the potential of personal injury due to excessive information sharing is also high, and the risk resulting from MSOC mission confusion is moderate. The risk associated with inadequate information sharing is of catastrophic severity and a probability measure of seldom which are cross referenced to identify a high risk level. The risk associated with too much information exchange also is catastrophic in its severity and the probability measure is occasional. Therefore, cross referencing these measures also identifies a high risk level. Finally, the risks associated with role confusion have a marginal severity and the associated probability measure is occasional. These measures are cross referenced to determine that the associated risk level is moderate. This assessment leads to the conclusion that there is a substantial requirement to mitigate the risks of deficient information

[87] Department of National Defence, *B-GJ-005-502/FP-000 Risk Management for CF Operations*, A-1.

sharing, and weakly controlled information sharing, while the risk associated with potential misunderstanding of the MSOC role is important but of a lower priority. Of note, the risks associated with insufficient information sharing and excessive information sharing are both judged to be high. This highlights the underlying tensions that are present in these opposing requirements in that it is almost equally important to resolve both these requirements. However, scrutinising the underlying assessment of severity and probability shows that while both risks are of catastrophic severity, the probability of inadequate information sharing is seldom while the risk of poorly controlled information sharing is occasional indicating that the latter should receive slightly greater attention in the implementation of mitigation measures. Possible mitigation strategies are the subject of the next chapter.

## CHAPTER 5 – RISK MITIGATION MEASURES

### Step 7 – Developing Possible Controls

Developing measures to mitigate and thus reduce the risks faced in the conduct of CF operations is ultimately the purpose of the CF risk management process. This chapter will consider the risks faced in the conduct of MSOC operations and identify changes in role, governance, procedures and structure of the MSOCs that could mitigate the risks that have been assessed. The risks will be considered in order of lowest priority to highest as indicated by the risk assessment process. The aim of identifying these mitigation measures will be to note changes to the MSOC construct that will enhance the overall mission effectiveness while limiting the potential of injury to individuals and their personal interests.

### The MSOCs' Role

The current national security role of the MSOCs is adequate for CF purposes and provides the CF with the authorities required to conduct the necessary MSOC operations, but leaves the requirements of the partner agencies unanswered and therefore should be changed. As

noted in Chapter 3, law enforcement and regulatory agencies working in the maritime domain require an interagency information sharing and coordination capability. For the sake of efficiency it is best to have a single facility for both national security purposes and law enforcement and regulatory purposes. Therefore, the MSOCs should formally be given the role of supporting national security and law enforcement and regulatory operations. This measure will also help to motivate partner agencies to provide their maximum support to the MSOCs since they will be dependent on these centres for their own interagency information sharing and coordination means. However, to enable this, the CF will need to review its procedures and documentation to ensure that the MSOCs' have the authority to conduct law enforcement support operations when such authorities are required. One approach to resolve this requirement would be for one of senior the CF representatives on the DMG to have the power delegated to authorise the MSOCs a narrow set of activities related to information collection and intelligence assessment in support of law enforcement operations. An alternative approach that would likely take longer to implement but may provide a more robust response is for the five core partners to develop an MOU detailing what activities the MSOCs will perform in support of maritime law enforcement operations. This memorandum would likely incorporate authority to conduct activities already identified in existing MOUs with some of the core partners. It is likely that an MOU will take some time to negotiate and implement, therefore, the delegation of powers may be the short term mitigation to this risk with the aim of developing a full MOU in the long term. These measures will significantly reduce the risks associated with role confusion. A small gap in the role will remain due to the close but separate relationship between the intelligence and operations function. This will be discussed in greater length later in the chapter. If the MSOCs are given a wider range of responsibilities, it is also possible that a change in governance is in order to facilitate enhanced effectiveness.

**Governance**

As discussed in Chapter 3, it is unlikely that the MSOCs could be designated investigative bodies to permit enhanced information exchange. The MSOCs were established within the CF with a focus on performing national security roles. As CF organisations, they are not generally considered to be investigative bodies and as such, their authority to handle personal information is restricted by the Privacy Act. An Order in Council could make an exception and designate them investigative bodies but this has the taint of a military state and would likely not be generally acceptable. As the risk of mission failure due to inadequate information sharing has been assessed as high, it is likely appropriate to change the governance of the MSOCs so that they may obtain a designation as an investigative body permitting a freer exchange of information within the MSOCs.

If the governance of the MSOCs was changed so that they became operating entities within a law enforcement agency, most likely the RCMP, the MSOCs would automatically become investigative bodies and would be permitted to handle personal information. The RCMP are one of the core members of the MSOC construct, have a strong national security and law enforcement mandate and the entire force is considered to be an investigative body. Encapsulating the MSOCs within the RCMP would be a relatively straight forward change that would give the MSOCs the ability to enhance their exchange of information and thereby increase their mission effectiveness. This change however, would likely worry some leaders within the CF as they would be concerned that the emphasis of the MSOCs would shift from responding to national security threats to supporting law enforcement operations. The reality is that while embedded within the CF, if the MSOCs' role was to support national security and law enforcement activities, all the other core partners would have some concerns that their particular area of focus is not being adequately addressed and this situation would simply be reversed if the MSOCs were re-aligned to a law enforcement agency. A more neutral option for governance may alleviate these anxieties.

The MSOCs could be established as independent operating elements while keeping their existing structures largely intact. If this approach is taken, it would be administratively more efficient for all the MSOCs to be developed into a single independent agency with the existing centres as subordinate units and possibly a centralised headquarters to perform administrative functions rather than have separate administrative components for each MSOC. As an independent element with a strong law enforcement as well as national security role, it would be practical to designate the overall MSOC structure as an investigative body enabling more liberal information exchange. Independent of the core partners, the MSOCs would be in a very strong position to evenly support all the partner mandates. This balanced approach could be further strengthened by having the organisation's head and key deputy roles divided up to all of the core partners, possibly in rotation. However, this approach would be very burdensome. It would involve establishing a new organisation with a new administrative structure and independent budget and financial management structure. This method of mitigating the risk of mission failure is feasible and would achieve the necessary enhancements in information sharing to achieve increased mission effectiveness but it would be very elaborate and resource intensive. This strategy may be acceptable if the structure is also changed to achieve additional benefits as will be discussed later. Regardless of which agency has governance over the MSOCs, the governing agency will need to review the MSOCs' procedures to ensure that not only is information exchanged more effectively, but also so that information exchange is controlled in a manner that protects individuals from injury or harm.

**Controlling information**

As noted in Chapter 4, the risk of personal injury due to weakly controlled information exchange within the MSOCs is high. It is the greatest risk faced in the course of MSOC operations and therefore it is critical that the MSOCs implement procedures to ensure that information sharing is adequately controlled. If the MSOCs are designated investigative bodies or

become part of an agency that is already and investigative body, they will need to implement the measures laid out in the Privacy Act to handle personal information. Such measures will include fully documenting all data banks that contain personal information, registering those data banks with the appropriate government authorities, and reporting regularly on the general contents of those data banks.[88] Additionally, the MSOCs should implement the recommendations of the O'Connor Commission regarding the sharing of law enforcement information. Important recommendations include documenting interagency information sharing arrangements; maintaining centralised oversight of information sharing; adhering closely to information sharing policies including policies for screening information for reliability, accuracy, relevance, and personal privacy concerns; employing caveats in the production of products intended for sharing; and most importantly establishing an independent review mechanism to ensure that information exchange policies and practises do not endanger individuals.[89] If the MSOCs remain part of an established agency, they can be incorporated into existing arrangements to safeguard information in the manner recommended by the O'Connor Commission. If the MSOCs are established as independent operating entities, then separate procedures and review mechanisms will need to be established. While it is likely that such an independent entity could adapt its information control arrangements from existing agencies, it would nonetheless contribute to the burden of establishing such an independent organisation. While the O'Connor Commission investigation and recommendations were focused on the RCMP, it is important that all government departments involved in the law enforcement and national security realms take heed of the findings and implement measures to prevent similar events in their own operations. As the risk of personal harm due to poorly controlled information sharing is entails the highest level of risk in MSOC operations, it is important that these lessons are fully applied within the MSOCs.

---

[88] Parliament of Canada, *Privacy Act 1980-81-82-83, c. 111, Sch. II "1". Consolidated*, 6 to 11.

[89] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Reporting the Events Relating to Maher Arar: Analysis and Recommendations*, 364 to 369.

**Integration of Intelligence and Operations**

As described in the previous chapter, the potential danger arising from the existing slight separation between the intelligence and operations coordination function is part of the larger risk condition caused by confusion in the role of the MSOCs and is assessed to be a moderate level risk. Nonetheless, this problem was one of the major lessons identified by the 9/11 Commission and merits some consideration for mitigation strategies. As outlined in Chapter 3, the problem has persisted beyond the publication of the NSP because the operations coordination authorities of the core partners can not be subordinated to a discrete unit within one of the involved agencies. The core partners have substantially mitigated this risk by creating a close relationship between the MSOCs and the DMGs. The mitigation measures outlined so far in this examination will have no impact on this aspect of the MSOC construct as they have not yet dealt with possible changes to the structure of the MSOCs.

Currently, the MSOCs exist as discrete operating units within the CF. The risks identified in this examination of their operations would be overcome if each MSOC was re-envisioned as a system. Each MSOC system would comprise the regional operations centres or offices of the five core partners and three of more core working groups. While the operations centres would retain their primary responsibility to their own agencies, they would have a secondary role as key elements of the regional maritime security system. At the core of the system there would be at least three interagency work groups with permanent secretariats to fulfill day-to-day working requirements. The first and most important would be the DMG comprising the regional chiefs of operations of the five core partners. The DMG would act as a board of governors for the system and as such would be responsible and accountable for the operation of the system. Since the system would not be part of any one partner agency, this board of governors would ensure balanced governance to the system and ensure the interests of all the partner agencies are met. The other two working groups would be the collection coordination working group and an

intelligence and risk assessment working group which would both be subordinate to the DMG. A possible further working group could be created subordinate to the DMG to conduct working level operations coordination if necessary. The leadership and key staff roles of the permanent secretariats of each subordinate working group could be divided up between the core partners and rotated over time to provide better interagency expertise to each working group and further reinforce the balance in addressing the interests of the core partners. The overall interagency governance of the system and even handed approach to addressing partner interests would help ensure that all the partner agencies remain committed to adequate resourcing of the system.

The role of the overall maritime security system would be to produce actionable intelligence, concentrating on national security, organized crime and other criminality and to coordinate interagency responses to these threats. The linkage between the DMG and the subordinate working groups will close any gaps that exist between the intelligence and operations function. As independent entities with a strong law enforcement role and presence; and identifiable and capable governance, the systems could be designated as investigative bodies authorised to collect and handle personal information thereby enhancing their effectiveness. Importantly, the system would still need to implement a reliable information control regime as outlined above and would need to develop an independent review mechanism that would need to be coordinated between all the partner agencies and their existing review mechanisms. Since operations are controlled by an interagency board of governors, administration will be a less contentious command and control responsibility and could be delegated to one of the partner agencies. As this is the case, administrative support could continue to be largely provided by the CF who have a substantial capability in this regard and have arguably the best ability to manage large projects similar to the one that would be required to implement the MSOCs as regional systems. To enable a systems approach toward the MSOC construct, this structure will require a dedicated information system to enable high quality, high capacity interaction between the

disparate elements of the entity including reaching into the operations centres of the core partners rather than just having partner networks reach into the MSOCs as is currently the case. Many of the organisational and operational elements of the systems approach to structuring the MSOCs have already been incorporated in the MSOCs' concept operations including some elements of the next higher level organisational structure.

As stated previously, if the MSOCs are to be independent structures, then it makes sense for them to be incorporated into a larger entity and this continues to hold true if applying a systems view. In this case, the MSOCs would become part of a system of systems. Like the regional systems, the larger system would require interagency governance in the form of a board of governors comprised of representatives from the five core partners. This board of governors could receive secretarial and administrative support from one of the involved agencies. As the CF already has in place a staff to help manage and direct the MSOCs they could continue in this role, albeit now in support of an interagency board of governors. The CF already has in place a national level project to develop an information system for the MSOCs which has already identified most of the information systems capabilities that would needed to enable a systems approach to the MSOC structure and this project could continue, again now in support of the interagency board of governors. The overall administrative and project support to the MSOC system could continue without substantial change.

The only significant obstacle to taking a systems view of the MSOC structure is gaining acceptance of a system as an organisational construct within the government. The systems approach is not a familiar one and could meet substantial resistance from government officials, legislators, and the public. Government structures are normally established with a very hierarchical structure with a single person being responsible and accountable for the activities of their offices. This is how the MSOCs are currently structured. The creation of dual lines of operations for the partner agencies' regional operations centres or offices will also be of concern.

However, the board of governors envisioned in the systems approach to the MSOC structure does provide responsible and accountable governance for the MSOC system and since its members are experienced and knowledgeable leaders who are also the operations managers for their respective agencies, they are in a strong position to deconflict the separate lines of operations for their operations centres. Implementing the systems approach will likely necessitate the negotiation of an MOU between the core partners to further detail the arrangements to deconflict the separate lines of operation; elaborate the roles, functions, responsiblities, and accountabilities of the MSOCs; and authorise the employment of the CF elements of the system to support law enforcement and regulatory activities on a routine basis for specific MSOC missions and tasks. Careful documentation of the systems operating concept, procedures, information safe guards, and responsibilities and accountabilities will help alleviate concerns of employing a system as a governmental organising construct. Education and experience will further help to alleviate any reservations. While the work involved in this approach is substantial, it is the best mitigation to the significant risks involved in MSOC operations.

**Summary**

The danger of mission failure due to inadequate information sharing, personal injury due to excessive information sharing, and role confusion leading to inappropriate use of military resources or gaps between the intelligence and operations function are serious problems that require mitigation. Measures that might be implemented to mitigate these risks include changing the MSOCs' role to include support to law enforcement and regulatory operations; putting in place the authorities for CF elements to participate in these actions; adjusting the governance to the most suitable organisation so that the MSOCs can act as investigative bodies allowing them to handle personal information; creating a strong linkage between the operations and intelligence function ideally within the MSOC construct itself; and most importantly ensuring that there are adequate controls on the sharing of information and that there is an independent review

mechanism to certify that these measures are effective. Taking a systems view of the MSOC structure best enables all these mitigation measures but may not be acceptable to government officials, legislators and the public. Even if this approach is not achievable, implementing the other measures discussed will mitigate the worst of the risks involved in the conduct of MSOC operations. These measures represent the best means of enhancing the MSOCs' operational effectiveness while safeguarding the safety and liberty of individuals.

## CHAPTER 6 – CONCLUSION

The conduct of MSOC operations entails high levels of risk. There exists a potential of mission failure due to the inadequate exchange of information and the risk that individuals monitored in MSOC operations may be injured by the inadvertent disclosure of their private information. As the risks present significant dangers, measures need to be implemented to reduce them to a minimum. Changing the role, governance, procedures, and structure of the MSOCs are viable solutions to minimising these risks. The optimum configuration for the MSOCs is to view them as independent systems directed by a board of governors drawn from senior, regional leaders from each of the core partner agencies and designated as investigative bodies. These systems will require thorough and effective information control regimes that should include an independent review mechanism. This approach will significantly reduce the tensions that exist between the need to share information and the need to prevent the inadvertent disclosure of private information.

While considerable work remains to be done to elaborate and document this concept of operations and detail the responsibilities and accountabilities of all elements of such a maritime security system, the systems approach to structuring the MSOCs will maximise their effectiveness and thereby fully realise the goals for which they were created. Optimising their effectiveness will enhance the security of Canada's transportation sector in the maritime domain. It will fully engage all the national security agencies operating in this domain in a coordinated and integrated

effort. These measures will ensure that the full range of maritime threats are identified, assessed, and effectively defeated by a coordinated response, effectively applying all the lessons learned from the 9/11 attacks. Through these efforts, Canada's maritime transportation security will be assured.

By enhancing the security of Canada's transportation sector, the maritime security system will contribute to the overall security of the nation. Importantly, they will do so without impinging on the safety and freedoms of individual Canadians. In this manner, the MSOC projects will meet all the goals of these organisations laid out in the NSP. Significantly, applying the transportation security enhancements outlined in the NSP will also reassure our allies.

Implementation of the NSP in general and enhancement to the MSOC system capability in particular will contribute to the continental security of North America. Enhancing out security efforts in the maritime domain will give the United States confidence that we are reliable partners. Improvements to our security measures will provide assurances that security threats cannot use Canadian waters as a transit route to attack our neighbours to the South. These assurances will contribute to maintaining the close integration of North American societies and a border with few restrictions to travel. In this way, increasing the effectiveness of the MSOCs not only provides Canadians with increased safety and security, but also helps maintain their economic prosperity, liberty to travel, and other social benefits from our close relationship with our neighbours. Achieving the maximum effectiveness in our maritime security systems is a step in the right direction that will benefit Canadians in many ways.

**BIBLIOGRAPHY**

Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. *Understanding Information Age Warfare*. Washington: Command and Control Research Program, 2001.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command, Control in the Information Age*. Washington: Command and Control Research Program, 2003.

Bruyn Martin, Lora E. *Information Exchange in Joint, Interagency, Multinational, and Public (JIMP) Operations: Final Report*. Guelph: Humansystems Incorporated, 2008.

Canada, Canadian Coast Guard "Canadian Coast Guard: Maritimes Region." Canadian Coast Guard. http://www.ccg-gcc.gc.ca/e0003796 (accessed 15 April 2011).

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

———. *Reporting the Events Relating to Maher Arar: Analysis and Recommendations*. Ottawa: Minister of Public Works and Government Services, 2006.

Canada, Department of National Defence. *B-GJ-005-502/FP-000 Risk Management for CF Operations*. Ottawa: Department of National Defence Canada, 2007.

———. *Canada Command Direction for Domestic Operations: Interim Version V1*. Ottawa: Department of National Defence, 2006.

———. "Canada Command: Operations General." Department of National Defence. http://www.canadacom.forces.gc.ca/daily/archive-opgen-eng.asp (accessed 12 April 2011).

———. *Canada First Defence Strategy*. Ottawa: DND Canada, 2008, http://www.forces.gc.ca/site/pri/first-premier/index-eng.asp (accessed 06 November 2010).

———. "Land Forces Knowledge Management System: Op POSEIDON 1-09." Department of National Defence. DND Intranet http://kms.kingston.mil.ca/kms/CentralInstance.aspx?Type=Rotation&Id=586 (accessed 16 April 2011).

———. "Land Forces Knowledge Management System: Op POSEIDON 1-10." Department of National Defence. DND Intranet http://kms.kingston.mil.ca/kms/CentralInstance.aspx?Type=Rotation&Id=587 (accessed 16 April 2011).

———. "Land Forces Knowledge Management System: 2010-0026-J2 INT Op POSEIDON After Action Review." Department of National Defence. DND Intranet http://kms.kingston.mil.ca/kms/CentralInstance.aspx?Type=Feedback&Id=227 (accessed 16 April 2011).

———. "Land Forces Knowledge Management System: JTFP Contingency Plan POSEIDON Information Brief." Department of National Defence. DND Intranet http://kms.kingston.mil.ca/kms/FileView.aspx?Id=3248&UniqueParameter=634387305394488546 (accessed 16 April 2011).

———. *Marine Security Operations Centres Project: Detailed Operational Requirements*. Ottawa: Government of Canada, 2010.

———. *Marine Security Operations Centres Project: Concept of Operations for Initial Operational Capability (IOC)*. Ottawa: Government of Canada, 2007.

———. "National Defence and the Canadian Forces - JTF2: National Counter-Terrorism Plan." http://www.jtf2.forces.gc.ca/ct/index-eng.asp (accessed 27 February 2011).

Canada, Fisheries and Oceans Canada. *Canadian Coast Guard: Maritime Security Framework*. Ottawa: Maritime Security, Canadian Coast Guard, Fisheries and Oceans Canada, 2010.

Canada, Integrated Threat Assessment Centre. *Integrated Threat Assessment Centre Website: Key Partners*. Ottawa: Government of Canada, 2011, http://www.itac-ciem.gc.ca/prtnrs/index-eng.asp (accessed 16 January 2011).

———. "Terrorism in Canada." Integrated Threat Assessment Centre. http://www.itac-ciem.gc.ca/thrt/cnd-eng.asp (accessed 16 April 2011).

Canada, Privy Council Office. *Securing an Open Society: One Year Later - Progress Report on the Implementation of Canada's National Security Policy*. Ottawa: Government of Canada, 2005.

———. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Government of Canada, 2004, http://www.publicsafety.gc.ca/pol/ns/secpol04-eng.aspx (accessed 13 July 2010).

Canada, Public Safety Canada. *Federal Emergency Response Plan*. Ottawa: Government of Canada, 2009.

———. *An Overview of Canada's Counter-Terrorism Arrangements*. Ottawa: Government of Canada, 2003.

Canada, Royal Canadian Mounted Police. "Marine Security Operations Centres." Government of Canada. http://www.rcmp-grc.gc.ca/mari-port/msoc-cosm-eng.htm (accessed 04 February 2011).

———.*Royal Canadian Mounted Police Website: Integrated National Security Enforcement Teams*. Ottawa: Royal Canadian Mounted Police, 2010, http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm (accessed 16 January 2011).

Canada, Transport Canada. "Transportation Security." Government of Canada. http://www.tc.gc.ca/eng/policy/report-aca-anre2006-4b_security-eng-1551.htm (accessed 05 February 2011).

Canadian Broadcasting Corporation. "In Depth Maher Arar: The Cases of Almaki, Nureddin and El Maati." Canadian Broadcasting Corporation. http://www.cbc.ca/news/background/arar/torture-claims.htm (accessed 16 April 2011).

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

Gravel, LCdr Paul. *The Canadian Forces and Inter-Departmental Cooperation Toward Domestic Security: Tear Down those Walls!*. Toronto: Canadian Forces College Joint Command and Staff Programme New Horizons Paper, 2009.

Hebert, Adam J. Noble Eagle without End. *Air Force Magazine,* February 2005. 42, http://www.norad.mil/News/2007/061907.html (accessed 06 February 2011).

Kreisher, Otto. The Years of Noble Eagle. *Air Force Magazine,* 19 June 2007. 50, http://www.norad.mil/News/2007/061907.html (accessed 06 February 2011).

Parliament of Canada. . *Canadian Security Intelligence Service Act. 1984, c. 21, s. 1.* Ottawa: Department of Justice, 2010, http://laws.justice.gc.ca/PDF/Statute/C/C-23.pdf (accessed 17 November 2010).

———. *National Defence Act. R.S., c. N-4, s. 1. Consolidated*. Ottawa: Department of Justice, 2011, http://laws.justice.gc.ca/PDF/Statute/N/N-5.pdf (accessed 06 March 2011).

———. *Privacy Act 1980-81-82-83, c. 111, Sch. II "1". Consolidated*. Ottawa: Department of Justice, 2010, http://laws.justice.gc.ca/PDF/Readability/P-21.pdf (accessed 17 November 2010).

———. *Security of Information Act. R.S., 1985, c O-5, s. 1; 2001, c. 41, s. 25. Consolidated*. Ottawa: Department of Justice, 2011a, http://laws.justice.gc.ca/PDF/Statute/O/O-5.pdf (accessed 09 February 2011).

———. *Security Offences Act. 1984, c. 21, s. 56. Consolidated*. Ottawa: Department of Justice, 2011b, http://laws.justice.gc.ca/PDF/Statute/S/S-7.pdf (accessed 06 March 2011).

Penn, Everette B., ed. *Homeland Security and Criminal Justice: Five Years After 9/11*. New York: Routledge, 2008.

Quiggin, Thomas. *Seeing the Invisible: National Security Intelligence in an Uncertain Age*. Danvers: World Scientific Publishing Co. Pte. Ltd., 2007.

Renuart, General Victor. *Remarks by General Victor Renuart Commander of NORAD and NORTHCOM to the Heritage Foundation*. Colorado Springs: United States Northern Command, 2008.

Roy, Jeffery. "Security, Sovereignty, and Continental Interoperability: Canada's Elusive Balance." *Social Science Computer Review* 23, no. 4 (Winter 2005).

Russell, Ivan. "Intergovernmental Cooperation and Cooperation within Canadian Disaster and Emergency Management: What Makes it Work?" Masters of Arts, Royal Roads University, 2009.

Salt, LCdr James. . *The Whole-of-Government Approach to Maritime Information Sharing: Reality Or Fiction?*. Toronto: Canadian Forces College Joint Command and Staff Programme New Horizons Paper, 2008.

Schilling, William R., ed. *Nontraditional Warfare: Twenty-First-Century Threats and Responses*. Washington: Brassey's, Inc., 2002.

Selbie, Colonel J. J. "Homeland Security: A Canadian Perspective." Carlisle Barracks: U.S. Army War College, 2001.

Thomson, Michael H. and Barbara D. Adams. *Network Enabled Operations: A Canadian Perspective*. Guelph: Humansystems Incorporated, 2005.

United States, National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton And Company, 2004.

Wilson, James Q. *Bureaucracy: What Government Agencies do and Why they do it*. Jackson: Basic Books, 1989.