

the Importance of Information Sharing to the Interdepartmental Security Approach

In the context of national security, it has been made clear that the terrorist has changed the battlespace. This is particularly notable in the realm of Maritime Security. Since the struggle against international terrorists doesn't focus on sovereign states in particular, the battlespace becomes equally local and federal, domestic and international, sensational and commonplace. We know that, like guerilla warriors, *terrorists own the timeline* – it's up to non-terrorists to disrupt that timeline. Since the battlespace is informational and ephemeral, it is not through over-powering physical means that we will neutralize their threat – it is through information superiority. Brains, not brawn. The emphasis in the new battlespace must necessarily be placed on finding the terrorist and understanding his plan before he executes.

Governments have traditionally had four major functional areas relating to national security: law enforcement; intelligence; infrastructure protection; and defence. The departments who have responsibility for these functional areas each have legislated mandates that bestow a certain specific authority to carry out their tasks. Thus, in the past, law enforcement agencies could very easily work independently from security intelligence agencies; the military could concentrate on external threats and rarely meet with departments with domestic concerns; and infrastructure protection or health officials could work in isolation ensuring that their specific tasks were successfully achieved.

Government organization for maritime security was no different. Individual fleets of government ships put to sea under separate mandates; independent surveillance effort over large ocean spaces has been largely uncoordinated; and collaboration took place in reaction to specific activities (usually criminal) that were already underway. Integration has always been a challenge.

In order for governments to respond to this challenge, they have to comprehend the new battlespace and react to its changed form.

As American security expert and author, Bruce Berkowitz, states, today's terrorist organizations can "organize themselves in ways that take advantage of geographic, political, and bureaucratic boundaries – that is, they often try to slip between the cracks where the authority of one intelligence or law enforcement organization ends and another begins." In so doing, the terrorist threat is having the effect of reshaping the response that governments use to counter its attacks.

In order to deal with the blurry and changeable nature of modern threats to security, governments have been forced to break down their traditional stovepipes and integrate their capability. In Canada, the interdepartmental approach has been utilized to make advances towards the desired level of integration. Information-sharing is the foundation for this improved capability.

Interdepartmental Initiatives

Since 9/11, in Canada there have been a number of interdepartmental initiatives proposed and commenced that deal with "integration," "collaboration," and "information-sharing." The current major integration projects are: the Maritime Information Management and Data Exchange (MIMDEX) system (sponsored by DND for the Interdepartmental Marine Security Working Group (IMSWG)); the Integrated Justice Initiative (IJI) which incorporates the work of the Interoperability Committee under the department of Public Safety and Emergency Preparedness (PSEPC); and the Integrated Threat Assessment Centre (ITAC) which is housed in the Canadian Security Intelligence Service (CSIS) but is also linked to the National Security Advisor in the Privy Council Office. The Government Operations Centre (GOC) and the Maritime Security Operations Centres (MSOC) are examples of operational environments that are being reconfigured to manage the information fused together by these new integration projects. Each of these projects is based on the idea that information-sharing in a community network will bring us toward an integrated government security system – a theme that figures prominently in the National Security Policy (NSP).

Challenges to Integration

The Auditor General has asserted that the importance of intelligence in the fight against terrorism cannot be overstated and that coordinating the efforts of the agencies involved is critical to their overall effectiveness. These assertions are now broadly accepted. Yet, the current arrangements for sharing information between departments continue to be constrained by the lack of legal clarity in individual departmental mandates to share information as collaborative communities. Put bluntly, the security-oriented departments and law enforcement departments are reluctant to share their information in an integrated fashion with other departments because the current laws place them in a position of high legal risk when certain information is shared. The legal risks associated with sharing in an integrated fashion arise primarily from the

Privacy Act and the Canadian Charter of Rights and Freedoms. Of the dimensions of interoperability (Technical, Semantic, Cultural, Inter-community, and Legal), it is the legal dimension that is most closely linked to information-sharing. While technical, semantic, and cultural changes can improve information-sharing to a certain extent, it is legislative change that will provide the "lawful authority" to share security information in an integrated fashion.

In the Report of the Auditor General of Canada – March 2004, one of the two overarching themes of the audit was "the co-ordination of intelligence among departments and agencies and their ability to provide adequate information to enforcement personnel." The main recommendation in this theme area was "the Privy Council Office and Public Safety and Emergency Preparedness Canada, with the assistance of the Department of Justice Canada and the Treasury Board Secretariat, should further examine and

about MIMDEX in the maritime security community delved into legal aspects of information sharing and found that sharing in an integrated fashion requires limits and safeguards with respect to collection, retention, and sharing of data that will inform the reasonable nature of the lawful authority. It was pointed out that legal risks are most serious if the integrated system is used for general law enforcement. Risks are lower if the data is shared for regulatory purposes. It was concluded that some degree of legislative change would likely be required to satisfy the requirements of the Charter and the Privacy Act if MIMDEX was to achieve optimum utility.

Way Ahead

An initiative is needed to bring central agencies, departments, security practitioners and legal officers together to produce a strategic guide to integrated information-sharing in government which strives for

Operations Centre with its interconnection to the various levels of government, from first responder to top officials in Ottawa.

Conclusion

The healthy friction that exists between civil rights and national security must be understood by Canadians. If interdepartmentalism in the context of integrated government is to become fully effective, Canada must engage more fully in the debate over the need to challenge existing legislation with regard to information-sharing between security partners inside government and out. The passing of the Anti-Terrorism Bill and the Public Safety Act demonstrates that this debate has commenced. However, the content of these laws also proves that Canada is approaching the matter in a piecemeal fashion that treats individual problems in a one-off manner. There has not yet been a strategic-level debate on the fundamen-

To deal with the blurry and changeable nature of modern threats to security, governments have been forced to break down their traditional stovepipes and integrate their capability.

provide guidance on the sharing of information among government departments and agencies while balancing privacy concerns with national security concerns."

The capability of government departments to share information and collaborate with other departments, civilian agencies, and other countries' organizations has been found wanting. The Cold War propensity to maintain a rigid, compartmentalized flow of information in organizational stovepipes has hampered national ability to integrate intelligence and information sharing efforts between departments who are outside the traditional public safety framework, yet crucial to connecting the dots in the new battlespace.

Even with recent improvements, the nature of information to be shared, the purpose for its initial collection, and the circumstances and context in which it will be shared can cause a high level of legal risk under the present legal framework – particularly in the realms of law enforcement and prosecution. In 2003, a debate

the required balance between civil liberties and national security in the current strategic threat environment. The Public Safety and Security Information Sharing and Interoperability Project launched in April 2004 promises to provide the Canadian government with a framework and strategy to better integrate information systems amongst all relevant organizations. This project is in its infancy and is positioning for action across government. With central agency direction and legal counsel, this initiative could bear valuable fruit.

It is essential in this process to anchor the proposed framework of information sharing and interoperability on the pillars of the NSP such that the public safety and security network corresponds to the foundation of common, agreed-upon strategy. The practical application of information sharing on government machinery will find its theoretical hub in the National Emergency Response System (NERS) and its physical focal point in the Government

tal issue of information-sharing that covers the full range of community concerns – both national security and civil rights. The preventive, "integrated" approach to national and maritime security that is envisioned in the National Security Policy will not be optimized unless such a debate occurs. And the debate must include an intense focus on information-sharing in the context of national security. Collaboration through information-sharing in interdepartmental communities will be limited in Canada unless this debate is undertaken in a strategic fashion and legislation is enacted to convey the results of the debate. **FL**



As Commanding Officer of HMCS Fredericton in 1999, Capt(N) Peter Avis participated in SNFL deployments and major NATO exercises. Recently, Capt(N) Avis has assumed the position of Director Maritime Policy and was transferred to the advanced training list.