Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Study on Persistent Monitoring of Maritime, Great Lakes and St. Lawrence Seaway Border Regions

Dr. John Leggat,
CFN Consultants

Tatyana Litvak,
AUG Signals

Ian Parker,
CFN Consultants

Dr. Abhijit Sinha,
AUG Signals

Serge Vidalis,
Blue Force Global

Albert Wong,
AKW Global Enterprises

Scientific Authority:
Pierre Meunier
DRDC Centre for Security Science

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Centre for Security Science

Canada

DRDC CSS CR 2011-28

December 2011

Study on Persistent Monitoring of Maritime, Great Lakes and St. Lawrence Seaway Border Regions

Prepared by:

Dr. John Leggat,
CFN Consultants

Dr. Abhijit Sinha,
AUG Signals

Tatyana Litvak,
AUG Signals

Serge Vidalis,
Blue Force Global

Ian Parker,
CFN Consultants

Albert Wong,
AKW Global Enterprises

Scientific Authority:
Pierre Meunier
DRDC Centre for Security Science

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence Research and Development Canada.

Defence R&D Canada – Centre for Security Science

Contractor Report

DRDC CSS CR 2011-28

December 2011

Principal Author

Original signed by [Principal Author]

Tatyana Litvak

Marketing and Special Projects Manager

Approved by

Original signed by [Approved By Name]

Jack Pagotto

[Approved By Position/Title]

Approved for release by

Original signed by [Released By Name]

[Released By Name]

[Released By Position/Title]

Abstract

This study employed a systematic and interdisciplinary analysis to better understand the current and arising capability gaps relating to the security of the maritime, Great Lakes and St. Lawrence Seaway (GLSLS) border regions. It examined strategies and technological approaches for persistent small vessel surveillance, and evaluated potential solutions that would address the identified gaps. The approach included a review of the technical literature, a qualitative survey of stakeholders, an analysis of requirements and resulting gaps, and an assessment of potential solutions enabled by new technological approaches and operational procedures.

This evaluation of a variety of potential systems, technologies and techniques resulted in a roadmap designed for a Surveillance, Intelligence, and Interdiction solution which allows persistent surveillance and the accurate, robust and timely identification of small vessels – compliant and non-compliant, while allowing the efficient operation of our maritime border areas.

Résumé

Cette étude se fonde sur une analyse systématique et interdisciplinaire visant à mieux comprendre les écarts de capacité actuels et en voie de manifester dans le domaine de la sécurité des régions frontalières des Grands Lacs et la voie maritime du Saint-Laurent(GLVMSL). Dans le cadre de l’étude, on a examiné les stratégies et les approches technologiques de surveillance permanente au moyen de petits navires, en plus d’évaluer les solutions qui permettraient de combler les écarts recensés. L’approche consistait à examiner la documentation technique, à faire une enquête qualitative auprès des intervenants, une analyse des besoins et des écarts qui en découlent, ainsi qu’une évaluation des solutions que pourraient apporter de nouvelles approches technologiques et modalités opérationnelles.

Cette évaluation d’un éventail de systèmes, technologies et techniques possibles a donné lieu à la création d’une feuille de route menant à l’adoption d’une solution de surveillance, de renseignement et d’interdiction permettant l’exercice d’une surveillance permanente et l’identification rapide, exacte et fiable des petits navires, conformes ou non, ainsi que la gestion efficace de nos frontières maritimes.

Executive Summary

Study on Persistent Monitoring of Maritime, Great Lakes and St. Lawrence Seaway Border Regions DRDC CSS CR 2011-28

Dr. J Leggat; Tatyana Litvak; Ian Parker; Dr. Abhijit Sinha; Serge Vidalis; Albert Wong; December 2011

The final report of Asymmetric Threat Mitigation in the Great Lakes, St. Lawrence Seaway and Maritime Ports and Inshore Waters provides an in-depth analysis of capability gaps associated with the threat from small vessels. With an emphasis on persistent surveillance, the report outlines potential strategies for mitigating the threat posed by small vessels, within the constraints of operational, organizational and technological challenges.

To provide context to the report, Section 1 starts with a brief overview of the study scope and outlines the approach taken during the study execution. Section 2 presents a discussion of the small vessel issues facing Canada and defines the small vessel surveillance problem. Following this background overview, the report goes on to describe the Canadian maritime regulations and mandates, and the deficiencies in these regulations pertaining to small vessels (Section 3).

Section 4.1 provides an overview of the many stakeholders with a vested interest in effective small vessel threat mitigation. Section 4.2 presents a qualitative analysis of the existing operational, strategic and technological small vessel threat mitigation capabilities and the present concerns expressed through stakeholders' feedback collected specifically for the purposes of this study. The report then continues to describe the various Canadian initiatives undertaken in the past decade to enhance operational maritime and naval capabilities, and draws attention to the fact that no significant efforts or investments were made to counter the emerging asymmetric threat despite its growing presence, thus increasing Canadian vulnerability to the dangers presented by small vessels (Section 5).

Sections 6 draws comparisons between US initiatives and mandates specifically focused on emerging maritime threats in the modern, post 9/11 era, and suggests that Canada's current difficulty in playing the role of an equal partner in combating illegal activities in the US-Canada border regions could potentially place limitations on trade and other cross-border activities between the two countries. Section 7 presents further examples of international approaches to asymmetric threat mitigation and outlines the implications those have on Canada's relative ability to effectively monitor its shores and waters.

Section 8 draws on the needs identified via primary and secondary research discussed in Sections 2-7 to elaborate on short and long term requirements that will enable the development of the necessary mitigation and response capabilities to counter the emerging small vessel threat. Section 9 provides an assessment of a variety of sensor technologies that may be used to provide maritime security stakeholders with the necessary tools to meet their short and long term needs

and categorizes these in terms of their ability to mitigate the small vessel threat in the context of specific geographic regions. Section 10 lists software technologies that can enhance persistent small vessel surveillance and reviews of several commercially available software products, none of which offers a comprehensive solution to the small vessel surveillance problem.

The Capability Gaps Identification section (Section 11), when combined with the organizational, operational and technological challenges identified in the course of the study, produces a focused summary of the most important capability gaps that pertain to the surveillance and mitigation of the small vessel threat.

Section 12 of the report describes the study's main output – a technological solution for small vessel persistent surveillance that factors in the technical, operational and mandate-related challenges of the Canadian maritime security landscape. To illustrate the solution's application in operational scenarios, case studies are presented in Section 12.5, outlining how the described multi-sensor surveillance solution will enhance Canada's ability to prepare for, and respond to, high consequence public events arising from the small vessel threat.

The report concludes with the presentation of a capability roadmap that describes the steps and timeframes necessary to operationalize the technology (Section 12.6). Because technology is only part of a small vessel persistent surveillance approach, the concluding section also summarizes the legal and policy implications and highlights the ongoing issues associated with information sharing among the maritime security stakeholders (Section 12.7). Finally, in Section 13 a brief analysis is presented on how capability gaps could be further addressed via legislative changes – a long term vision for Canadian maritime security.

Sommaire

Étude sur la surveillance maritime des persistants, des Grands Lacs et du Saint-Laurent Régions frontaliers voie maritime DRDC CSS CR 2011-28

Dr. J Leggat; Tatyana Litvak; Ian Parker; Dr. Abhijit Sinha; Serge Vidalis; Albert Wong; Décembre 2011

Le rapport final sur l'atténuation des menaces asymétriques dans les Grands Lacs, la Voie maritime du Saint-Laurent, les ports maritimes et les eaux côtières présente une analyse approfondie des écarts de capacité associés à la menace posée par les petits navires. Mettant l'accent sur la surveillance permanente, le rapport propose des stratégies en vue d'atténuer la menace que représentent les petits navires, dans les limites imposées sur les plans opérationnel, organisationnel et technologique.

Voici un survol du contenu du rapport. D'abord, la section 1 présente un bref aperçu de la portée de l'étude et décrit l'approche adoptée pour son exécution. La section 2 porte sur l'enjeu que constituent les petits navires pour le Canada et définit le problème que pose la surveillance des petits navires. Suite à la présentation du contexte, le rapport énonce les règlements et les mandats du Canada dans le secteur maritime, ainsi que les lacunes que ceux-ci comportent en ce qui a trait aux petits navires (section 3).

À la section 4.1, on présente un aperçu des nombreux intervenants intéressés par l'atténuation efficace de la menace posée par les petits navires. La section 4.2 contient une analyse qualitative des capacités opérationnelles stratégiques et technologiques actuelles en matière d'atténuation de la menace posée par les petits navires. Elle expose également les préoccupations exprimées par les intervenants dans le cadre d'un sondage effectué aux fins de la présente étude. Le rapport décrit ensuite les diverses initiatives prises par le Canada au cours de la dernière décennie en vue d'améliorer ses capacités maritimes et navales opérationnelles, et attire l'attention sur le fait qu'aucun effort ou investissement significatif n'a été fait dans le but de contrer la nouvelle menace asymétrique bien que celle-ci ne cesse de grandir. Le Canada se trouve par conséquent de plus en plus vulnérable aux dangers que représentent les petits navires (section 5).

La section 6 établit des comparaisons entre les initiatives et les mandats états-uniens se concentrant tout particulièrement sur les nouvelles menaces maritimes de l'ère moderne, après les événements du 11 septembre 2001, et laisse entendre que la difficulté qu'éprouve le Canada à agir en tant que partenaire à part égale dans la lutte contre les activités illicites aux frontières canado-américaines pourrait nuire au commerce et à d'autres activités transfrontalières entre les deux pays. La section 7 fournit d'autres exemples de méthodes d'atténuation de la menace asymétrique adoptées par d'autres pays et décrit les incidences qu'ont ces méthodes sur la capacité relative du Canada de surveiller efficacement ses rives et ses eaux.

La section 8 porte sur les besoins recensés par le biais de la recherche principale et secondaire dont il est question aux sections 2 à 7 en vue de préciser les besoins à court et à long terme

desquels on s’inspirera pour élaborer les capacités d’intervention et d’atténuation nécessaires afin de contrer la nouvelle menace posée par les petits navires. À la section 9, on fait l’évaluation de diverses technologies de capteurs qui pourraient être utilisées pour fournir aux responsables de la sécurité maritime les outils nécessaires pour répondre à leurs besoins à court et à long terme et les catégoriser en fonction de leur capacité d’atténuer la menace présentée par les petits navires dans certaines régions géographiques. La section 10 offre une liste de technologies logicielles pouvant améliorer la surveillance permanente des petits navires et examine plusieurs produits logiciels disponibles dans le commerce, mais aucune de ces technologies ne permet de régler tout à fait le problème de la surveillance des petits navires.

La section sur le recensement des écarts de capacité (section 11), combinés avec les difficultés d’ordre organisationnel, opérationnel et technologique relevées au cours de l’étude, contient un sommaire axé sur les plus importants écarts de capacité liés à la surveillance et à l’atténuation de la menace posée par les petits navires.

À la section 12 du rapport, on trouve la description du produit principal de l’étude – une solution technologique pour assurer la surveillance permanente des petits navires qui prend en compte les défis techniques, opérationnels et liés au mandat présents dans le paysage de sécurité maritime du Canada. Dans le but d’illustrer l’application de la solution dans des scénarios opérationnels, des études de cas sont présentées à la section 12.5, démontrant comment le système de surveillance à capteurs multiples améliorera la capacité du Canada à se préparer à faire face à des événements publics susceptibles d’avoir de graves conséquences qui pourraient découler de la menace posée par les petits navires.

En conclusion, le rapport présente une feuille de route des capacités décrivant les étapes et les délais nécessaires pour opérationnaliser la technologie (section 12.6). Comme la technologie fait uniquement partie d’une approche de surveillance permanente des petits navires, la conclusion résume également les incidences d’ordre juridique ou stratégique et met en lumière les problèmes actuels liés au partage de l’information entre les responsables de la sécurité maritime (section 12.7). Enfin, à la section 13, on peut lire une courte analyse démontrant d’autres moyens de combler les écarts de capacité, notamment en modifiant la législation – une vision à long terme pour la sécurité maritime du Canada.

Table of contents

List of figures

List of tables

Acknowledgements

This work was supported by the Defence Research and Development Canada Centre for Security Science Public Security Technical Program (PSTP 02-341BTS) and led by Dr. Andre Brandao, Communication Research Centre Canada.

The authors of this report would also like to thank the participants who provided commentary and reviewed earlier versions of this document for their helpful insights and suggestions, we have incorporated these comments to the best of our ability, and any errors are ours alone. Alphabetically: Peter Berry of Windsor Port Authority, Steve E Brown of GL-MSOC, S/Sgt. Dave Cassady of Windsor Police Services, Commander Mark J. Chupick of Canadian Navy, LCdr Ian Cook of MSOC East, LCdr Tom Fredericks of MSOC East, Ron Funk of DND, Wynford Goodman of IHMA, Andrea Heba of Port Metro Vancouver, Dave Hoto of GL-MSOC, Steve Hughes of DRDC, Shane Kyle of GL-MSOC, George J. Lepine of TC, Xia Liu, Abir Mukherjee, Gordon Nash of NRPS, Tim Nohara of Accipiter Radar, Gary Paulson of Prince Rupert Port Authority, Brianne Pozzobon of GL-MSOC, John Richard of MSOC East, Dan Riley of TC, Sam Ryan of DFO, Brad Schlorff of OPP, Commodore Daniel Sing of DND, LCdr Kevin Stewart of MSOC West, Alexandra Tsourkis, Dave Weston of GL-MSOC, Cst. Adam Young of Windsor Police Services.

1. Introduction – Study Approach

With the emergence of asymmetric threats characterized by unpredictable military or paramilitary operations, smaller vessels have become a medium of choice for adversaries operating on the high seas, coastal areas or in-land waterways. The transition from regular to asymmetric warfare requires new approaches including the adaptation of current Surveillance, Intelligence, and Interdiction (SII) capabilities to enable efficient detection, identification and tracking of small craft before they can breach the defensive layers of ships, ports or shore facilities. Small craft are also the platform of choice in many instances for organized crime. Smuggling activities, whether they involve narcotics, weapons or people, typically make use of small craft because they are unregulated and hard to detect.

This study employed a systematic and interdisciplinary analysis to better understand the current and arising capability gaps relating to the security of the maritime, Great Lakes and St. Lawrence Seaway (GLSLS) border regions. It examined strategies and technological approaches for persistent small vessel surveillance, and evaluated potential solutions that would address the identified gaps. The approach included a review of the technical literature, a qualitative survey of stakeholders, an analysis of requirements and resulting gaps, and an assessment of potential solutions enabled by new technological approaches and operational procedures.

The reviews of the open literature and discussions with stakeholders (both military and civilian from all levels of government) provided extensive information on the nature of the existing and emerging small vessels threat at maritime borders and along the GLSLS. The subsequent identification of persistent surveillance requirements and capability gaps provided deep understanding of the challenges associated with small boat surveillance and insights into what options are available to Canada to detect and interdict illegal activities. The surveillance systems considered included those employing ground-based, space-based, underwater, and airborne sensors and advanced signal processing and information fusion techniques. Each approach was reviewed and categorized according to its effectiveness in the detection, tracking and identification of small vessels and ultimately in its ability to mitigate the small vessel threat in the context of specific maritime environments.

The analysis identified emerging systems that would be able to improve the national ability to mitigate the small vessel threats. The assessment of Technology Readiness Levels and the evaluation of impacts for the identified technologies vis-à-vis legal, cultural, privacy and ethical concerns led to the development of a framework for a multi-sensor persistent surveillance system, including both sensor and processing components. The framework included the steps and the timeframe needed to operationalize study outputs. Border management and law enforcement agencies as well as DND and non-law enforcement stakeholders were briefed on study findings and key conclusions relevant to their mandates.

This evaluation of a variety of potential systems, technologies and techniques resulted in a roadmap designed for a Surveillance, Intelligence, and Interdiction solution which allows persistent surveillance and the accurate, robust and timely identification of small vessels – compliant and non-compliant, while allowing the efficient operation of our maritime border areas.

2. Defining the Small Vessel Threat

The small vessel threat to Canadian and US national security has existed for many decades with its roots in the contraband smuggling, primarily of alcohol, during the Prohibition, and most recently tobacco, within the joint waterways between both countries. The threat evolved during the middle part of the 20th century, witnessing the migration of Cuban refugees, then Haitian refugees to the US. By the 1980s, the influx of narcotics from South and Central American countries turned the US Gulf states into a battle zone. Counter-smuggling operations extended to Canada in the last 20 years and small vessels have continued to pose growing threats to both nations with the increase in trafficking of narcotics and weapons and the emergence of human smuggling by organized crime groups.

Today's threat includes the trafficking of contraband, narcotics and weapons, human trafficking, transportation of terrorists / dangerous persons, and the potential of smuggling weapons of mass destruction (WMD). The terrorist risk manifests itself in several forms, including: transportation of Weapons of Mass Destruction (including chemical, biological, radiological, nuclear and explosives), the use of small vessels to deliver waterborne improvised explosive devices, for the smuggling of wanted persons, as well as a platform for standoff weapons and attacks.

Emerging threats are being signaled by events in other countries such as Colombia and Mexico where there is a growing use of submersibles or miniature submarines, partially submerged vessels (presenting a small radar cross section) and high-powered low freeboard vessels (Pangas). The latter is an emerging practice currently employed by Mexican drug cartels delivering contraband in the San Diego, California, area. Finally, the use of float planes by criminals is a risk that is not traditionally considered as a maritime security threat.

The threat to Canada's maritime borders has increased. New technologies are available to and utilized by both criminal elements and would-be terrorists. Terrorism is top of mind for governments because of the rise of global terror related to events that pre-date 2001. The threat of foreign non-state actors executing a sea-borne attack is very low; however, that posed by radicalized ideologues residing in Canada or the US is more likely. The existence of such a threat underscores the importance of intelligence operations, enforcement, patrol operations and surveillance of economic, environmental, public and critical infrastructure sites that could be targeted.

In the area of the Great Lakes and St. Lawrence River, there are an estimated 6.2 million small boats, not including small commercial vessels. The area has an estimated 200,000 plus kilometres of Canadian shoreline, and 3.7 million square kilometres of marine surface area [GLC2007]. Therefore, concerns with small vessels are several particularly when considering the vastness of area that must be monitored and patrolled.

3. Regulation Overview

In Canada, the creation of policy and development of regulation regarding transportation policies is determined by Transport Canada (TC). Within TC, the Marine Security Directorate is responsible for the development of policies, legislation, regulations, standard procedures and guidance to marine transportation security, in addition to enforcement and compliance measures. Within its mandate, the Marine Security Directorate is responsible for the promulgation of Canadian Marine Transportation Security Regulations (MTSR) - regulations that have been invigorated by the adoption of the International Ship and Port Facility Security Code (ISPS) in 2004. Compliance of the MTSRs is executed by Transport

Canada inspection teams that also operate jointly with US Coast Guard inspectors on shared Canadian / US waterways.

Through Transport Canada, the regulatory requirement to carry AIS came into force in 2005 as set forth in the Additional Requirements section of The Navigation Safety Regulations, pursuant to th*e Canada Shipping Act.* As Canada is a supporter of International efforts with respect to vessel identification and tracking technologies, it also incorporates the policy, legislation and regulatory practices of the International Maritime Organization (IMO), the Safety of Life at Sea Convention (SOLAS), the International Telecommunications Union (ITU), and the Arctic Waters Pollution Prevention Act, among others.

While Canada adheres to all IMO-mandated AIS carriage requirements, small vessels more than 100 tons (non-SOLAS ship) but less than 500 tons (SOLAS ships), carrying more than 12 persons, engaged on a voyage from a port in one country to a port in another country must comply with the Marine Transportation Security Regulations. However, according to Section 201(2) of the reference, the application of the MTSR "does not apply to pleasure craft, fishing vessels, government vessels or vessels without a crew that are in dry dock, dismantled or laid-up" [DJC2010]. The IMO, meanwhile, mandates that all passenger ships, irrespective of number of passengers must be fitted with AIS.

As such, small vessels operating in Canadian waters are excluded from Canadian Maritime Transportation Security Regulations. However, small vessel operators are subjected to four primary regulations that include: port of entry reporting in accordance with Canadian Border Services Agency requirements, boater safety in accordance with Canadian Coast Guard vessel operations, licensing in accordance with Transport Canada regulations, and operations of a motor vessel / vehicle in accordance with the Canadian Criminal Code and Provincial Motor Vehicle Acts, as they apply to impaired driving, criminal activities and accidents. Small vessels operating in Canadian coastal waters, inland waters and rivers are unregulated with respect to maritime security matters.

This model of Marine security, the **Diffused Responsibility and Jurisdiction Approach**, where there is a central policy authority, Transport Canada, but there is no one central planning, coordination and execution authority. Other models that exist internationally include the **Navy as a Coast Guard Approach**, where the Navy, with control of a Coast Guard, retains the single responsible federal agency but generally dilutes the Navy's traditional rolls of combat, sovereignty and interdiction. This model is generally used in the third world as well as Australia and some European Nations. Most nations that use this model, with the exception of Australia, have small coastlines.

Finally, the approach where a **Single Federal Agency** or authority is assigned both the responsibility and the accountability for marine security which includes small boats/vessels exists in countries such as used the US, through the USCG and Italy through the Guardia Costiera. This model allows for centralized planning and coordination with other federal agencies as well as centralized implementation, and generally has proven to be the very effective in planning, coordination and execution against the marine threat, including the small boat/vessel threat.

4. Maritime Security Stakeholders

4.1 Stakeholder Overview

Maritime security stakeholders vary in jurisdiction and operational functions. The following captures the current operational responsibilities and jurisdictions of each organization within the marine security program in Canada:

A. **Royal Canadian Mounted Police (RCMP)** – Possesses specialized integrated teams for marine security operations, however, these assets are often minimally manned and equipped, are required to assume other responsibilities due to manpower shortages, unable to manage multiple caseloads or extend investigative efforts due to manning and budgetary constraints. Marine assets are very limited and are primarily used as mobile police detachments, reducing their ability to concentrate of maritime security within domestic waters. In the GLSLS, the RCMP retains the mandate for border integrity, whereas the Ontario Provincial Police (OPP) and Sûreté du Québec (SQ) are the police of jurisdiction and will support if required. In general, the RCMP is ill equipped and understaffed to effectively perform this function. Area of jurisdiction is national.

B. **Department of National Defence (DND)** – Possesses the technological and operational expertise for conducting marine security operations, however, lacks the enforcement and investigative capabilities. As with the RCMP, DND suffers from human resource and financial shortages, and is operationally overextended due to the ongoing war effort in Afghanistan. DND is very well positioned to lead the Strategic and Tactical aspects of marine security operations but is unable to do so due to the above noted matters, inclusive of legislation limitations. However, under the domestic operations umbrella of Canada Command, DND has provisions to expand its role if required to assist Other Government Departments (OGD). Doctrinally, DND is best suited for the introduction and deployment of new technologies aimed at marine security efforts. Area of jurisdiction is Canadian territorial waters to Economic Exclusive Zone.

C. **Canada Border Services Agency (CBSA)** – CBSA is a progressive organization that in the last several years has embraced new technologies to enhance their operational mandate. From a maritime element, their primary mandate is the security of Canadian Ports of Entry. The specific threat of concern for the CBSA is radiological detection, subsequently followed by other hazardous materials and cargo, human smuggling, contraband, revenue and taxation. Area of jurisdiction is national yet specific to ports of entry.

D. **Canadian Coast Guard (CCG)** – The CCG, an organization under the Department of Fisheries and Oceans (DFO), does not possess the mandate to participate in marine security operations except in support of the RCMP or OGD. CCG capabilities exist primarily in its fleet of vessels, therefore possessing the ability to support tactical operations, surveillance, intelligence collection, reporting functions, and vessel traffic management. As an organization that possesses marine expertise throughout Canada and operates various types of vessels, the CCG could be restructured to lead the maritime security effort in Canada. However, this would require extensive doctrinal change, legislative changes, extensive training and equipping of vessels and personnel, yet the CCG possesses the necessary maritime skills and motivation. Area of jurisdiction in national including Pacific, Atlantic and Arctic.

E. **Canadian Security Intelligence Service (CSIS)** – Providers of support services in intelligence collection, analysis and dissemination. The area of jurisdiction is national with international networks.

F. **Port Authorities** – Responsible to the Directorate of Marine Security, Transport Canada. Primarily concerned with compliance of MTSRs within their port of jurisdiction. Operations are limited to physical security of the authority’s properties utilizing uniformed security patrols, access control systems, CCTV, surface radar (not all locations), and patrol boat (not all locations). Support to law enforcement is provided upon request. Area of jurisdiction remains within the confines of the authority’s property and area of operation.

G. **Provincial and Municipal Law Enforcement** – Law enforcement agencies possess limited capabilities in the marine environment, primarily in the form of small boats, dive teams and emergency response teams. As border integrity is not in their jurisdiction (rather it is of the RCMP), they support such operations as requested to do so or when incidents develop in the performance of other duties. The danger exists in regions of Canada where there is an overlap of jurisdiction and where incidents may go undetected or not interdicted due to poor communication and or perceptions that the other agency will take action. Specific concerns are within the Great Lakes region where multiple agencies operate within the same geographic area: Windsor, Ont. or Toronto, Ont. where there exists municipal, provincial and federal law enforcement. Areas of jurisdiction limited to municipal or provincial.

H. **Marine Security Operations Centres (MSOC's)** – The primary function of the MSOC's is to enable agencies to work collaboratively on the identification, intent and movement of personnel and cargo in the maritime approaches of Canada. The five core partner agencies (Canada Border Services Agency, Canadian Coast Guard/Department of Fisheries and Oceans, Department of National Defence, Royal Canadian Mounted Police and Transport Canada) work together to collect and analyze intelligence in order to develop a solid and comprehensive Common Operating Picture (COP). All personnel are located in close proximity to one another, which opens up both trust and communication channels. Area of jurisdiction is specific to each geographic area where each MSOC is located: East Coast (led by Navy), West Coast (led by Navy) and Great Lakes (led by RCMP). However, even here representatives still operate 'in silo' to some degree. This is a reflection of the obstacles preventing clear and open communication between stakeholders, some caused by federal legislation, others caused by organizational cultures.

As can be seen above, the tasks of investigation, enforcement, intelligence collection and analysis, command, control, communication, and coordination of assets are fragmented in nature, and as such pose capability vulnerabilities. The fragmented nature of operations creates organizational competition and impedes information flow. Though each stakeholder organization is capable of operating proficiently within its own organization, doctrinal and operational differences reduce the overall effectiveness of joint operations, with the exception of the three MSOC's. The lesson to be drawn from the MSOC's is the effectiveness of joint operations conducted through a 'combined' approach to the mission. Even within the MSOC, however, while the effectiveness of coordination is well demonstrated at the local level, it does tend to deteriorate when issues are addressed at the regional or national levels.

Internationally, another important stakeholder in the Canadian maritime security arena is the US Coast Guard (USCG). The USCG is a military organization within the US Department of Homeland Security with the overall responsibility and accountability for ensuring the safety of the US maritime borders and protecting the maritime economy. With the growing cooperation between Canada and the US on matters of maritime security, this organization becomes an important strategic partner on matters of small vessel surveillance.

4.2 Questionnaire Feedback and Responses

For the purposes of this study, a specially designed questionnaire was distributed to key stakeholders of GLSLS and maritime border regions security, including law enforcement agencies, military and civilian agencies and personnel from all levels of government. Stakeholders were asked to provide information on: The Threat Perception, Current Operational Capabilities and Limitations. The data received was amalgamated and the analysis results can be found in Appendix A. In addition to the questionnaire, select stakeholders were also interviewed in a less formal manner, with questions more targeted toward their specific area of expertise and operations as it relates to the project. A summary of the differences and similarities in the received responses is presented herein:

The respondents to the questionnaire and interview requests provided representation of the West Coast, Maritimes and GLSLS stakeholders. Though each respondent entity operates under a different mandate, all recognize and draw attention to the small vessel threat as an existing and emerging issue that is not regulated by Transport Canada (Marine Transportation Security Regulations – MTSR) nor the ISPS Code (International Ship and Port Security Code).

Stakeholder responses indicate that the greatest concern lies with fibreglass vessels of less than 10 metres in length. These craft could carry contraband or alternatively provide a means for illegal immigrants to enter the country. The vessels normally operate in high traffic areas; they travel at a high speed and are equipped with technology that helps avoid detection by the authorities, hence detecting and identifying these vessels presents a challenge.

With respect to regional differences in threat perceptions, respondents within the Great Lakes region indicated they possess greater concerns with pleasure crafts, whilst the Prince Rupert Port Authority (British Columbia) indicated greater concern with small commercial vessels operating in the border region with Alaska. While the Great Lakes MSOC expressed the greatest overall concern with small vessels, considering the large number of small vessels that operate within that region and expressed terrorism, in the form of damage to critical infrastructure and the resulting potential damage to the economy and trade with the US, as one of the top specific threats that the small vessel posed, the Prince Rupert Port Authority suggested the largest threat to be the use of these vessels in the trafficking of narcotics between both countries, particularly due to the burgeoning marijuana market originating in British Columbia (BC). Additionally, due to the rapid growth and expansion of the Mexican drug cartels, BC law enforcement agencies indicated the presence of cartel traffickers and increased threat of cocaine shipments.

Differences in the perception of the threat and operational capabilities can also be seen within the 3 MSOC's themselves. As mentioned above, the Great Lakes MSOC is mainly concerned with the protection of critical infrastructure, while the coastal MSOC's are more concerned with smuggling and trafficking of goods and people. The coasts are also much better equipped in terms of technology (sensors and software) to detect, identify and track the small vessel, but none report to have all the desired capabilities for complete maritime domain awareness.

Generally speaking, the majority of respondents indicated that they do not feel that the current surveillance capabilities are sufficient to counter the small vessel threat, and that a change is needed to enhance Canada's preparedness to counter this type of attack.

5. Canadian Government Initiatives

Canada's current maritime security program can best be described as a work in progress and non-homogenous with respect to deployed technologies, operational capabilities and perceived threats.

Since the September 2001 attacks on the US, the Government of Canada has invested $7.7 billion to fight terrorism and reinforce public security [TC2010]. Of this amount $60 million was to enhance marine security policy and increase Canadian domain awareness. In 2005, the Government of Canada announced a $300 million, five year plan to enhance the security of the Canadian maritime borders, adding to the $930 million already invested in marine security initiatives across various federal departments [TC2005].

Regrettably, the marine-based threat was at the time poorly understood and efforts to improve the security of marine stakeholder operations resulted in millions of the marine initiative program funding being spent primarily on security fencing, CCTV systems and lighting. Though the program improved land-based security for many operators and port authorities, little has been done to address the seaward side of marine security operations. Additionally, the development of a Threat Risk Assessment matrix to provide realistic consequences based on type and size (i.e. Explosive threat and quantity to calculate damage) of a threat, target and delivery means does not appear to exist. Such a tool would enable marine security agencies to profile potential threat vessels and strategically deploy sensors to provide adequate warning and information for mitigation purposes.

Cohesion of the security program is noticeably evident within the three Marine Security Operation Centres (MSOC). All three are supported by the Department of National Defence, Canadian Border Services Agency, Canadian Coast Guard, Royal Canadian Mounted Police, Canadian Security Intelligence Agency and Transport Canada. Although all these agencies are located in one common establishment, representatives still operate ‘in silo’ to some degree. This is a reflection of the obstacles preventing clear and open communication between stakeholders, some caused by federal legislation, others caused by organizational cultures. These silos also reflect the state of sensor deployments, data collection and dissemination, operational capabilities and enforcement. Perhaps the best manner to describe the limitations of the security program is to suggest that the greater prominence a stakeholder possesses within the organization the greater influence, funding and capabilities one has, and the inverse is true for those stakeholders operating at the regional or local level in remote areas.

The MIMDEX Project, funded through the Marine Security Coordination Fund, was conceived as means of creating a centralized common data repository that would give users access to information on a selective basis. However, due to legal constraints associated with information exchange (similar to the constraints faced today by the MSOCs), as well as the high risk that was associated with the project delivery this initiative was stopped. Similarly, the MARSIE Project of 2005, initiated by DRDC and CF, attempted to improve marine security operations in Canada through the field trials of technologies within a real world scenario using a multi-agency approach. It too, however, did not go far enough to achieve its desired objective.

Many studies advocate the need for advanced technologies in data fusion for the creation of the common operating picture. The National Maritime Domain Awareness Strategy 2020, issued by Transport Canada in 2009 calls for a fully integrated government approach that would clarify responsibilities and strengthen coordination between department, a multi-layer architecture and the creation of an unclassified COP through information fusion. Some projects are beginning to address these requirements, including recent work led by DRDC Atlantic that aims at determining the optimal sensor data fusion network to track small vessels in harbour environments, principally through anomaly detection [Hammond2011]. Another PSTP project led by the Royal Canadian Mounted Police and executed by Accipiter Radar examined the feasibility of surveillance of the GLSLS region using an advanced radar networks that would deliver real time as well as archived data about vessel movements in this area [McBryan2011]. Such initiatives provide the groundwork for persistent surveillance capabilities in the GLSLS region, including the surveillance of small vessel movements.

The Northern Watch Technology Demonstration Project, initiated by DRDC, aims to “identify and characterize combinations of sensors and system for the cost effective surveillance of the unique maritime environment of the Canadian Arctic” [NorthernWatch2010]. In this environment however, most of the vessels that operate are large rather than small.

Canada’s approach to marine security, both prior to and after 911, has only born incremental but limited success due to a paucity of understanding of this complex issue at all levels of government coupled with limited resources. Granted, steps have been taken to address large vessels, specifically commercial vessels operating on international sea routes, but only tentative steps have been taken to address the internal and the external small vessel/boat challenge or indeed the issue of on water coordination and jurisdiction. In all of this activity there appears to be no coherent strategy or approach to marine security. This exacerbates the physical, the geographical and the numeric challenges posed by small vessels and small boats.

6. US Maritime Surveillance Initiatives

6.1 US maritime Security Overview

Small boat detection is not a new challenge for the US. Before 911, in the days of the war against drugs, US agencies led by the US Coast Guard (USCG) and the Drug Enforcement Administration (DEA) were actively seeking solutions to the tracking and identification of small boats used for the illicit transportation of drugs in the Caribbean and the Gulf of Mexico. At the time, they used manned aircraft and shore-based radars to maintain a maritime operational picture and to detect unusual traffic patterns. Among several thrusts, the USCG experimented with Canadian-developed Over the Horizon (OTH) Surface Wave Radar for long range detection of small and fast boats.

Airborne patrolling remains a preferred way of monitoring activity in coastal areas of interest to the USA. In the post 911 era, with heightened sensitivity to terrorism and security at their borders, the Americans have become increasingly interested in the border defined by the Great Lakes and the St. Lawrence Seaway. Securing the border is a common concern for the USA and Canada and several initiatives have been undertaken jointly by the two countries to coordinate efforts and to develop common approaches to border enforcement. Integrated Border Enforcement Teams (IBETS) are one example of several joint initiatives between the two nations.

In 2008, the US Department of Homeland Security (DHS) published a Small Vessel Security Strategy. The document notes the US Government's incomplete knowledge of the international recreational boating public and their travel patterns. It also points to the multitude of small commercial vessels that operate in the coastal regions of the US and the complexity this generates. A significant gap in knowledge about small boat traffic and in the capability to address the knowledge gap is identified in the background and environmental scan that support the strategy development. The scale of the challenge that small boats present is summed up in the statement that "the dearth of information regarding the user, owner, or operating patterns of those vessels make it extremely difficult to precisely identify the population and distinguish the legitimate users from those with the intent to do harm" [DHS2008].

The strategy identifies four principal risks associated with terrorists: domestic use of waterborne improvised explosive devices, conveyance for smuggling weapons including WMDs into the US, conveyance for smuggling terrorists into the US and waterborne platform for conducting a stand-off attack. Consistent with research in the Canadian context, the vision for improved small vessel security states that technology will serve to complement plans, initiatives and actions, but is not the sole answer to ensure small vessel security.

The envisioned solutions incorporate a mix of technological advancement with improved cooperation among agencies and between agencies and the boating public. The strategy points to the need for a layered approach to enhancing security that relies on a high degree of cooperation in the areas of information collection and processing, development and implementation of standing operating procedures, deployment of techniques for detection, identification, tracking and interdiction, and engagement of the public in the form of education, awareness and reporting of suspicious activity. The strategy is not specific with respect to priorities and allocation of resources. These are contained in operational plans and the specific details are most likely found in reports of projects undertaken by the DHS and possibly by other organizations.

6.2 US Technology Approaches

To establish priorities for maritime security, the US government formed the Maritime Capstone Integrated Project Team (MC-IPT). The IPT is responsible for gathering and prioritizing the requirements of its members and stakeholders[1]. Presently the focus is on communications, sensors, and surveillance capabilities leading to better operational situational awareness and mission related information management. The IPT aims to build the maritime security knowledge base and to develop technology to inform policy development and enable cross-component acquisition and procurement.

The Budget for the entire Borders and Maritime Programs, Projects and Activities (PPA) is about $40 million per year. The portion set aside for Maritime Technologies is about $7.1 million [DHS-S&T2008]. In 2010, these funds were devoted to several new prototype systems for tracking vessels in port and coastal regions, and tracking dangerous cargo barges in inland waterways. The program is also funding the testing and evaluation of 15 newly-developed prototype shipboard AIS and radar contact reporting (SARCR) systems and demonstration of their capability to identify vessel traffic via shipboard AIS and radar in maritime regions without shore-and space-based surveillance system coverage. The prototype systems developed under this project will enhance currently fielded systems' capabilities to detect and track targets, increase the correlation of AIS to radar system vessel tracks, improve detection and tracking of slow moving vessels, reduce radar track false alarms and reduce radar track fragmentation. This project points to the interest in the US in creating greater situational awareness through the integration of radar and AIS information; thereby providing reliable tracks of ships in an area for which there is a high degree of confidence in the ship identity and in the purpose of the ship's voyage. Additionally in 2010, there was work underway to develop a prototype OTH system and associated specifications for the Boarding Team Communications project. Work is also underway to demonstrate and transition to Customs and Border Patrol (CBP) and USCG initial Automated Scene Understanding (ASU) maritime capability based on cameras, radar and AIS. The goal is to reduce operator workload while maintaining effectiveness and improving the detection of anomalous behaviour. Pattern recognition is at the heart of the innovation in ASU. It can be either rule based, where operator assists are used to perform pattern matching and determine anomalous behaviours, or learning-based pattern recognition where artificial intelligence techniques and neural network classifiers are used to learn context-sensitive models of vessel behaviour and to provide alerts to operators. Both approaches are in development. It is expected that the rule-based approach will be operational before the learning-based approach.

The total investment by DHS over the five year period of the plan in maritime technologies is projected to be $33.5 million [DHS-S&T2008]. The principal interest over that period appears to be improvements in sensors, sensor integration and the ability to make sense out of data and information to assist in the identification of targets of interest and the determination of their intent. Both wide area and local approaches to maritime surveillance are being pursued. The DHS Wide Area Surveillance study considered tethered aerostats, airships and high altitude UAVs. Its plans for the near future include harbour small boat surveillance systems and the installation of surveillance and tracking systems mounted on off-shore an inland waterway buoys.

6.3 Implications for Canada

The US technology plans for maritime security are comprehensive and well funded. The view for vessel management is one that projects a future where there is a high degree of understanding of the vessel traffic picture in coastal areas, ports and inland waterways. This understanding will be developed using advanced sensors in the air, on the shores and in the water, and will be supported by sophisticated sensor

[1] The members and stakeholders include US Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, the Transportation Security Administration.

fusion and tracking algorithms and operator decision aids. Such an approach is fine for large vessels that can be tracked using AIS and that provide advance notification information. It can also be used to maintain an operational picture of small vessel traffic. The latter presents a significant challenge, however, because of the large number of small craft in many areas and the lack of knowledge of the small craft intent – the great majority of which are non-malicious.

The American interest in pursuing solutions to the small vessel problem that rely heavily on traditional surveillance approaches should be viewed with some degree of concern in Canada. To date we have done well in keeping abreast of US implementation of maritime security measures. We are compliant with the standards associated with the Container Security Initiative, Advance Notification and AIS reporting. There has been excellent cooperation between the US and Canada in security for coastal, Great Lakes and St. Lawrence Seaway border areas. As the Americans move toward highly technical and integrated approaches to the monitoring of marine traffic, Canada will need to be wary of the implications for investment in new monitoring and tracking installations and for the hiring of operators to man the systems.

It is unlikely that Canada will be able to afford or even want a “boil the ocean” approach, and therefore it will need to think about how to on one hand be compatible with and leverage the US advances in technology, and on the other hand, implement smart approaches that rely on other than technological solutions to understand and react to the small boat threat. Increased cooperation with the US is likely to result in better information sharing and coordination of functions between the two countries, and having the ability to equally participate in surveillance activities will only strengthen the Canada-US relationship. On the other hand, lagging behind the US in surveillance and monitoring may jeopardize not only the integrity of the Canadian border but also Canada’s interests in US-Canada border regions, potentially severely limiting and impacting trade and other cross-border legal activities.

7. Foreign Marine Security Overview

7.1 Foreign Marine Security Capabilities and Strategies

With nearly seven years since the adoption of the ISPS Code, many maritime nations have continued to improve their maritime security measures and strategies that are inclusive of addressing the small vessel threat. The impetus of many nations to expand their maritime security measures is based on the value of their maritime commerce and the existence of current and active threats within their region, the majority of which are presented by small vessels.

In this summary, we focus on several nations in two regions of the globe: Persian Gulf to the Arabian Sea, and the Indian Ocean to the South China Sea and identify current capabilities and strategies being pursued to improve their security measures whilst also attempting to mitigate the active small vessel threat. Within these two regions, a large percentage of maritime commerce is bound for North American markets. As such, those exporting nations have and continue to be pressured to improve their maritime security measures.

Most nations within these two regions have implemented a ‘military approach’ in addressing the small vessel threat. Those countries use a military or paramilitary force to conduct domestic maritime security functions, as opposed to a policing force. Notable in pursuing a military approach in combating the maritime threat in the Indian Ocean, South China Sea, and Northern portion of the Arabian Sea are: Pakistan, India and China. The responsibility to address the trans-national threat, identified primarily as trafficking of drugs, weapons and people, has resulted in an increase in each of their respective naval forces (much less so for Pakistan). The conflicts in Afghanistan and Iraq, coupled with the dramatic increase in piracy have also contributed to the increased attention to their respective maritime security programs.

In consideration of the militarization of maritime security operations taken by these three nations, one must recognize that the nature and capabilities of such a security force is formidable, not only from a weaponry perspective but also sensor capabilities. By understanding the capabilities from a sea-going security force, it is possible to also identify current and developing capabilities of sea and land-based operations and technologies. The following illustrates current and planned capabilities:

China	**India**	**Pakistan**	**Persian Gulf Region States**
• China Maritime Surveillance staff of 10,000 persons; • 300 Marine surveillance ships; • 10 Planes and 4 Helicopters for marine monitoring; • 36 Inspection ships by 2016; • Deployment of: o Detection & Interrogation cameras / CCTV: B&W, Colour, Thermal, IR o Surveillance systems o Perimeter protection systems o Access control and Biometrics o Underwater security sonar and Security o Communication systems o GPS o Chemical & Biological sensors o Integrated management platforms with GIS mapping o Virtual fencing (geo-targeting / geo-fencing) o Analytics / Proactive Alerts	• Biometric identity card for fisherman; • 1000 man security force equipped with 80 fast boats; • Coastal Command and Maritime Security Advisory Board; • Nine additional Coast Guard Stations; • Additional static radar stations; • AIS chain along coastline; • 100 AIS transponders for 330,000 crafts below 300 tonnes	• Ship and aircraft fitted sensors (operated by Coast Guard and Maritime Security Agency); • GPS with GIS integrated surveillance; • Acquisition of 5 patrol vessels (former US Navy); • Acquisition of Patrol aircraft (former US Navy P3 Orion); • VTS (Vessel tracking systems); • Video management systems;	• CCTV; • Satellite monitoring systems; • Floating barrier systems; • Sensor fitted floating barriers; • Automated video analytics systems; • Integrated surveillance systems; • Thermal, IR Cameras with integrated surface radar; and • Radiation and explosive detection sensors;

Table 1: Foreign current and planned capabilities

Nations within the Persian Gulf to the Arabian Sea present a similar engagement of military forces in maritime security operations. Of these nations attention is drawn to Bahrain, Qatar, and the United Arab Emirates as these nations have benefited from US funding initiatives to enhance maritime security operations. “American security initiatives were put forward even as Arab governments began considering the purchase of such systems. Thus, for those governments, acceding to American wishes fit well with efforts to improve their own security arrangements” [Martin2007].

Table 1 provides a description of current technologies deployed in the Persian Gulf Region States, and it is expected that future technologies will be consistent with those developed for the continental US Maritime Security plan.

Though the capabilities identified above were initiated by the implementation of the ISPS Code and directed toward large vessels, the existing threat has and continues to be from the small vessel. Robust investment in maritime security technologies coupled with active marine security patrol and interdiction operations will prove to be beneficial to their efforts. It is also expected that due to the increased level of piracy, the nations identified within this section will continue to pursue operational and technological developments to protect their national borders and maritime commerce.

7.2 Implications for Canada

Canada shares similar threats as the one's identified by the regions described above, however the threats of dangerous persons or terrorists being transported to the shores is lower in Canada. This assessment is founded on the premise that during the past ten years of armed conflict in the region of the Persian Gulf, sea routes were utilized by terrorist / Al Qaeda fighters to flee and evade capture by Coalition Forces. Many countries in these regions have incorporated a security approach that utilizes one agency that leads the technological and operational functions with fused and shared data products that can reduce threat levels and therefore provide greater likelihood of operational cohesion, versus the diffused approach used in Canada. Those countries, however, have a smaller geographic footprint to monitor and so the task of maritime security is easier to execute based on the geographic extent.

Also of importance is the availability of patrol and interdiction assets (both terrestrial and marine) to respond to events that develop, and to provide deterrence. Failure to have access to such technologies and lack of resources may result in Canada continuing to possess marginal capabilities to mitigate the small vessel threat.

8. Needs Assessment – Short and Long Term

Based on the needs identified via primary and secondary research discussed in Sections 2-7, below is a summary of the short and long term requirements necessary to enable the proper mitigation and response capabilities to counter the emerging, small boat asymmetric threat, based on Canada's existing vulnerabilities.

Today's list of potential threats include the trafficking of contraband, narcotics and weapons, human trafficking, transportation of terrorists / dangerous persons, and the potential of smuggling weapons of mass destruction (WMD) to include: chemical, biological, radiological, nuclear and explosive. The risks to Canadian security interests exist mainly because of weak maritime security regulations for small vessels, problems associated with enforcement and the ability of small vessels to operate virtually invisibly within Canadian and US waters. Unlike the coasts, where response time to a threat can be several hours, the authorities in the GLSLS region need to be able to respond to a threat within minutes, before the threat reaches the shore. There is a vast amount of commercial infrastructure on the GLSLS shores, which necessitates the need for Exclusion Zones around nuclear facilities, bridges, chemical factories etc. There is a need for quick threat identification and accreditation, which may require new approaches to the tracking of vessel movements. Both tracking systems and personnel resources also need to be available. Several types of strategically positioned sensors (with the positioning based on calculated Threat Risk Assessments) and technologies need to be integrated together. This requires the use of advanced data fusion tools and decision support systems by well trained operators. There is a need to develop comprehensive situation awareness using a layered approach. This layering needs to take place in both time and space and will have to include the fusion on intelligence and policing information with information derived from wide area and local sensors. The operators and analysts will need tools that allow them to zoom on to specific areas or vessels of interest for data capture and display.

There is a need to increase awareness within the boaters' community, as well as among those responsible for the management of shore and port facilities. This would involve education about what constitutes a threat, and the procedures one should follow when a suspicious activity is noticed. The information derived from sensors and related technologies can be significantly enhanced through the integration of Human Intelligence (HUMINT). It is important to include the boating public in the surveillance program.

Consideration must also be given to the availability of advanced technologies that may be employed by various threat groups. These include the availability of Autonomous Underwater Vehicles (AUVs) and re-breather diving apparatus. These technologies permit criminal activities to be conducted covertly whether for the purpose of trafficking or terrorism. Further, in recent years there has been an increase in piracy attacks throughout the globe, and so there is an emerging threat of groups adopting pirate-like tactics in their attempts to gain access to goods, people and infrastructure.

We can anticipate that with time the number of small vessels will increase. This will result in more sensor data, and the need for increasingly sophisticated data fusion and decision support tools. Climate change effects are now opening new northern transportation routes. This will generate a requirement to track and identify vessels of all kinds including small boats in these new areas of maritime transportation and commerce.

Specific sensor system requirements vary because of the specific characteristics of each geographic region. A few examples of how geography affects requirements are provided below:

Commercial Marinas/ Ports – This includes large commercial ports and marinas located on the GLSLS and on the Coasts, such as ports of Montreal, Toronto, Thunder Bay, Halifax and Vancouver. This environment requires medium area surveillance. Many tracking surveillance systems are already in place in major ports, but most are monitoring the shore perimeter of the facility. Few systems monitor harbour and port activity continuously. Ports have a need for information to be stored in databases so that operators can have access to historical data for determining patterns of behaviour or for the review of the history on a particular type of vessel. As ports have a variety of critical commercial infrastructures, the response window to a threat can be quite narrow. Security operators in ports require agile, accurate and quick decision support systems.

Private Marinas – Private marinas for the use of local residents are usually located near or in urban areas, and are normally equipped to berth a small number of boats (usually 1-2). This environment features a small number of vessels familiar to the local residents. The personal marinas are used mainly in the summer months. The main issue with private installations is the possibility of the small boats being stolen and subsequently used by groups for illegal activities. Owners need to be encouraged to install intrusion alarms.

Shoreline/ Coastline Persistent Surveillance – This region includes the coastal and shore areas between ports and marinas that are not equipped for docking and feature a large number of small vessels. The activities of the small vessels may vary; the majority will be recreational. The requirement here is for wide-area persistent surveillance. Strategic placement of sensors is necessary because of the large area under surveillance. Studies should be performed to determine optimal sensor locations.

Navigable and In-Land Waterways – Include waterways that border with the US (the areas of St. Lawrence Seaway and the Niagara River), including chokepoints. This region features a large number of small vessels. There are significant seasonal variations owing to the fact that most of the activity is recreational. The response window to a threat will be narrow and so there is a requirement for real time sensor information and decision support. Information should be stored to allow operators to view historical data.

Exclusion Zones – These are usually located around critical infrastructure, such as nuclear facilities, bridges, chemical factories etc. Access to these areas by any type of vessel is prohibited. Small area persistent surveillance systems equipped with alarms are needed to detect unauthorized entry.

In nearly every region of interest there is a requirement for sensor systems that are able to detect track and identify small boats. In all but the coastal area, reaction times are likely to be short. This gives rise to the need for real time information integration and rapid decision support.

9. Sensor Technologies Overview

Sensor technologies suitable for small boat surveillance are available, and can be largely found in the commercial domain, some cooperative, some uncooperative. This section provides a technological overview of various potential sensor options that can be used to provide maritime security stakeholders in different geographic regions with the necessary tools to meet their short and long term needs. The tables below list technologies that are currently used for maritime surveillance and the evaluation of these based on their ability to monitor for the small vessels in particular.

Persistent, 24/7 surveillance can be delivered in four domains: airborne, underwater, ground and space based. Sensor technologies that are currently used within these domains were reviewed based on their ability to mitigate the small vessel threat, versus the cost and potential legal, ethical, environmental implications that they present:

Ground-based systems

Criteria/ Sensor	Ground-based Class A AIS	Ground-based Class B AIS	HARTS
a) Ability to mitigate the threat by accurately detecting, identifying and tracking small vessels of concern	Detection, identification and tracking are possible and the technology is mandated for by international agreement through the IMO. Class A AIS is mandatory for larger ships. The technology is useful for cooperative vessels only.	Detection, identification and tracking are possible. AIS Class B is not mandated by any international treaty. The technology is useful for cooperative vessels only.	Detection, identification and tracking are possible. The technology is useful for cooperative vessels only.
b) Range of coverage, cost / feasibility to achieve a persistent and sustainable surveillance solution	• 50NM. • Costs $5000 per unit. • Continuous: Information transmitted every 2sec – 3min.	• 20 NM. • Costs $1000 per unit. • Continuous: Information transmitted every 20sec – 3min.	• Same as GSM network. • Costs $700 per unit. • Continuous: transmitted at a shorter interval than AIS B.
c) Usability of data considering potential communication constraints	Spectrum allocated for class A AIS may not be sufficient in areas of considerable small boat traffic.	Spectrum allocated for class B AIS may not be sufficient in areas of considerable small boat traffic.	Depends on the availability of GSM Network
d) Aptitude for convergence with current doctrine	limited potential given current regulations, but of use in de-cluttering the COP	limited potential given current regulations, but of use in de-cluttering the COP	limited potential given current regulations, but of use in de-cluttering the COP
e) Level of disruption to legitimate passage of people / goods	No disruption.	No disruption.	No disruption.
f) Extent to which proposed solutions respect international laws, environment issues, protection of natural resource exploitation, and the social, cultural, and economic fabric of First Nations communities	Mandated by the IMO for large ships. Ground stations are required to be built along the shoreline, which will increase jobs in the region, but may also disrupt the surrounding ecosystem. Privacy concerns may become an issue.	Ground stations are required to be built along shoreline, which may result in the disruption of the surrounding ecosystem. Workers are needed to build stations, and so will create jobs in the region of installation. Privacy concerns may become an issue.	If required for all ship types, may violate certain mobility rights as expressed in section 6 of the Canadian Charter of Rights and Freedoms. Availability of data to general public may raise privacy concerns.

Table 2: Ground Based Sensors I

Criteria/ Sensor	**Microwave radar**	**Over the Horizon (OTH) Radar**	**High Frequency Surface Wave Radar (HFSWR)**
a) Ability to mitigate the threat by accurately detecting, identifying and tracking small vessels of concern	Useful for detection and tracking, but limited identification capability.	Useful for detection and tracking, but limited identification capability.	Useful for detection and tracking, but limited identification capability.
b) Range of coverage, cost / feasibility to achieve a persistent and sustainable surveillance solution	• Up to 20NM. Portable radars can be used for coverage further away from coast. • Cost: Depends on radar type, for example the cost for navigation radar is $5,000. • Continuous coverage and real time information.	• Detection range data for small targets is not available. • Cost: Very high cost. For example Jindalee Operational Radar Network (JORN) in Australia costs more than $1.5 billion. • Real-time operation, but weather dependent.	• Up to 220NM, detection range varies with vessel size and weather conditions. An estimated maximum range for fast small boat detection is 44km [Blake2004]. • Cost: The radar system costs about $5 million; total cost including installation can reach as much as $10 million. • Data is refreshed every few minutes.
c) Usability of data considering potential communication constraints	N/A	N/A	Conflict with Industry Canada's spectrum management guidelines has forced the stakeholders of Canadian HFSWR to engage in reconfiguration of HFSWR system.
d) Aptitude for convergence with current doctrine	Good potential – needs to be integrated, fused and linked to an operations centre	Not practical due to high cost	Range limited for small craft. Only works in salt water so not suitable for surveillance in the Great Lakes
e) Level of disruption to legitimate passage of people / goods	No disruption.	No disruption.	No disruption.
f) Extent to which proposed solutions respect international laws, environment issues, protection of natural resource exploitation, and the social, cultural, and FNC	Radar stations are required to be built along shoreline, which will increase jobs in the region. Stations may hinder the surrounding ecosystem.	Radar stations are required to be built which will increase jobs in the region, but may also disrupt the surrounding ecosystem.	Radar stations are required to be built along shoreline which will increase jobs in the region, but may also disrupt the surrounding ecosystem.

Table 3: Ground Based Sensors II

Criteria/ Sensor	**Ground-based optical imaging systems**	**SONAR**	**Passive acoustic systems**
a) Ability to mitigate the threat by accurately detecting, identifying and tracking small vessels of concern	Useful for detection and tracking, and has some identification capability.	Useful for detection and tracking, and has some identification capability.	Useful for detection and tracking, and has some identification capability.
b) Range of coverage, cost / feasibility to achieve a persistent and sustainable surveillance solution	• Up to 10NM, detection range varies with vessel size and weather conditions. • Cost: depends on type and resolution. Usually less than 10,000$ per unit. • Refresh rate can be adapted and persistent surveillance possible.	• Up to 1NM, detection range varies with vessel size and transmitted signal power. • Cost: Single sensor head costs from $75K upward to $500K plus. • Refresh rate is in the order of minutes.	• Detection range can be as long as 10 NM. Coverage depends on number of sensors in the suite and target vessel characteristics. • Cost: Depending on the detection range such systems can cost up to $1million. • Refresh rate can be adapted and persistent surveillance possible.
c) Usability of data considering potential communication constraints	N/A	N/A	N/A
d) Aptitude for convergence with current doctrine	Good potential – EO, IR LIDAR. Needs to be linked to operation centres and supported by other sensors. Needs to be sensitive to geography	Good potential - best use is in choke points. However, installations in open waters could be expensive.	Good potential – best use is in choke points. Open ocean and lake installation could be expensive
e) Level of disruption to legitimate passage of people / goods	No disruption.	Sensor placement may limit accessible areas for boats.	Sensor placement may limit accessible areas for boats.
f) Extent to which proposed solutions respect international laws, environment issues, protection of natural resource exploitation, and the social, cultural, and economic fabric of First Nations communities	Requires ground installation. Need to also consider privacy issues related to captured images.	Use of sonar causes underwater noise pollution that can affect marine life.	Required underwater installation may limit public access.

Table 4: Ground Based Sensors III

Space-based technology

Criteria/ Sensor	LRIT	VMS	Space-based AIS
a) Ability to mitigate the threat by accurately detecting, identifying and tracking small vessels of concern	Detection, identification and tracking possible and the technology is mandated by international agreement through the IMO. LRIT carriage is mandatory only for three categories of ships making international voyages: cargo ships over 300 GT, passenger ships, and mobile offshore drilling units. The technology is useful for cooperative vessels only.	Detection, identification and tracking possible but the technology is mainly targeted at larger commercial fishing vessels and useful for cooperative vessels only. VMS is mandated on larger commercial fishing vessels by most Regional Fisheries Management Organizations (RFMOs) and many countries have mandated its use.	Detection, identification and tracking possible and the AIS transmitters are mandated for by international agreement through the IMO (however, only for larger vessels). The technology is useful for cooperative vessels only.
b) Range of coverage, cost / feasibility to achieve a persistent and sustainable surveillance solution	• No bar on range for the flag state. 1000 NM for coastal states. • Cost: around $5000 per transponder. • Coverage not continuous. Every 15min – 6hrs.	• No bar on range. • Cost approximately US$1000-4000 each, with operating costs of a few hundred dollars a year [Brooke2010]. • Coverage not continuous. Information transmitted every 1-2 hours.	• No bar on range. • The cost of AIS-S is considerable, with a flat-rate yearly subscription fee in the order of a few million dollars. • Coverage not continuous: refresh rate about 30 min for Polar Regions and 90 min for equatorial regions.
c) Usability of data considering potential communication constraints	N/A	N/A	Spectrum allocated for space based AIS may not be sufficient in areas of considerable small boat traffic; signals arriving at each micro-satellite will consist of overlapping signals from ships transmitting in the same time-slot
d) Aptitude for convergence with current doctrine	Very costly – not much scope for convergence here	Very costly – not much scope for convergence here	Very costly – not much scope for convergence here
e) Level of disruption to legitimate passage of people / goods	No disruption.	No disruption.	No disruption.
f) Extent to which proposed solutions respect international laws, environment issues, protection of natural resource exploitation, and the social, cultural, and economic fabric of FNC	N/A	N/A	If required for all ship types, may violate certain mobility rights as expressed in section 6 of the Canadian Charter of Rights and Freedoms. Availability of data to general public may raise privacy concerns.

Table 5: Space-based Sensors I

Criteria/ Sensor	**Space-based imagery**	**Space-based SAR**
a) Ability to mitigate the threat by accurately detecting, identifying and tracking small vessels of concern	Useful for detection of large and medium ships as well as small fast boats and can be useful for identification as well.	Useful only for detection of large ships. Not useful for identification or tracking.
b) Range of coverage, cost / feasibility to achieve a persistent and sustainable surveillance solution	• No bar on range. • $5000 per image (coverage about 15km x 15 km). • Coverage not continuous: requires a few hours lead time.	• No bar on range. • $4000-5000 per image (max. coverage 300km x 300 km). • Coverage not continuous: requires a lead-time of 4-12 hours minimum.
c) Usability of data considering potential communication constraints	N/A	N/A
d) Aptitude for convergence with current doctrine	Good potential but revisit time may make it hard to track fast boats. Needs to be supported by cueing.	Good potential but revisit time will make it hard to track fast boats. Needs to be supported by cueing and identification sensors
e) Level of disruption to legitimate passage of people / goods	No disruption.	No disruption.
f) Extent to which proposed solutions respect international laws, environment issues, protection of natural resource exploitation, and the social, cultural, and economic fabric of First Nations communities	N/A	N/A

Table 6: Space-based Sensors II

Airborne technology

Criteria/ Sensor	**FLIR**	**SLAR**
a) Ability to mitigate the threat by accurately detecting, identifying and tracking small vessels of concern	Detection, tracking and limited identification of vessels.	Detection, tracking and limited identification of vessels.
b) Range of coverage, cost / feasibility to achieve a persistent and sustainable surveillance solution	• Range may vary • Cost: around $5 million • Continuous coverage only for boats close to surveillance aircraft trajectory.	• Range: 40 km both sides of aircraft. • Cost: From $2 million to 4 million. • Continuous coverage only for boats close to surveillance aircraft trajectory.
c) Usability of data considering potential communication constraints	N/A	N/A
d) Aptitude for convergence with current doctrine	Good potential – needs cueing	Good potential – needs cueing
e) Level of disruption to legitimate passage of people / goods	No significant disruption	No significant disruption
f) Extent to which proposed solutions respect international laws, environment issues, protection of natural resource exploitation, and the social, cultural, and economic fabric of First Nations communities	Air pollution increases as the number of flights increases.	Air pollution increases as the number of flights increases

Table 7: Airborne Sensors

Criminal or terrorist operations could be detected using all or any one of these domains. Ideally, a surveillance network should be able to fuse information from sensors in one or more of the domains. In the air, surface and space applications, video, infra-red (IR) and radar sensors cover nearly all possibilities for area surveillance. For the underwater, passive and active acoustic sensors are likely the most effective options. An all-weather, day/night capability can only be delivered using a radar-based solution. Video and IR provide the best resolution, and hence better classification, but only in circumstances where there is good visibility. An optimum solution speaks to a multi-sensor, layered surveillance capability which relies on the most cost effective sensor suite to meet the requirements of long, medium and short range detection, classification and tracking of potential threats.

The fulfillment of the needs identified in Section 8 will require different sensors and placement strategies and solutions. In locations where some surveillance infrastructure already exists, a gap analysis will help identify any further enhancements that may be required. In other cases, where no infrastructure is currently present, the placement strategy will involve the initial survey of requirements. This section provides a summary of the characteristics of the specific regions, the likely threats and possible sensor solutions.

It is important to note that the selections itemized below are based on a cost/ benefit analysis. Many of the sensors that were reviewed provide great capabilities, but may not present feasible solutions when considering the cost and/ or current doctrine. Nevertheless, even though some of the sensors may be pricey, they may be required to enhance security in areas of critical importance and high risk. The ultimate selection of the sensor system must therefore depend on Risk Assessment studies that should be performed for each area of interest.

Target Area	Characteristics	Threat	Need	Beneficial Sensors

GLSLS Commercial Marinas/ ports	High concentration of small vessels;
	possible narrow response window;
	commercial infrastructure nearby
		Terrorism
		Trafficking of controlled substances/ firearms/ human;
		Alcohol/ tobacco Smuggling;
		Theft
			Medium area persistent surveillance;
			mostly seasonal;
			Storage of sensor information for long periods of time;
			Decision support required
				Ground based radar;
				SONAR;
				Ground based AIS B;
				Ground based optical imaging systems;
				Passive acoustic systems

GLSLS Private Marinas	Small number of small, familiar vessels; possible narrow response window; amount of vessel movement decreases significantly during winter months	Alcohol/ tobacco Smuggling ; Human/ Weapon/ drugs/ trafficking;	Small area persistent surveillance; mostly seasonal; Intrusion alarm required	Ground based optical imaging systems;

GL Shoreline Persistent Surveillance	Large number of small vessels; significant seasonal variations;
	many marinas along shoreline
		Alcohol/ tobacco Smuggling;
		Human/ Weapon/ drugs/ trafficking;
			Large area persistent surveillance	FLIR;
				SLAR;
				Portable radar;
				Airborne AIS;

Navigable and in-land waterways	narrow response window;
	Large number of large and small vessels; significant seasonal variations in number of
		Alcohol/ tobacco Smuggling;
		Human/ Weapon/ drugs/ trafficking;
		Theft
			Large area persistent surveillance;
			Real time sensor information and decision support;
				Ground based radar;
				Ground based optical imaging systems;
				Airborne sensors;

	small vessels; many marinas along shoreline	Terrorism	Storage of sensor information for long periods of time;	SONAR

Maritime Ports	Large number of both large and small vessels;
	larger response window;
	tracking technologies already in place;
	infrastructure nearby
		Terrorism
		Trafficking of controlled substances/ firearms/ human;
		Alcohol/ tobacco Smuggling;
		Large scale theft
			Medium area persistent surveillance;
			Storage of sensor information for long periods of time;
			Decision support required
				Ground based radar;
				SONAR;
				Ground based AIS B;
				Ground based optical imaging systems;
				Passive acoustic systems;
				Space based AIS;
				Space based SAR

Maritime Private Marinas	Small number of small, familiar vessels; amount of vessel movement decreases significantly during winter months	Alcohol/ tobacco Smuggling ; Human/ Weapon/ drugs/ trafficking;	Small area persistent surveillance; mostly seasonal; Intrusion alarm required	Ground based optical imaging systems;

Maritime Coastline Persistent Surveillance	Number of vessels varies depending on season
	wider response window;
	vast surveillance area
		Human/ Weapon/ drugs/ trafficking;	Large area persistent surveillance	FLIR;
				SLAR;
				Portable radar;
				Airborne AIS;
				Space based AIS;
				Space based SAR

Exclusion Zones	Small restricted area with no boat access;
	tracking needed to detect unauthorized entry;
	narrow response window
		Terrorism;
		Theft;
		Personal injury/ vessel damage
			Small area persistent surveillance;
			Intrusion alarm required
				Ground based radar;
				SONAR;
				Passive acoustic systems

Table 8: Target Area Needs Assessment

Sensor technologies suitable for small boat surveillance are available, and can be largely found in the commercial domain. However, additional technological developments of high resolution radar and high range imaging sensors will further enhance the overall effectiveness of small boat surveillance. Using currently available technologies, no one sensor will be able to address the entire needs of most geographic regions. As such, a key to a sound solution would be selection of suitable sensors, the strategic positioning of these sensors and intelligent fusion of sensor data which will allow for timely detection, identification and tracking of suspicious vessels. These are described in the next section.

10. Software Technologies Overview

Various techniques for surveillance can enhance Surveillance Intelligence and Interdiction (SII) capabilities and reduce operator overload. Some technologies suitable for this already exist in the maritime security domain. Others can be found in other security environments, and could be adapted for the purposes of small vessel surveillance. In general, **Target detection** technologies suitable for performing in high clutter conditions can be adapted to detect malicious vessels well before they enter into close proximity and become a threat. **Tracking** techniques can then be utilized to determine a vessels` trajectory and assist in pattern analysis. **Classification** techniques can be adapted to assist in maintaining target trajectory and provide relevant information regarding target capabilities (such as boat type, maneuverability and capacity). **Data fusion** techniques can be directed toward the small vessel surveillance application to provide a COP that can be used as a quick and comprehensive reference to the area under surveillance. Combining surveillance data with information generated elsewhere is potentially a powerful means of enhancing domain awareness and screening. Automatic **target identification,** provided principally through AIS, can help in managing clutter by discarding known targets and reduce false alarm rates. **Decision support** tools help with arriving at timely and correct decisions. **Databases** can be used for the storage of surveillance information for post incident analysis, recovery and continuity of operations to assist in prosecution and pattern analysis.

The vast quantity and type of sensors that need to be deployed in the marine environment to address small vessel detection, tracking and identification can be overwhelming when considering the large number of small vessels particularly during the summer months. This creates an inevitable multi-sensor information overload. Any technique utilized for small boat surveillance should be capable of handing large amounts of data. In addition, the large number of stakeholders with varying mandates requires different types of data processing and support capabilities, and so a flexible analysis system, with capabilities to serve different user requirements will be required.

Another problem, particularly evident in the GLSLS, is the presence of closely-spaced targets. This creates track ambiguity and can therefore deteriorate the COP. Signal processing techniques capable of either resolving the ambiguities, or when resolution is not possible, alerting the operator of the ambiguities are required.

Several signal processing and information fusion solutions relevant to small boat surveillance were reviewed as part of this study, including:

A. **Raytheon Marine Small Target Tracker** – Raytheon developed this microwave radar processing and display software which is already deployed for surveillance of the Straits of Gibraltar and waterways near New York airports. The system can interface with microwave radars from different manufacturers and it can fuse information from multiple radars. The software uses Interacting Multiple Model (IMM) – Multiple Hypothesis Tracker (MHT) algorithm for tracking and can detect and track small boats at a distance of 10 nm.

B. **Multi-Mission Radar Surveillance Networks -** Accipiter Radar developed a radar surveillance network solution, which is effective for small boat surveillance. A network is built using off-the-shelf radars that can be placed on rooftops, water towers, mobile vehicles, aerostats and towers [Nohara2010]. Apart from radar, each network node consists of controller and processor units. The processed information at a radar node, which includes radar plots as well as track information (using IMM-MHT tracker), is sent over a secure network to a data server. The data server interfaces with the end-users applications. End-users get access to geo-referenced track display, track fusion and classification output. The system has been demonstrated to different public organizations in USA and Canada, including the RCMP, and it is currently deployed for surveillance of portions of Lake Erie and Lake Ontario.

C. **SeeCoast Port Surveillance** – This system detects, classifies and tracks vessels by fusing EO-IR video data with radar and AIS data and provides decision support. The system is built upon the USCG Hawkeye system and provides tracks by combining EO-IR video with radar and AIS information. The system uses automated camera control for track acquisition, ship size classification, and track maintenance. Unsafe, illegal, threatening, and other anomalous vessel activities are detected based on rule-based and learning-based pattern recognition algorithms. A prototype SeeCoast system has been deployed in Coast Guard sites in Virginia [Seibert2006].

D. **Harbor Surveillance System -** This surveillance system, developed by DSIT Solutions, is effective for swimmers, submarines, mini-subs, and small surface vessels including rubber boats and kayaks. The system uses multiple sensors, including radar, sonar, and EO-IR devices. The system can detect divers at about 1 km distance, swimmer at 2-3 km distance and small boats at considerably larger distances. The system also uses an Autonomous Underwater Vehicle (AUV) that performs underwater surveys using forward-looking and side scan sonar systems.

E. **HarborGuard** – The surveillance system, developed by L-3 Klein, combines radar, EO-IR, and sonar (optional) to provide over and underwater surveillance. The system integrates all sensors on a common operating picture; provides remote control and operation of all sensors; and generates alarms based on programmable rules and criteria. The system is currently deployed by the US Navy for protection of base facilities; local governments for bridge, port / harbor and critical infrastructure security; and commercial companies for oil drilling rig and critical asset protection.

F. **COMMANDER -** Thales Canada is developing an Interdepartmental Maritime Integrated Command, Control and Communications (IMIC3) system, called COMMANDER, in which the Command, Control, and Communications (C3) nodes will be integrated through a satellite communications network to provide Canada-wide coverage. The system will enable real-time sharing of contact data, messages, and geo-referenced map overlays.

G. **Automated Ship Image Acquisition (ASIA)** – developed by DRDC Atlantic, this automated system is used for acquisition of boat images by the utilization of AIS information. In this system, an SLR digital camera is directed toward ship targets based on location information provided by AIS, takes a picture of the object and stores it in a searchable database. Required camera calibration and pointing procedures are developed. The system has been tested in the Halifax Harbour as well as through deployment in Canada’s North.

None of the reviewed systems addresses the requirements for clutter reduction, ambiguity resolution and reporting. Except for Multi-Mission Radar Surveillance Networks developed by Accipiter Radar, none of the other systems is designed to serve multiple end users. Hence, these systems are not flexible enough to simultaneously serve end users with different mandates. Multi-Mission Radar Surveillance Networks provide this capability, but are restricted to the use of radar. Hence, the system has limited classification capability at its current state. Automated Ship Image Acquisition (ASIA) uses AIS information which is generally not available for small boats. To increase its effectiveness in small vessel surveillance tasks, ASIA needs to be augmented for utilization of position cues from other sensors. The COMMANDER system presently being procured by the Government for the Canadian Coast Guard and the Navy provides a new and needed capability to exchange contact information and to develop a shared operating picture, but would need to be developed significantly for it to be able to address the small boat detection challenge. In its present form it is useful as a “feed” to a comprehensive information sharing and analysis capability that would be needed to address the small boat threat. Although the systems discussed above do not provide a complete solution for small vessel persistent surveillance, they provide components that will be useful for development of a comprehensive small vessel monitoring system.

Consequently, there are lingering gaps in software technologies that hinder successful monitoring of small vessels in the GLSLS and maritime regions. For a successful surveillance program, these gaps must be addressed. A potential solution to fill in the identified gaps is presented in Section 12, along with the appropriate rationale.

11. Capability Gaps Identification

Comparing the security requirements and current and emerging threats identified in Sections 2-8 with the technologies identified in Sections 9-10 indicates that there are several lingering capability gaps that prevent robust persistent small vessel monitoring in Canadian waters. This section aggregates the organizational, operational and technological challenges identified in the course of the study to produce a focused summary of top capability gaps that pertain to the surveillance and mitigation of the small vessel threat.

Due to the absence of maritime security regulations for small vessels, and the ability of small vessels to operate virtually invisibly within Canadian and US waters, the threats posed by small vessels are increasingly becoming of concern to the integrity of border security. Strategically, the ability to counter the small vessel threat is difficult if, for example, we consider only the challenge presented by the number of small vessels within the GLSLS region, estimated at approximately 6.2 million, excluding commercial vessels. Within this region, the modus operandi of criminals indicates that their cargo is transported either under the cover of darkness or within the unsuspecting population of boaters. The limited ability for small vessel detection and identification by authorities restricts the ability to screen vessels and therefore recognize a threat in a timely manner.

As outlined in Section 5, Canada’s marine security program is indeed improving, but is not yet able to provide adequate threat mitigation. Stakeholder responses and organizational analysis suggest that there are key areas where our security strategy can improve. Specifically, attention is drawn to the following:

1. Organizational gaps
2. Operational gaps
3. Technological gaps

<u>Organizational:</u> Until events of September 11, 2001, Transport Canada’s primary concerns revolved around transportation safety. The rapid move to introduce an international marine security program and pressure from the United States following 9/11 necessitated the creation of new Canadian marine security regulations, a task assigned to Transport Canada. The approach taken by the Canadian Government can best be described as ‘plug and play,’ whereby Federal Departments mandated and capable of delivering on the new marine security measures were assigned new roles and responsibilities, and in some cases, expanded responsibilities. Unlike the United States, that possesses one lead organization to execute the strategic and tactical operations relating to marine security (the US Coast Guard), Canada does not possess such an entity that would deliver a unified doctrine and subsequent common operational capabilities, operational platforms and sensor suites.

This deficiency inevitably introduces hindrances in inter-departmental communication, information sharing, and resource acquisition / deployment. Improving this aspect of Canada’s marine security program should entail a close look at the ‘combined’ operations of our national Marine Security Operation Centres as a starting point for improving the organizational structure and jurisdictional issues.

The current functioning of the security program is considered ‘closed’ in that non-governmental data is not being captured systematically for optimization of the COP. **There is considerable opportunity for exploiting data supplied by others to contribute to security efforts.**

A single government entity should be assigned both the responsibility and the accountability for marine security, including small boats/vessels. This will allow for centralized planning, coordination with other federal agencies and non-governmental stakeholders to ensure all relevant data streams are being included in the surveillance strategy. Alternatively, the present system of shared responsibility could continue. This is not the best approach and from an organizational and accountability perspective, standing operational procedures will need to be reviewed and practiced so as to ensure effective operations.

Operational: In the absence of a clear leading agency for maritime security, the program is divided among numerous federal departments, who each compete for funding to support their operations and asset acquisitions. Also, as marine security is not the primary function of these organizations, the contributions made by them are limited. **Financial and human resources are most affected** in the ability to deliver dedicated resources to the marine security program.

Further, **effective positioning of resources is vital** for an effective implementation of any surveillance strategy. With the budgetary constraints facing most government departments, the marginal effectiveness of added resources has to be measured and a cost-benefit analysis conducted. Based on the results of these analyses, a positioning strategy must be developed.

Technological: The necessity for appropriate and suitable sensors is primary, followed by their strategic positioning based on calculated Threat Risk Assessments and matrix. Advanced software technologies need to be used to differentiate between legal and illegal activities. Three areas where we have noted the need for technological improvements are:

> **Sensors -** Currently there is only a limited number of sensors with complementary capabilities (detection, classification, and tracking) useful for layered surveillance that are deployed. **An optimum solution speaks to a multi-sensor surveillance capability** which relies on the most cost effective sensor suite to meet the requirements of long, medium and short range detection, classification and tracking of potential threats. This requires risk assessment studies to be conducted to pinpoint proper sensor placement locations, followed by sensor deployment. Most of the sensors necessary for comprehensive small vessel surveillance are commercially available. However, additional technological developments are required for high resolution radar and high range imaging sensors to further enhance the overall effectiveness of the small boat surveillance strategy.
>
> **Detection/ classification/ tracking tools –** Even though those technologies exist, they are yet to be combined together and implemented in the context of small boat surveillance in Canadian waters. Therefore, **procedures for detection, classification and tracking of small vessels need to be clearly defined**, and technologies that present the best alternative in the context of small vessel surveillance identified.
>
> **Data fusion and decision support technologies -** Of importance to the security strategy is the acquisition of data for intelligence and development of the COP. The difficulty is the ability to

> fuse large amounts of data for analysis and reporting. Data fusion therefore is critical for the success of a national marine security strategy. None of the commercially available systems address the requirements for clutter reduction, ambiguity resolution and reporting, required for effective small vessel surveillance. **There is a need for effective data fusion tools that will allow for a layered surveillance approach and intelligent situation assessment and decision support.**

Dealing with the above concerns needs a multifaceted approach starting with the development of policies and procedures that support the operational interests, and finishing with specific solutions that are tailored to the geographic area, the interests of the stakeholders and the scenarios that the areas are most likely to experience. For an effective small vessel surveillance strategy to emerge, organizational, structural and jurisdictional issues that exist today need to be resolved. In particular, the underlying problem of no single government authority with the responsibility for marine security is an area that cannot be resolved in this study. **Thus solutions to provide enhanced situational awareness will have to work within the current organizational construct, at least in the short to medium term** until proper structural modifications have taken place.

The next section provides an overview of a multi-sensor surveillance system that accommodates the various jurisdictional differences that currently exist. It provides a common platform that can be utilized by users with specific departmental mandates that are located in different regions within Canada. Through this system, users can choose the specific sensors and tools they require to deal with the specific threats that are of concern to them.

12. Multi Sensor Surveillance System for Asymmetric Threat Mitigation

Following an assessment of the current and emerging threats and capability gaps associated with small vessels surveillance within Canadian waters and a review of persistent surveillance requirements, a novel, scalable and data-centric multi-source information fusion concept was developed by the study consortium to provide persistent monitoring of Maritime, Great Lakes and St. Lawrence Seaway border regions, specifically aimed at countering the small vessel threat. The concept takes into account the current capability gaps and limitations faced by stakeholders from the organizational, technological and operational aspects in the Canadian maritime security landscape.

12.1 System Overview

The Vessel Intelligence Centre (VINCENT) is a systems concept design that aims to address the small vessel surveillance issues identified throughout this report. VINCENT is a multi-sensor persistent surveillance system design, including both sensor and processing components that will support border enforcement and surveillance/ response mechanisms in asymmetric threat mitigation. This concept will provide a common platform for contributors and recipients of data to interact. Data recipients, such as law enforcement personnel, will be able to access the system and receive data streams of information that is of interest to them. Information will be presented on a user friendly interface, complete with data processing and information sharing tools. Data contributors, both governmental and non-governmental organizations, will provide data streams to the system. A third party organization / agency will be responsible for system maintenance and coordination between the recipients and contributors. The suggested platform delivers data not only about small vessels, but rather about all vessels. This allows the recipient to create a Common Operating Picture (COP) with comprehensive situation awareness.

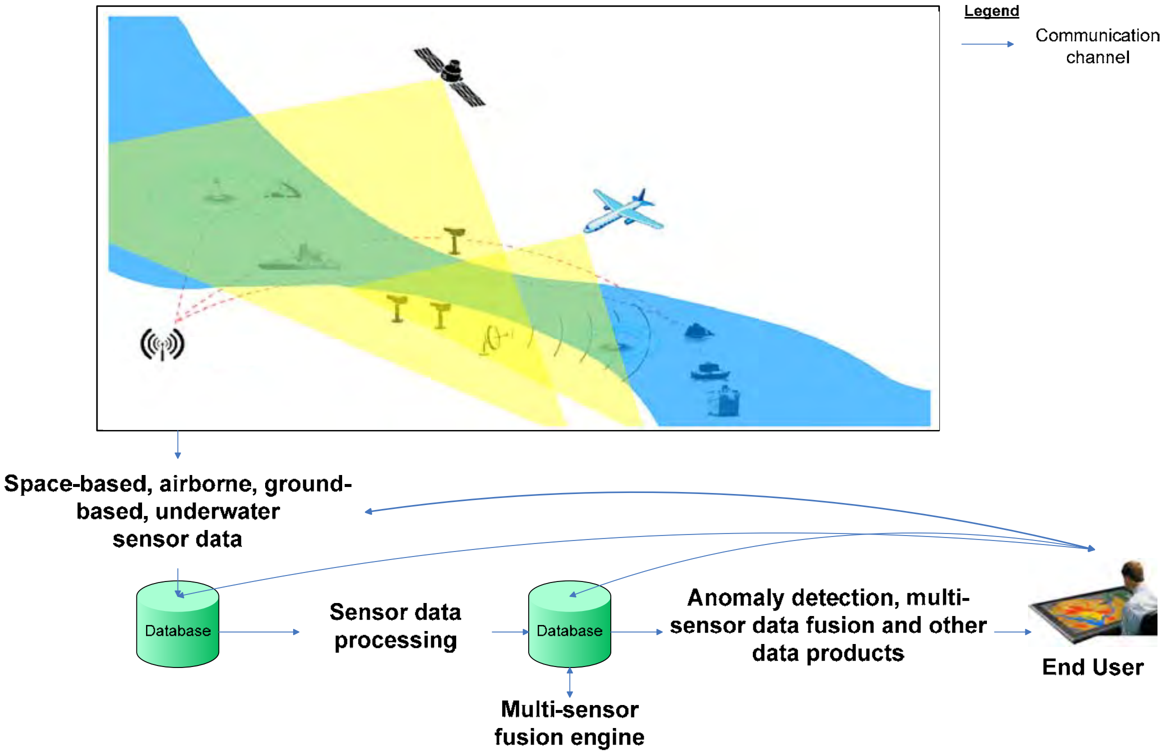

Legend
Communication channel
Space-based, airborne, ground-based, underwater sensor data
Database
Sensor data processing
Database
Anomaly detection, multi-sensor data fusion and other data products
End User
Multi-sensor fusion engine

Figure 1: High level system overview

The system should take advantage of all available data streams and information sources relevant to small vessel surveillance. End users (the Stakeholders) who require such data should be able to access the system and receive relevant data streams. Contributors (both governmental and non-governmental) should be able to supply data to the system and may be compensated for doing so. Organizations that are outside of the government or Crown agencies would have to be cleared with a security screening before being able to participate or 'plug-in' to the system.

This approach provides an incentive for contributors to share the data, and allows end users to choose which data streams to receive. Whether a specific end user only requires access to one type of information stream, or would like to receive the complete set of data available, each is an option. As such, end users who have developed their own COP will be able to use this system to further enhance their COP. Other users, who may not have sophisticated COP, will be able to acquire one specifically customized to their requirements. This contributor / recipient relationship ensures that end users are able to access timely, relevant data when needed. Furthermore, the adaptability and flexibility of the system ensure that stakeholders with varying mandates and requirements are able to reap the benefits of this system by only accessing those data streams that are of relevance to them. New information streams could be easily added to the system upon stakeholder request.

Section 9 outlines the suggested sensor technologies that different geographic regions could benefit from. Sensors that are already deployed should be integrated into the system. Other sensors should be added based on end user and strategic requirements of each geographic region. Regardless of the geographic area in question, Risk Assessment studies should be performed in order to identify the most fragile areas that present high potential for criminal activities, and priority should be given to securing those locations.

A list of potential Recipients and Contributors of data is illustrated below:

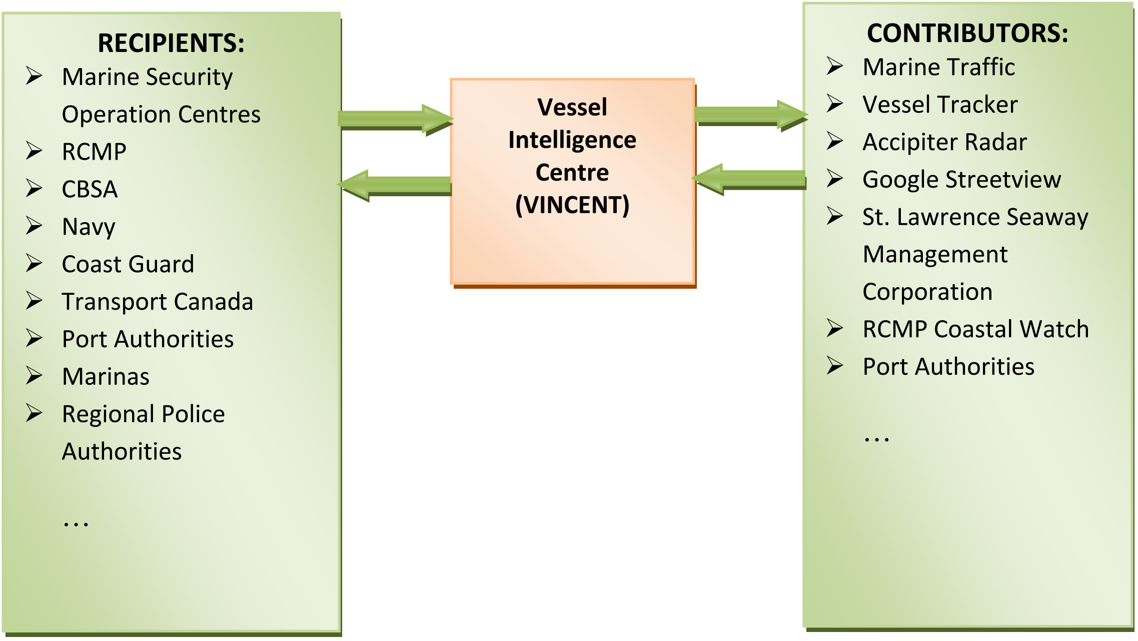


Figure 2: Potential Recipients and Contributors of Data

The system should act as a central repository for data contributors and recipients. The stakeholders outlined in Section 4 are the primary data recipients, and could also act as data contributors, as well as exchange information with other stakeholders through the system. This platform will allow for information growth as the demand for data increases.

12.2 System Capabilities

VINCENT should not simply be an information gathering and processing system, but should also provide multi-faceted services for end users to choose from based on their needs. The system functionalities should address all the technological capability gaps outlined in Section 11 and provide the following services:

- **Multi-Layer Data and Processing Service** – a central database should provide prolonged data storage of all the raw sensor data and processed data (current or historical) at different processing levels for authorized users to access. End users can use that data for further processing or as an input to their own systems. Processing levels that should be offered include:
    - Raw Data Service
    - Processed Data Service:
        - Automatic Detection and Alerting Service
        - Classification/Identification Service
        - Tracking Service
        - Fusion Service
    - Decision Support Service

- **Sensor Control Service** – if authorization is provided by the sensor owner, temporary control of certain sensors in the system (such as EO/IR sensors) should be given to authorized users/ data recipients to capture information of interest. For example, an end user may need to zoom onto a specific vessel of interest to confirm identity. He/ she will send a request to the central command centre, and provided the user has the proper security level, he/ she will be able to direct the EO/ IR sensor and capture the zoomed object. After control is provided, the sensor should have an automated realignment function that will allow it to return to its original baseline position.

- **Information Sharing Service** – the system should include a platform that allows authorized end-users to share information, such as sensor data, human intelligence, and other (when permitted) on case-by-case basis through an Inter-Group Shared Information (IGSI) protocol. In the event of an emergency, various departments may wish to exchange or share intelligence for maximum situation awareness; this can be done via the IGSI protocol.

- **Complete Graphical User Interface (GUI)** – a GUI should be included in the system. The GUI should contain a layered display of information requested by each end user, including a display of vessels of interest, tools for controlling sensors for authorized users, drill-down capability for data at different levels (raw, processed, etc.) and various decision support tools, such as virtual fence setup around exclusion zones, borders and other tools specified by end users.

12.3 System Architecture

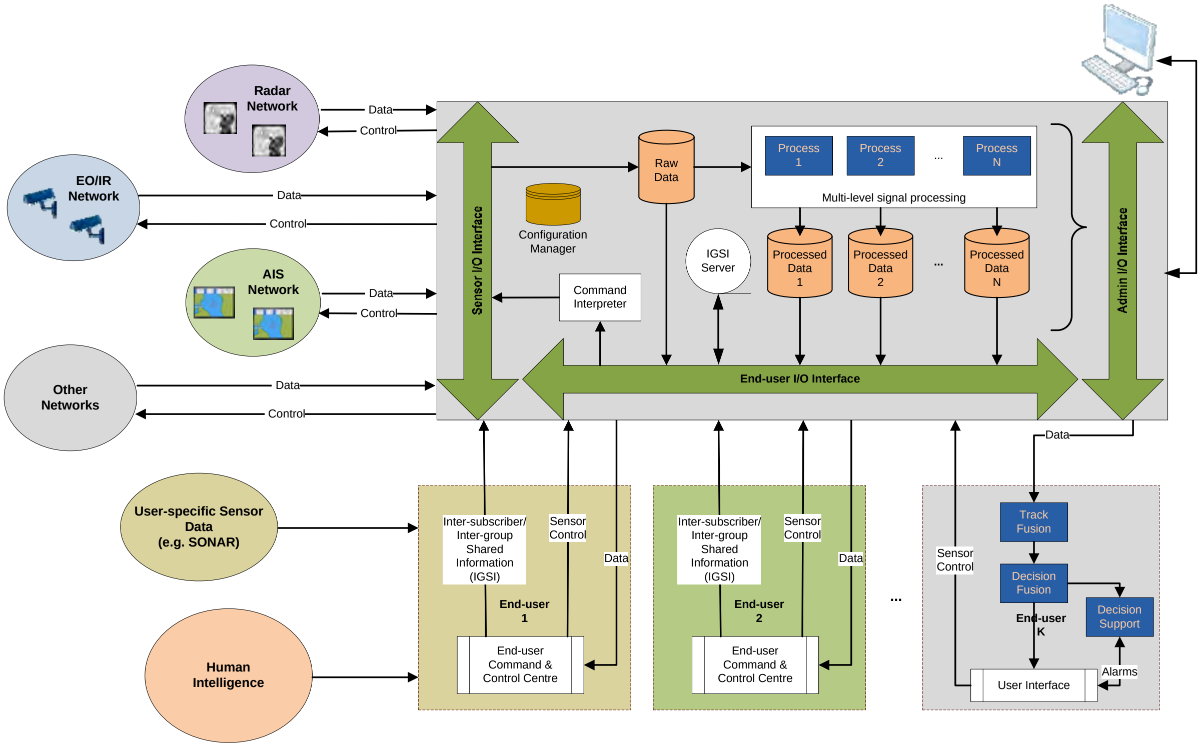


Figure 3: Multi-sensor system architecture

There are three major components to the system architecture that was conceived: Data Networks, Central Data Repository and User Terminals. A fourth component – the Inter-subscriber/Inter-Group Shared Information (IGSI) protocol allows two users to exchange information without making it available to other users. The Data Networks should consist of existing public and/or commercial sensor networks that will provide a significant amount of information to the system. Through a standard “Sensor I/O Interface”, data networks should be connected to the Central Data Repository. The Central Data Repository should use the data from contributors to perform single-sensor processing operations (e.g. small boat detection, tracking and classification operations, when required). It should provide prolonged data storage of all the raw and processed data for authorized end users to access. Through a standard “End-user I/O Interface”, relevant stored data should be made available to all authorized User Terminals. In these terminals, fusion of data from different sources and decision support operations required by the end user should be performed. In addition, sensor control tools should be available for authorized end users to access. The End-user I/O interface should also allow for information exchange between two users through the IGSI protocol. In this case, the data communicated between end users should not be observable or storable in the Central Data Repository. The IGSI server should only keep communication protocol information that facilitates information exchange between users. Any additional information available to end users, from sensors or human intelligence, should be seamlessly added in order to obtain user-specific complete COP. Advanced end-users, with their own fusion and decision support capabilities should be provided with the data of their choice from the Central Data Repository, and if authorized, utilize sensor control tools available in the system. The “Admin I/O interface” should be used to configure, manage and maintain the system during its operation.

The sensor networks should include Radar Network(s), EO/IR Network(s), AIS Network(s), and others, depending on end user needs. An existing wireless / wired network should be utilized to communicate data (raw data as well as on-site processed data that is encrypted to ensure data integrity) from the sensor sites / contributor locations to the data repository through a standard "Sensor I/O Interface". The system should be flexible so that different end users coming from different departments or different jurisdictions can have a customized display of the current or historical situation, without necessarily forcing them to share confidential information with each other. A case-by-case information sharing mechanism should be provided in the system through an Inter-group Shared Information (IGSI) protocol, which should allow end users to only share information in certain instances or events, for a fixed duration.

The system should provide multi-level signal processing for small vessel surveillance. The processing chain is illustrated in the figure below:

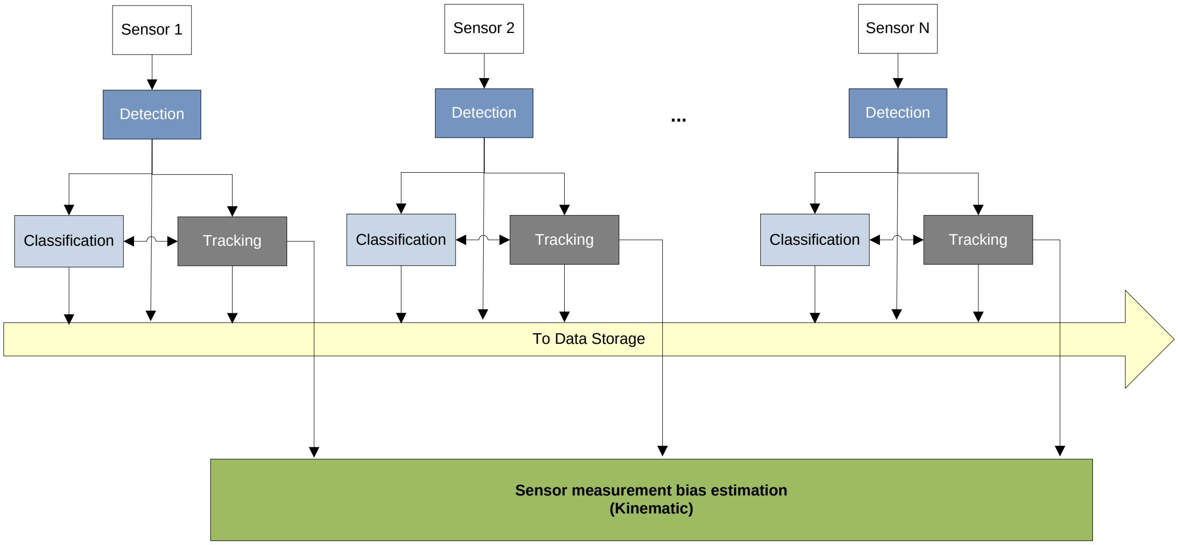


Figure 4: Multi-level processing chain

12.3.1 Operations Performed at the Central Data Repository

In the following, an inventory of potential technologies that should be deployed for the processing and storage tasks is presented. This inventory lists technologies that present the highest potential for small vessel monitoring activities, as described below:

12.3.1.1 Detection

The primary task of sensors used for the surveillance of small boats is to detect all targets in their observation region. Target detection in constant background can be simply achieved by thresholding of the sensor-acquired signals. However, the constant background assumption can generate an unacceptable number of false targets due to reflections from rough water surface which can have regional variation due to wave patterns and temperature variations in littoral environments. These non-target background reflectors are often denoted as clutter. Although there have been detection procedures developed based on learning the clutter density and its variation in the detection region, the "blind" techniques, which do not require any knowledge of underlying clutter density are more practical and computationally efficient. Constant False Alarm Rate (CFAR) detection is a procedure which has been successfully used for detection for multiple sensor types, including Radar, Sonar and imaging sensors. CFAR detection is performed by comparing a particular data point with a suitable threshold based on its neighbouring data points. This procedure, unlike constant thresholding, does not assume globally constant clutter statistics.

In cell averaging (CA) CFAR, the average of neighbouring cells is used to compute the threshold. This has the drawback of misdetection when multiple targets are present in close vicinity. To avoid this, Order Statistic (OS) [Rohling1883] CFAR was developed, which determines the detection threshold based on the amplitude of a neighbouring a data point. This neighbouring data point has a pre-defined position in the ordered set of all neighbouring data points.

The above mentioned procedures achieve limited detection performance in a low signal-to-noise (SNR) environment. Since only a single scan, such as a radar scan or an image is used for detection, these methods can be identified as single-scan methods. An alternative is multiple scan based methods, which are often called track-before-detect (TBD) in the literature. These methods exploit the fact that signals from targets show higher degree of consistency than the background clutter. Hence, by processing multiple frames at the same time, the clutter can be suppressed and a better detection decision can be made. A number of TBD methods are available [Hadzagic2005]: Hough transform, dynamic programming algorithm and recursive estimator.

The Hough transform detects lines and has proved to be useful for detecting small targets with few scattering centres and non-fluctuating amplitude of the measured signals. However, the method is computationally expensive and useful for distinct straight line trajectories only. In the dynamic programming framework, the data points in signals are considered as the nodes of a trellis of possible solutions. The trellis is expanded incorporating the next frame using state transition models. The algorithm is computationally even more expensive than Hough transform. Both Hough transform and dynamic programming method requires storage of a number of sensor scans for simultaneous processing. The recursive estimator shows similar memory and processing requirements owing to the need to explore all position and velocity values of the unknown target.

The detection system should use OS-CFAR for medium to high SNR (greater than 10dB) scenarios and switch to TBD algorithm, such as EM-ML, for lower SNR scenarios.

12.3.1.2 Tracking

After detection is performed, tracking of small boats is an essential step to ensure the situational awareness of the system. Tracker estimates the kinematic states of a small boat, such as its position, velocity and acceleration. At the Central Data Repository, sets of tracks from disparate sensors are not fused together but rather kept separate for each type of sensor to facilitate the possibility of users choosing to receive streams from different sensors. As each new scan of data is received at the Central Repository, detection is performed and the detected small boats are associated with existing tracks for the particular type of sensor. This is called track maintenance and is performed separately for each sensor. Track maintenance can be divided into two interacting modules: data association procedure and tracking filter. The Probabilistic Data Association (PDA) [Bar-Shalom1995] is a popular approach, which relaxes the otherwise binding constraint of assigning one track to only one measurement and weighs the contribution of each measurement by the probability that it is target originated.

Unlike the PDA, another group of data association algorithms enforces the single-track-to-single-measurement association constraint. These algorithms are known as assignment-based algorithms since they use assignment approaches to associate measurements to tracks. Examples of assignment-based trackers are 2-D assignment tracker [Wang1999] and multidimensional assignment tracker [Poore1991].
The above discussed PDA-based and assignment-based data association approaches are suitable for different tracking scenarios. The PDA-based track maintenance approaches are suitable in scenarios with low target density and high false alarm density. In closely spaced target scenarios, particularly when targets move in parallel for some time, PDA-based approaches lead to track coalescence. On the other hand, assignment-based track maintenance approaches are suitable for low false alarm and high target

density scenarios. Due to possible hard (rigid) associations with false alarms, assignment-based approaches suffer from significantly higher track loss compared to PDA-based approaches in high clutter scenarios.

Both data association approaches should be used, depending of clutter density specific to particular sensor type and observation region.

Assignment-based algorithms can evaluate multiple association possibilities or ranked solutions [Murty1968]. This characteristic is exploited in Multiple Hypothesis Tracker (MHT) [Blackman1986] which delays measurement-to-track association decisions by updating multiple track hypotheses. MHT is particularly effective in closely-spaced target scenarios and can be used to track targets that are occasionally unresolved [Blackman2004]. MHT is already being used in radar-based small boat tracking applications [Nohara2010,Ponsford2011].

The main reason for the development of MHT is to avoid track switches (due to measurement association ambiguity), which can considerably degrade the surveillance picture. However, in order to make MHT manageable, hypotheses must be pruned, thus undermining the theoretical benefits of the method. The pruning of hypotheses may result in a failure to resolve ambiguity of track identity (origin, feature etc.), if the period of measurement association ambiguity is long.

A novel framework of tracking is presented in [Sinha2010] to overcome the above-discussed limitation of MHT, particularly in scenarios with severe and prolonged measurement association ambiguities. In this framework, the tracking picture consists of tracks, IDs, and a list of global track-to-ID association hypotheses – each with a probability score. An ID is created whenever a new track is confirmed. Track-to-ID associations are treated dynamically: their probabilities are either 1 or 0 at track initiation, but then are allowed to vary throughout the interval between 0 and 1 in response to track association ambiguities. In order to retain ID purity, the updating of an ID is restricted in the presence of ongoing association ambiguities. Once the period of association ambiguity is over, track-to-ID associations can be resolved if targets have distinctive features. Until then, the algorithm explicitly indicates that some ID-to-track associations have not been resolved. The ID-aided tracking approach can also be applied to kinematic-only measurement scenarios to provide users with track-to-ID association probabilities. This information can be used to determine the possible origins of a target track. Even when it cannot resolve all track switches, the procedure acknowledges the switches, thus making the operator aware of ambiguities in the track picture.

The ID-aided tracker should be used for robust tracking of small boats.

Tracking filter is an important component of track maintenance. The Interacting Multiple Model (IMM) filter, which supports different target motion models, is a popular choice for manoeuvring small boat tracking [Nohara2010] and is suitable for the system. IMM uses Kalman filter for measurements that have linear relationship with small boat kinematic states (position, velocity and acceleration). This relationship is, in general, true in the case for radars with linearized measurements. When the relationship can be approximately linearized, such as for EO/IR images, the extended Kalman filter (EKF) is used. For highly nonlinear measurements, such as for passive sonar, unscented Kalman filter [Julier1997] is used.

Although no track fusion operation should be performed at the Central Data Repository, data from different sensors should be registered to estimate and compensate for track position biases introduced by the sensors.

12.3.1.3 Classification / Identification

Single-sensor based classification/identification is important for situation assessment during small boat surveillance. This functionality is performed separately for each sensor type. AIS provides information which can be directly used for vessel identification; Radar provides target amplitude and extent information; EO sensors provide boat size, shape, color and wake information; and IR sensors provide the boats' IR profile information. Different sensors identify distinct small boat features which provide different classification capabilities. The key procedure in boat classification / identification is to find useful features to reduce ambiguity among boat classes. With properly selected features, a classifier is trained based on prior knowledge such as feature model or even training samples. For this reason a feature database will be maintained at the Central Data Repository and this database will be expanded based on the analysis of classification performance. Classification is then performed by applying the trained classifier to the test data. Image based object classification [Yang2008] and landmark recognition [Cummins2009] have shown great degrees of success. However, the application of this technology for classification of small boats is not mature.

12.3.1.4 Data storage

Such a system will require long term storage and retrieval of raw as well as processed information. Hence, a network storage architecture that is capable of handing the storage and retrieval of large volumes of data will be appropriate. Traditionally, network storage resides on hard disks in individual servers. A problem with this approach is that servers only hold a limited number of disks and network traffic to the server could easily form a bottleneck. In recent years, technologies such as Network Attached Storage (NAS) and Storage Area Network (SAN) have emerged and matured to overcome this constraint.

Network Attached Storage is a file system attached to the network that acts solely as a storage center with one or more hard drives, often arranged into logical, redundant storage containers or RAID arrays. A NAS device usually connects to the LAN with Gigabit Ethernet (GigE) ports; some NAS products provide multiple Ethernet connections for network interface aggregation, redundancy or failover. Compared to file servers, NAS provides scalable data storage, faster data access, easier administration, and simple configuration. It can be clustered to distribute data across the cluster nodes or storage devices and still provide unified access to the files from any of the cluster nodes, unrelated to the actual location of the data. Database vendors such as Oracle provide support for using a NAS device for its software and database files. Vendors of NAS systems/devices include NetApp and Hitachi Data Systems.

Unlike NAS, which resides on the user's current network, SANs are separate and dedicated networks that house the storage devices and provide access to consolidated, block level storage. The following figure shows a tiered overview of a SAN connecting multiple servers to multiple storage systems [Tate2006].

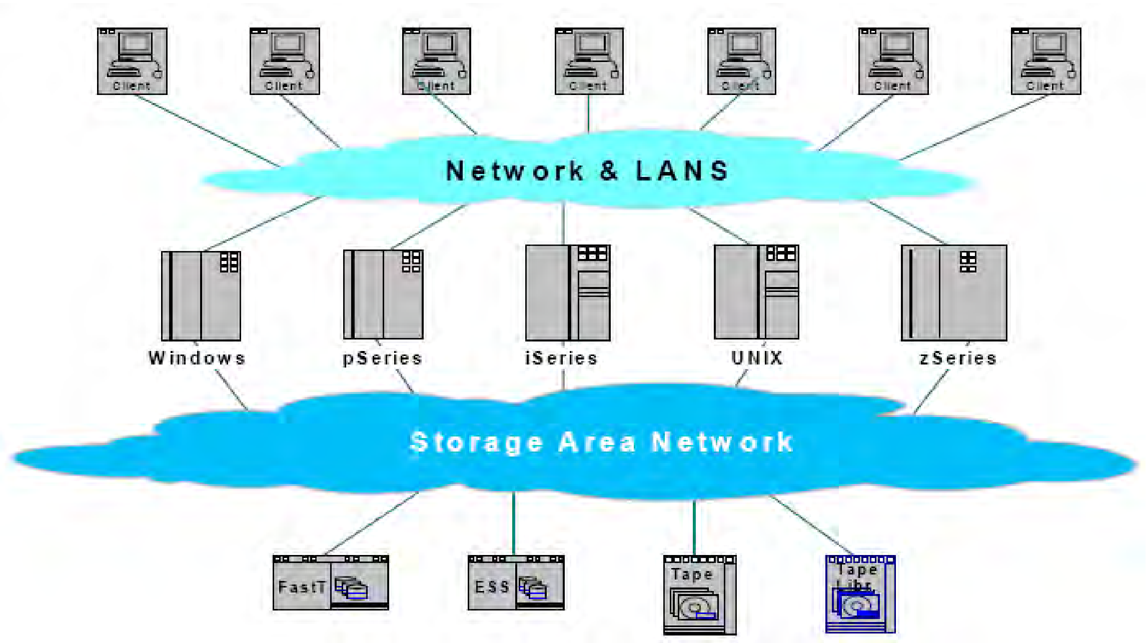


Figure 5: Overview of SAN network

SANs often utilize a Fibre Channel fabric topology - an infrastructure specially designed to handle storage communications, which provides faster and more reliable access than higher-level protocols used in NAS. A typical Fibre Channel SAN fabric is made up of a number of Fibre Channel switches (such as Brocade VDX 6720 Data Center Switches). SANs create new methods of attaching storage to servers and enable large improvements in scalability, availability and performance. They bypass traditional network bottlenecks and facilitate direct, high-speed data transfers between servers and storage devices. The cost and complexity of SANs dropped in the early 2000s, but they are still more expensive solutions than NAS.

NAS is a good candidate for data storage due to its lower cost, however the system can run on either a NAS or a SAN and the decision on which one to use should be based on the expected volume of data, the cost of infrastructure and the geographic extent of the repository.

12.3.1.5 Communication

In the VINCENT concept, it is essential to have fast, reliable and secure data communication from the sensor sites / contributor locations to the Central Data Repository and from Central Repository to User Terminals.

Data Security

Secure communication employs cryptography tools such as confidentiality, authentication, and access control to ensure that end users can share information with varying degrees of certainty that a third party will not be able to intercept the data [AUG2007].

Information confidentiality is provided via data encryption. There are two types of encryption schemes: Symmetric Key Encryption and Public Key Encryption. Symmetric key encryption, also referred as conventional encryption, secret-key, or single-key encryption, remains by far the most widely used of the two types of encryption. In symmetric key encryption, the same key is shared by sender and recipient to encrypt / descript messages. There are three important symmetric block ciphers: the data encryption standard (DES), triple DES (3DES) and the advanced encryption standard (AES). Public key encryption, on the other hand, uses different keys for the sender and the recipient. Thus, unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one or more secret keys between the sender and the recipient. The public key encryption is designed in such a way that the sender encrypts the message using the public key and the intended recipient decrypts the message using the private key, and hence it is extremely difficult for third parties to decipher the private key based on their knowledge of the public key.

Message authentication is another security tool that allows communicating parties to verify that the received messages are authentic. Two important aspects here are to verify that the contents of the message have not been altered and that the source is authentic. Message authentication is achieved using a one-way secure hash function. The purpose of a hash function is to produce a “fingerprint” of a file, message, or other block of data. To be useful for message authentication, a hash function must be relatively easy to compute for any given data, making both hardware and software implementations practical. On the other hand, for any given hash output, it is computationally infeasible to find the corresponding input. Moreover, for any data, it is computationally infeasible to find another data such that they produce the same hash value. This is sometimes referred to as weak collision resistance. Finally, for a secure hash function, it is computationally unfeasible to find any input pair such that their hash values are the same. This is sometimes referred as strong collision resistance. Some widely used secure hash functions include MD5, SHA-1 and HMAC algorithms.

Access control is a system which enables an end user to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure. The possession of access control is of prime importance when personnel seek to secure important, confidential, or sensitive information and equipment. Item control or electronic key management is an area within (and possibly integrated with) an access control system which concerns the managing of possession and location of small assets or physical (mechanical) keys.

All three types of secure communication measures discussed above, namely confidentiality, authentication and access control, should be part of the architecture for communication between the Central Repository and User Terminals. Communication between Data Networks and the Central Repository should also be secured using the tools discussed above.

Connectivity

The connectivity provided by commercial internet service providers should be utilized where it is available. For sensor sites / user locations that are not served by commercial internet service providers (this is typically the case for rural and remote sites in Canada), several potential connectivity solutions are proposed in the following based on input received from the Communications Research Centre Canada [Brandao2011]. However, these solutions are also useful for sites in urban areas where internet access is not possible or not economically viable.

The topology for a wireless sensor network / user network is the digital half-duplex (TDD) system with a wireless hub/controller in the middle of a star configuration as shown in Figure 6 below. This forms a local network that is limited in size around the monitoring facility. In the figure, the end points are the sensors and actuators (i.e. switches) that are used for monitoring and/or control equipment. The communications between the wireless hub and sensors / users may be performed by several types of technologies. The most common types include Zigbee, WiFi and Homeplug technologies. The wireless hub forwards the sensor data to a central station that is responsible for processing and storing all information. The connection between the wireless hub and the Central Repository can be achieved through a microwave link, satellite, mesh network, HF/VHF or other types of links. The choice of link is often specific to each remote site and there is no one solution that fits all.

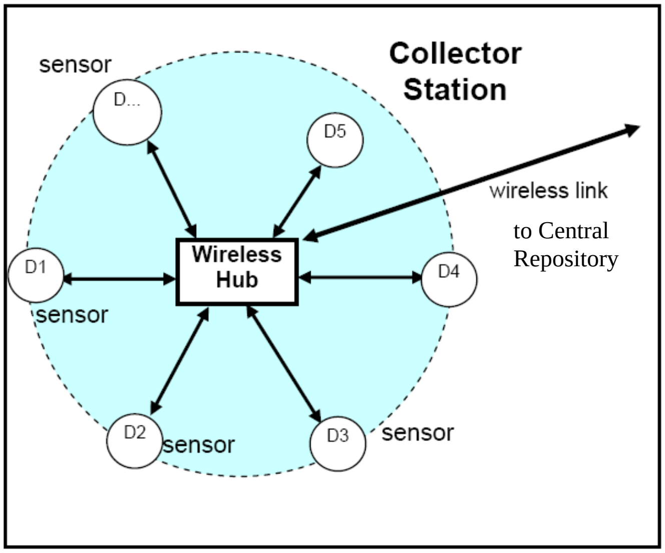


Figure 6: Star topology for a sensor network collector station

Sensor−to−Hub Connectivity using Zigbee at 900 MHz

Zigbee has its PHY layer based on IEEE 802.15.4 standards. It is organized in ten channels at 902 to 928 MHz frequency band in Canada (ISM bands, license exempted). The maximum data rate is 40 kbps for 900 MHz region (North America). For the surveillance system this capacity may be sufficient. Zigbee technology works on the principles of spread spectrum and has a chip rate of 600 kchips/s on the 900 MHz carrier. It employs digital modulation with BPSK (with 40 kbaud). Maximum output power obeys FCC Part 15 that limits radiation at 100 mW (20 dBm) for devices using omni-directional antennas (EIRP power). It operates with RF bandwidth of 1200 kHz in North America.

Hub-to-Central Repository Connectivity

The use of WiFi

The best known wireless technology today is WiFi for broadband communications in short distances. In certain cases WiFi can be used for backhaul (i.e. links with long range, greater than 10 km). WiFi can deliver a basic bit rate of 11Mbps in its simplest configuration and uses 20 MHz of signal bandwidth, which is enough bandwidth for transmission of even video signals. The configuration in the figure below is for a point-to-point link between the wireless hub and a central repository”

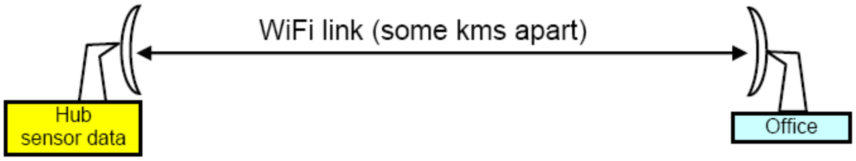


Figure 7: Point-to-point link provides sensor network/hub-to-central repository connectivity.

Frequency of 5.8 GHz for hub − Central Repository link

Power masks for 5.8 GHz are set by SITT/Industry Canada and follow FCC Part 15.407 for UNII bands. Radiated powers for the band 5.725–5.825 GHz is set to 17 dBm per 1MHz of frequency bandwidth for antenna gains below 6dBi. Maximum EIRP is 36 dBm (1W + 6dBi antenna gain). If transmitting antennas of directional gain are greater than 6 dBi, then the peak power spectral density is reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi. However, for fixed point-to-point U-NII devices, the use of directional elements up to 23 dBi is allowed without any corresponding reduction in the transmitter power spectral density. This means that point-to-point can put out up to 53 dBm of power. U-NII devices require additional awareness against interference to radar systems that may be located nearby the wireless system.

The Issue of Wireless Reliability in Remote Sites

The reliability of the communication system is often specified as a probabilistic number that represents the percentage of time the system operates without failure. In other words, it is the complement to the ratio between the system downtime (in hours or minutes) per year. If the failure F is the ratio of the system downtime/year, then reliability R = 1- F. In cities, it is common to find a cellular phone service operating with reliability greater than 99%. But in remote/rural communities this number is likely to be smaller than 99%. The degree of reliability of the communications link that is necessary for a monitoring station is related to the requirement of delivering sensor data. This requirement is often given in terms of a threshold number for maximum latency allowed. In other words, sensor data / processed data may be delivered with a delay that can vary from seconds to minutes. The system should be capable of handing this delay in data communication.

12.3.2 Operations Performed at the User Terminals

The following processing and control operations should be performed at the User Terminals:

Data Fusion

Recipient-received sensor information should be fused in order to provide a comprehensive operational picture of small boat activity in the region of interest. Fusion of kinematic and non-kinematic information, known as track fusion and decision fusion, respectively, should be performed at the User Terminals. The goal of data fusion is to combine boat track information obtained mainly from radars, and boat classification / identification information obtained mainly from EO/IR and AIS, based on similarity of location and features.

The track fusion algorithms can be classified as follows based of their approach for handling the cross-correlation among the local track errors:

- Algorithms that estimate and account for cross-correlation
- Algorithms that de-correlate the track estimates from different sensors
- Algorithms that assume the cross-correlation is unknown

The first type of algorithms requires computation of the exact cross-correlation [Li2003]. In most cases the exact cross-correlation can be obtained only if certain information, such as the individual sensor updates times and gains and state transition model corresponding to the sensor specific tracks is available at the User Terminals. This will require huge communication bandwidth. In [Saha1998] an algorithm to compute the steady-state cross-correlation matrix is presented to avoid transmission of the above information. However, a general solution does not work for vessels with different levels of manoeuvring capabilities.

The second type of track fusion algorithms attempts to de-correlate the track estimates [Drummond1997]. The decorrelated estimates are assumed to be independent and, hence, can be fused with the existing tracks at the User Terminals by using the minimum mean-squared error criterion. If process noise in small boat position prediction is ignored, this procedure generates optimal fusion results and requires communication of only tracks and their associated covariances to the User Terminals.

There are cases when the cross-correlation cannot be estimated and consequently the sensor specific tracks cannot be decorrelated. The Covariance Intersection (CI) algorithm is applicable [Julier2001] in such a case to obtain a consistent estimate. It should be noted that the fusion performance would be far inferior to that of the optimal one (assuming the knowledge of cross-correlation).

The second type of track fusion procedure - algorithms that fuse de-correlated track estimates from different sensors at the user terminals after determining which sensor-specific tracks are from the same small vessels should be used.

A decision fusion procedure is required to combine the detection/classification information from multiple sensors. With separate detection or classification operations from different sensors, decision fusion combines these individual results to obtain a final decision using specific fusion rules. The combination of individual results allows for the exploitation of complementary information, thus provide higher detection/classification performance than any single sensor. An optimal decision fusion rule can be derived in CFAR detection [Thomopoulos87] using a randomized Neyman-Pearson testing criterion. A decision fusion scheme that includes several bits of degree of confidence [Lampropoulos98] results in further improvements in system detection performance.

Decision fusion methods that utilize confidence information should be used by the system.

Decision Support Tools

Decision support tools generate alerts about unsafe, illegal, threatening and other anomalous small vessel activities [Seibert2006]. This frees the operators from anomaly detection activities and provides them with time to conduct threat analysis tasks instead. The decision support tools facilitate threat analysis by de-cluttering the surveillance picture according to criteria provided by the operators, such as boat type, boat direction and boat origin. In addition, long-term forward prediction picture of boat tracks (with highlighted uncertainty area) and track history information that should be provided by the system will help operators in their analysis.

Decision support tools should utilize the following information:

1. Geographical data, such as depth of water and location of fishing grounds
2. Unusual boat trajectory information, such as loitering in unusual location and rendezvous with a boat from a different country
3. Human Intelligence information, such as suspected boat type and possible location of illegal activity

For rule-based anomaly detection, end-users should configure the decision support tools by identifying anomalous behaviours, such as indicating an exclusion zone, restricted access zone, particular rendezvousing activity, cache drop activity, loitering activity, vessel speed limit etc. Exclusion and restricted zones can be defined as static (such as critical infrastructure) or dynamic (moving along with a target, such as moving vessels with dangerous or valuable cargo). A user interface, similar to the one in SeeCoast system [Seibert2006], is recommended for this purpose.

Tools should be provided in the User Interface and Decision Support module to allow operator interaction with the system. Drill-down tools in the User Interface module should allow operators to obtain and display information at different detail level, from the comprehensive operational picture of small boat activities in a particular region to the track history, detection/classification results, and even the raw sensor data for a particular boat. Operators should be able to configure the system such that the monitoring will be focused on areas of interest, e.g. adding, modifying and deleting exclusion zones, restricting access zones using drawing tools included in the User Interface module; and adjusting the alert threshold based on non-sensor information available to the operators, such as human intelligence. Input tools in the User Interface module should allow operators to confirm or disregard alerts raised by the system or decisions made by the system; this operator validation information should be saved for the system to learn and improve its decision making capability, which is the second type of anomalous behaviour detection procedure. This procedure learns normal traffic behaviour over time with or without input from the end user and detects boats whose position, speed or other characteristics differ from regular traffic for the season and/or time of day. A procedure for learning regular vessel traffic behaviour is available in [Rhodes2005], which is being used in the SeeCoast system.

The system should incorporate both rule-based and learning-based small vessel anomalous behaviour detection.

Sensor Control Tools

Sensor control tools, such as EO/IR camera pointing and zooming should be available to authorized end-users to enable them to scrutinize small vessels. The user should be able to indicate a particular location and configuration of sensors or indicate a small vessel from the list of tracks to be scanned. For the latter, track prediction capabilities should be provided in the user-terminal to determine scan parameters for user selected boats. Control of sensors should be provided based on the agency type and incident priority.

12.3.3 Inter-Subscriber/Inter-Group Shared Information (IGSI)

End users can fuse the data in the Central Data Repository with additional user specific data to generate a more comprehensive COP. Some users may want to share this picture (or a part of the picture) with another user. The IGSI is an additional feature that should be provided in such as a system and enable inter-group information sharing. It will allow a user, User A, to exchange information with another user, User B, without making this information visible to the others. Information shared as IGSI is not stored in the Central Data Repository and cannot be accessed by any user other than the intended recipient. The IGSI protocol should utilize a standard data exchange model such as the National Information Exchange Model (NIEM). The NIEM, developed in cooperation with the US Department of Homeland Security, provides a common set of standards and lexicon for intergovernmental information exchange across a variety of applications, including public safety, emergency and disaster management and homeland security among others, with the aim to make enterprise information sharing possible among various agencies and jurisdictions [NIEM2007].

IGSI creates a secure channel for information exchange between two users. Data security, as discussed in Section 12.3.1.5, should be implemented for the IGSI channels as well. IGSI is intended to act as a real-time information exchange feature. As a result, any information sent should be delivered to the recipient right away and should not be stored to future access. This will ensure additional information security and overcomes major buffering and storage issues.

IGSI is a useful feature that can benefit users immensely. IGSI can be designed to exchange text, images and voice information. In that regard, it can be viewed as a real-time secure chat system. The technology to implement this feature is available in the market. It involves client applications at the end-user terminals that connect to a server application running within the system. The server application coordinates data streams between any two users connected through a channel. Since the nature of the information to be exchanged is not clear at this time, further user input is required to design and develop this utility. Apart from the nature of information, users will dictate the degree of automation of the IGSI application and the level of integration with their local command and control centre.

12.3.4 Training

The system architecture is to be designed with an intuitive Graphical User Interface (GUI), with the assumption that operators will have maritime surveillance related background knowledge. As such, no extensive training should be required for operators; only a couple of days of training for operators to familiarize with the tools/procedures provided at the user terminal. Under normal circumstances and depending on the areas operators have to monitor, one to two operators should suffice for full surveillance capabilities. For everyday monitoring, one operator is enough to watch over the area of interest and perform routine analysis; however, when suspicious behaviour appears, the operator may need assistance from others to perform more specific analysis on the suspicious boat(s) while he/she continues the routine monitoring procedures.

12.3.5 Long Term Capability Enhancements

In the long-term, if information sharing between departments and agencies becomes more open, the scalability of the system should allow for any sensor data available to the end user to be easily added to the system following the “Sensor I/O Interface” and/or “Stakeholder I/O Interface” definitions and shared with other authorized end users. Thus original recipients can in essence also become data contributors. Such a system will provide a central repository for contributors and recipients of data to transact, and will be self-sustained through the expansion of the user network.

12.4 System Benefits

VINCENT is designed to address the technological capability gaps discussed in Section 11. It is configured to not only collect information about small vessels, but rather about all vessels as means of creating a complete COP. By obtaining all relevant information, users will be able to dismiss compliant targets and zoom onto the non-compliant one’s for further investigation.

In terms of the organizational gaps, this concept provides a common platform applicable to various departments and jurisdictions, with each stakeholder choosing the specific data streams that are of relevance to them. Also, it does not require federal departments to share sensitive information with each other if they cannot or do not wish to do so. From an operational perspective, the ability to engage non-governmental stakeholders in the process will reduce the need for governmental resources – both in terms of assets and personnel to be dedicated to this initiative. Finally, the utilization of the most advanced technologies will ensure that tools that are best equipped for small vessel surveillance tasks in particular are utilized by the system and available to stakeholders.

The system will provide end users with the requested sensor data and corresponding processing results (detection, estimation and classification/identification), sensor data fusion, decision support and sensor control capabilities. For users with their own data fusion and decision support tools, the system will provide additional information helpful for obtaining enhanced operational picture, which will lead to better utilization of surveillance and interdiction assets. The sensor control capability provided by the system will further help in this direction.

For users with limited tools, the system will also provide data fusion capability. Fused information helps to obtain compact representation of the data which in turn helps in reducing the time required to make decisions. For example, radar generated tracks linked with EO/IR images, AIS identity information and/or other features help in achieving high-accuracy automatic decision-support, which in turn helps in timely decision making by operators.

A layered display, which is part of the decision support system, will assist in clutter reduction based on user selected criteria of boat type, origin, destination etc. Considering the large number of small vessels particularly during the summer months, this will enhance the operators' ability to investigate suspicious vessels. Decision support tools provided in the system will enable fast detection of anomalous small vessel behaviour (such as rendezvous, loitering, speeding etc.) based on user-provided rules, as well as normal behavioural patterns learnt by the system. Other than anomalous behaviour detection, the system will also assist in securing static targets (such as critical infrastructure sites) and dynamic targets (such as vessels with dangerous or valuable cargo).

This concept could also provide census/ demographic pattern data, such as the number of vessels in a particular area and the type of vessel; information that can be used by authorities for better targeting of security efforts. To illustrate the VINCENT concept in operational scenarios, examples are presented in Section 12.5 outlining how the described multi-sensor surveillance system will enhance Canada's ability to prepare for, and respond to, high consequence public events arising from the small vessel treat.

12.5 Operational Scenarios

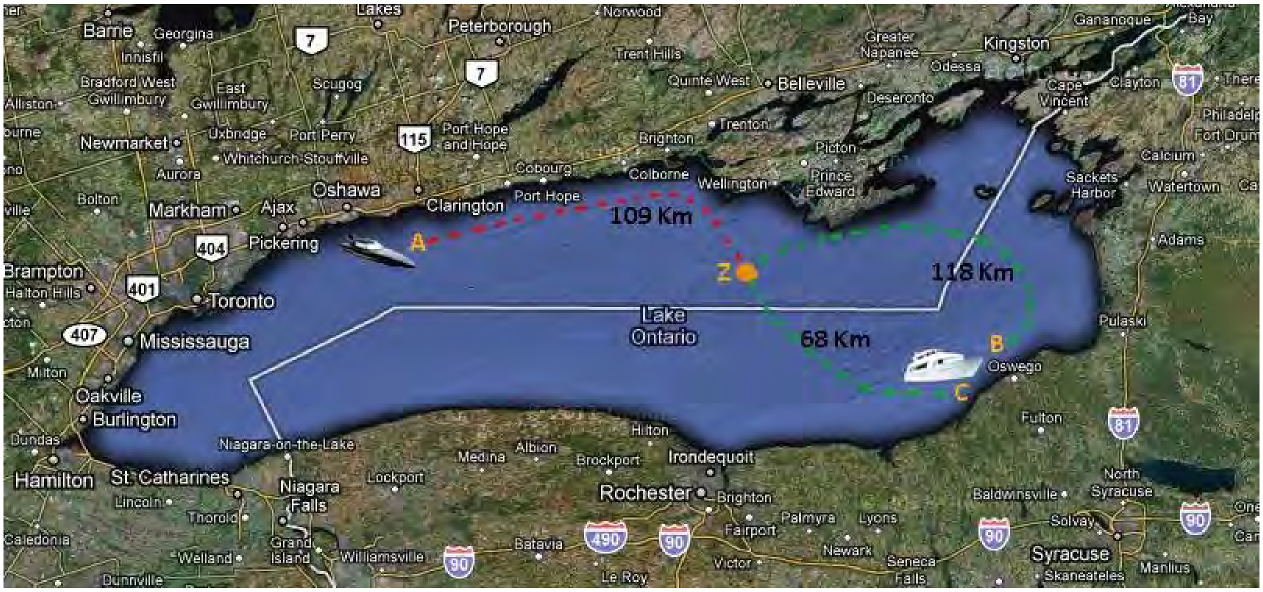
12.5.1 Gun Smuggling Scenario

In preparations for a gun smuggling operation, the American smuggler purchased a small fishing vessel and registered it under his name. He then took the license number off that boat and put it on another, a more high-end Yacht, thinking that law enforcement personnel will be more reluctant to search this type of boat without clear evidence of criminal activity. He went on and bought sophisticated fishing equipment, as well as bait, beer, fish, and food in order to properly disguise himself as if he was coming from a leisurely fishing trip. He planned to meet his partner in crime, who will be arriving on a speedboat from Oshawa, Ontario (Point A) later that day, exchange cargo with him, and return to his home base in Oswego, NY (Points B, C). The meeting point (Point Z) is about 25 Km south off Wellington, ON, just above the Canada-US border.

The Canadian smuggler was to use a speedboat. He was to secure the cargo and quickly transport it back to Oshawa, Ontario. He also switched the registration of the boat from Canadian to U.S. He had sophisticated equipment on board that allowed him to interdict the high-frequency radio signals used by law enforcement personnel.

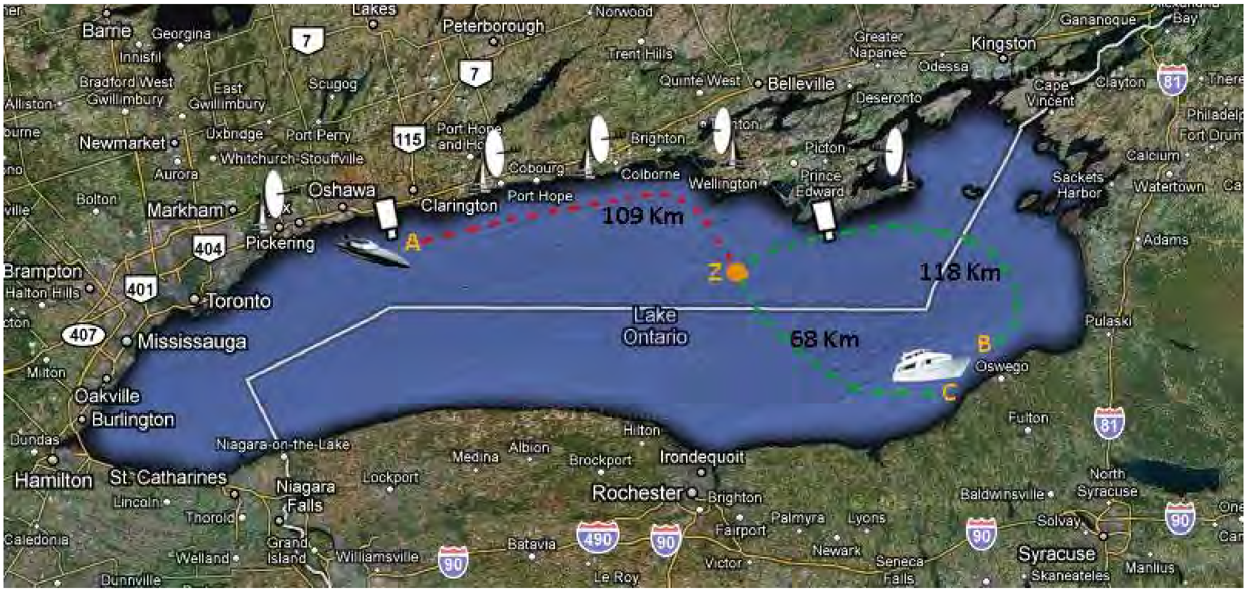
Since the smugglers wanted to blend in with the normal traffic of sailors and fishermen, they decided that a Saturday departure would be best as the number of small boats increases during the weekend. They also got acquainted with the normal traffic of patrols in the port of Oswego and the neighbouring marinas along the route both in NY and Ontario.

The Canadian speedboat will travel from Point A to Z (109 Km distance), and return back using the same route. The US yacht will travel from Point B to Z (118 Km distance), drop the cargo, and return back from Point Z to Point C (68 Km distance).



Yacht speed: 40 Km/ hour
Speedboat speed: 90 Km/ hour

How VINCENT can help:
The system will provide comprehensive coverage of Canadian waters using radars. While radar will provide excellent detection and tracking capabilities, cameras placed at ports/marinas and other strategic locations provide classification/identification capabilities and AIS receivers provide support in clutter reduction and anomaly detection. The figure below shows possible locations of microwave radars and EO/IR cameras that are helpful for detecting the smuggling operation and identifying the boats used in the scenario discussed above. It is assumed that the specific user is interested in activity of boats in Lake Ontario and, hence, receives all relevant radar, AIS and camera information available in that region.



The yacht coming from Oswego, NY, is detected by radar before it enters Canadian waters and its path is tracked. Radar detection and tracking operations are performed at the central repository. These tracks are available to the specific user. The decision support module, available to the specific user, automatically directs a camera strategically placed near the shore in Prince Edward County to take a picture of the yacht when it comes in close proximity to the shoreline (less than 10km distance in this case). The accurate track obtained by radar data processing helps to accurately direct the camera toward the yacht. The picture is analyzed at the data central repository to detect the boat and classify the boat as a yacht. At the user end, the fusion algorithm links the yacht picture with the yacht track. As specified by the particular user, the operation to obtain the picture is performed for all boats in Lake Ontario when they come close enough to the camera locations.

Pictures are taken regularly by a camera placed at the marina in Oshawa, Ontario. At the central repository, the pictures are analyzed to detect boats, classify them and determine their trajectory. These processing steps provide information about boats arriving and leaving the marina. By processing the radar data at the central repository, the speedboat track is obtained. The speedboat track and its picture are connected by the fusion algorithm at the user end.

The decision support system at the user end detects rendezvous between two boats coming from different origins and raises an alarm. An operator, based at the user location, analyzes the situation by looking at the boat trajectories and associated pictures. When the boats begin to depart from one another, the operator decides that the situation calls for further investigation and alerts proper authorities about the incident. Based on the operator input and accurate tracking information, the boat is searched when it reaches the Oshawa marina and the smuggled items are found. The US counterpart of the user is informed about the incident. The yacht’s trajectory and other information are provided to US authorities to act upon.

The apprehension discussed above is assisted by technologies such as **automatic control** to direct camera towards the boat, **detection** of small boats in images, feature aided **tracking** capable of ambiguity resolution and reporting, **fusion** of tracks and images, and rule-based **decision support**. Currently, these tools vary in their levels of maturity, are scattered across a variety of defence applications and are not combined together and utilized as part of the small vessel surveillance strategy. The ability to combine these essential small vessel surveillance technologies in a single system is key to prevention and interdiction of asymmetric threats.

12.5.2 Additional Scenarios

In the following we provide brief descriptions of further scenarios considered during this study, the unique challenges they present and how the system concept described above can help marine stakeholders in these situations.

Additional scenario 1: Intelligence information collected by various domestic and international sources indicates that a shipment of narcotics is set to arrive within a two week window. The suspect vessel is described as: small commercial fishing vessel estimated at 120 feet with a 90-tonne displacement. Further source information indicates that the vessel will not dock in a Canadian port until the narcotics have been off-loaded. Rendezvous with smaller fast boats will take place and proceed independently to differing docking points. No information has been provided to identify the operators or location of the small boats, nor where the rendezvous will occur. This scenario is likely to occur in the coastal regions of Canada.

The key challenge in this case is tracking of the vessel among numerous fishing vessels or fishing fleets and the number of nearby islands and inlets that can provide concealment. The system concept developed in this project will be able to track the vessel through unobservable stretches by using the geographical knowledge and performing long-term track prediction. The system will perform track ambiguity resolution using features obtained by sensors, such as EO/IR. The decision support module will help the operators to follow all boats fitting the vessel description and then pinpoint the particular vessel based on its unusual track and/or rendezvous behaviour.

Additional Scenario 2: Vessel number one departs a US residence on the shores of the St. Lawrence near 1000 Islands area and proceeds at a normal speed toward the Canadian border. The course and speed are typical for other vessels in the area. The vessel comes to a stop and loiters. A similar vessel departs a Canadian residence on the shores of the St. Lawrence in the Kingston region and proceeds at a normal course and speed as other vessels on the water. The vessel is proceeding to the vicinity of the suspect US vessel. The vessels have now rendezvoused and are now observed as one larger contact by surface radar (if not in a blind spot where coverage is not possible). Within 15 minutes of rendezvous, both vessels depart and proceed out of the area. Another possibility is potential use of drop-off points, where cargo may either be dropped onto the surface of the water for pickup (not likely in day conditions) or where cargo is dropped into the water with anchor. When this method is used, the location of the drop-off is provided by the transfer of a GPS unit that has the way-point established in order to re-locate the drop site. In the case of a cache drop, it must be understood that such locations will need to be in an area where the current is minimal, where depth is minimal (for fast retrieval) and where detection is also minimized. There is no necessity for the drop-off and pickup to occur within the same time frame. The risk of detection is reduced by creating several hours or even days between both events.

The challenges in this scenario are high concentration of vessels on the St. Lawrence Seaway and the narrow response time. High pleasure-craft activity makes separation of loitering and recreational activity difficult. In the case of a cache drop, a time interval between the pick-up and drop-off event means such events cannot be detected by looking for rendezvous behaviour. In this scenario the narrow waterways, which appear to be providing cover for unlawful activities, make application of high resolution but short range sensors possible. The conceptual system will use strategically placed (this will minimize blind spots), high resolution and short range radars and EO/IR sensors that ensures that boats will be detected from their onset and tracked robustly (without ambiguity). The decision support system will also utilize high sensor resolution to detect and document rendezvoused boats more accurately. In addition, geo-spatial information as well as loitering events of boats at the same location but different times will be utilized for detection of cache drop events. Unusual boat behaviour, such as night-time loitering near remote locations for surface drop-off, will be a giveaway of the criminal activity.

Additional Scenario 3: A boat departs a private area on the waterfront, one that permits the attachment of a parasitic pod to the hull by use of divers which is then removed when the boat reaches its destination. Parasitic pods may be fixed to the hull by use of a ‘C’ clamp often used to carry the pod to the keel of the vessel or other manufactured fittings on the hull below the waterline. Such a vessel would be compliant with all normal vessel regulations, and behave like all other vessels on the water. It is also possible that the occupants of such a vessel may not be aware that they are transferring a parasitic pod. Additionally, such activity also makes commercial vessels susceptible to be utilized as a smuggling mule without knowledge of the Master, crew or occupants.

Underwater surveillance by Sonar will be required for detection of parasitic pod placement and retrieval events. If required by the end user, the system concept discussed above will incorporate Sonar information in the COP and the decision support module will use it to detect such events.

Additional Scenario 4: Contraband cargo is loaded into the vessel (pleasure craft) at an undisclosed location, and sheltered with boat cover. The vessel is taken by trailer to the launch point, but will remain on the trailer until the pickup party is in place and ready to receive the cargo and or vessel. When it is determined that all parties are prepared and enforcement agencies are not in the area, the suspect vessel is launched and proceeds to the drop location at high speed. Often, both parties are within sight of each other, and light signals or other visual signs are used to initiate the operation. As the suspect vessel arrives to the delivery location, the receiving party either places a boat trailer to recover the suspect vessel and departs the area, or the cargo is removed and transferred to a waiting vehicle. This scenario is also favourable for the use of kayaks, canoes or other low freeboard vessels made of plastic or fibre-glass which presents a small radar cross-section.

The short time span of the operation and minimal loitering provides unique detection challenges in this case. The decision support module of the conceptual system will utilize the unusual movement of boat between two jurisdictions to raise a flag and direct EO/IR sensors to gather more information. The event will be analyzed by an operator based on boat track and fused EO/IR information and the event will be detected. Low Signal to Noise Ratio (SNR) target detection procedures based on radar and IR data, discussed as part of the processing capabilities of the conceptual system will enhance detection of small radar cross-section vessels.

Additional Scenario 5: A vessel originating from Detroit moves closely to the Canadian shoreline of the Detroit River. The boat makes several passes and then the front passenger throws a bag onto an abandoned dock. A car approaches, picks up the package and leaves the area.

The challenge in this case is that the boat never stops and, hence, it will not raise suspicion in a conventional system. The system concept described will use the fact that the boat is performing repeated loops in a known smuggling area to raise a flag and direct EO/IR sensors to gather more information. An operator will be able to detect the event based on the fused EO/IR and track data. Details about the boat, car and package will enable the authorities to take action against these criminals.

12.6 Capability Roadmap

This Capability Roadmap outlines the steps by which VINCENT will become operational and sets the long-term goals for the development of the VINCENT capabilities through to 2018. The Roadmap includes a 7-year timeframe. Of course it is presumed that VINCENT will be operational for a longer period of time and enhancements will be made to the system after this initial time period, but those activities are not within the scope of this Roadmap.

Underpinning the capability requirement are three key components:

1. the Technological Component
2. the Operational Component
3. the Organizational Component

All three components require development in order to realize the full potential of a future VINCENT capability. The Roadmap identifies key actions in each of these components necessary to set the stage for full implementation of VINCENT. These actions are:

Year/ Component	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**VINCENT OPERATIONAL**
Technological	Develop technologies in low TRL levels to TRL 9		System integration (no communication component)	Communication system interface development	Demonstration and refinement		Full system deployment		
Operational	Vulnerability studies	Resource evaluation	Interdepartmental doctrine development and data sharing agreements	End user education		Establish network that links data contributors and recipients for requirement gathering		End user training	
Organizational			Establish an agency responsible for oversight of VINCENT	Enable programs that encourage sensor infrastructure development and associated standards					

Table 9: Capability Roadmap

12.6.1 The Technological Component

The technology development roadmap consists of five stages: develop technologies with low Technology Readiness Level (TRL) values to TRL 9; system integration without communication component; communication system interface development; demonstration and refinement; and full system deployment.

Technology Readiness Level analysis[2] was conducted for the technologies that are to be used in VINCENT:

Technology Group	Specific Technology	TRL	Explanation
Detection	*Ordered Statistics CFAR*	9	The OS CFAR is already a part of operational systems such as the Marine Small Target Tracker (MSTT) deployed for surveillance of Straits of Gibraltar and waterways near New York Airports [Ponsford2011].
	Track-Before-Detect	5	The effectiveness of track-before-detect (TBD) algorithms, such as ML-PDA [Chummun2002] and EM-ML [Cai2005] was successfully demonstrated on a 78-frame long wave infrared (LWIR) data sequence consisting of an F1 Mirage fighter jet in heavy clutter, collected during the Laptex data collection in July 1996 in Crete, Greece. In addition, the effectiveness of ML-PDA in bistatic sonar application was demonstrated in 2003 by [Willett2005] based on DEMUS (deployable multistatic sonar) data sets from sea trials. However, an extensive real-data based trial has not been performed on TBD procedures, particularly for small boat detection. There are other track-initiation procedures, similar to track-before-detect, which are already operational. The Jindalee tracker [Colegrove1999], for example, uses a PDA filter with a non-uniform clutter model and performs multiple velocity model based initiation.
	EO-image based small boat detection	3	Although EO images are used for other types of object detection [Yang2008], small boat detection

[2] The analysis does not provide information about Technology Maturity Levels (TML), which combines TRL information with interface maturity level, design maturity level, system readiness level, and manufacturing maturity level [Hobson2006]. TML values for technologies are in general identical to the corresponding TRL values. However, in cases of track fusion and learning-based decision support there are lags in design maturity level and system readiness level. The overall TRL of the system is 3 as proof of concept studies have already been completed for all component technologies. The TML of the overall system is 2 as interface requirements are specified and understood, but not demonstrated at modular level.

			in water is a new type of application and the development of a detection procedure for it is required.
Tracking	*ID-aided tracking*	3	Recently, a set of simulation results provided the proof of concept [Sinha2010].
	Probabilistic Data Association (PDA) filter	9	PDA filters are already operational. An example is a Joint PDA (JPDA) filter that processes the already established tracks for Jindalee Over the Horizon (OTH) radar [Davey1998].
	Extended Kalman Filter (EKF)	9	EKF is possibly the most widely used dynamic parameter estimation algorithm for nonlinear systems [Julier2004] and EKF is part of many operational tracking and other systems [Jassemi-Zargani2002].
	Unscented Kalman Filter (UKF)	9	UKF is already operational in target tracking, navigation and other dynamic estimation applications.
Classification / Identification	*Training based classification approach – EO boat classification*	3	Training based object classification has been used in other domains. For example, image based object classification [Yang2008] and landmark recognition [Cummins2009] have shown great degrees of success. However, the application of this technology for classification / identification of small boats is not mature.
	Radar-based boat size classification	9	Target size classification based on radar signature is a mature technology which is deployed for different surveillance applications, including boat size classification [Nohara2010].
	IR signature based classification	3	IR signature-based boat classification is successfully applied to images taken by airborne sensors [Giompapa2007]. However, the technology is not mature, particularly when considered for small boat classification.
Data Storage	*Network storage architecture capable of handling large volume of data*	9	Network Attached Storage (NAS) and Storage Area Network (SAN), which are considered for the system, are commercially available.
Data Fusion	*Track fusion*	6	The tracklet fusion method has been extensively studied in tracking literature. The fusion performance of tracklet fusion is also demonstrated in simulation environments [Barker1998]. However, we could not find any operational fusion systems that use tracklet fusion.

	Decision fusion	4	The recommended decision fusion procedure [Lampropoulos1998] has been tested only in laboratory environment.
Decision support	*Rule-based decision support*	9	Rule-based decision support is available commercially for marine surveillance [Seibert2006,Nohara2009].
	Learning-based decision support	5	Learning-based decision support tools, although available commercially [Seibert2006], are not a mature technology. Available approaches need to be further tested and refined.
Sensor control Tools	*Radar control tools*	9	Software control of radar scan is a mature technology already in use for over-water surveillance.
	EO/IR control tools	9	Software control of camera is a mature technology.

Table 10: TRL Evaluation

The results of this analysis indicate that there are several technologies that require TRL improvements:

1. Track-before detect,
2. EO-image based small boat detection,
3. ID-aided tracking,
4. Training based classification approach – EO boat classification,
5. IR signature based classification,
6. Track fusion,
7. Decision fusion,
8. Learning based decision support.

In case any of the above cannot be developed to the point of commercial readiness, a risk mitigation plan should be employed. If alternative procedures with TRL 9 are available, such as the case for the Multiple Hypothesis Tracking (MHT) as an alternative to ID-aided tracking, these techniques should be considered as contingency plans. A Go / No-Go decision should be part of the process to ensure the technology development is progressing as planned. In cases where an alternative with TRL 9 is not available, such as the case of learning based decision support, more than one lower-TRL technologies should be initially evaluated as a mitigation plan and only the most promising one would be fully developed.

After all lower TRL technologies have been upgraded to TRL 9, technologies already at TRL 9 should be acquired and the system should be integrated and tested without the communication component. The next stage of integration would include communication and the corresponding interfaces. Following this, a demonstration project should be initiated and system refinements should be executed based on system performance and end user feedback. The last stage of technology development would be the deployment of the complete system.

12.6.2 The Operational Component

The first step in ensuring the operational component is met is the study of vulnerable areas. Risk assessment studies should be conducted to ensure that locations that are most sensitive are secured first. The next step is the evaluation of current resource availability, to determine if there are, and if so how many resources (both in terms of personnel and assets) are available and could be utilized for the purposes of VINCENT. In the absence of a clear leading agency responsible for maritime surveillance, it is also important to develop a shared interdepartmental doctrine specifying the strategy and tactics that will be employed to ensure robust and persistent small vessel monitoring as well for the agencies to develop data-sharing agreements with one another.

The next step is end user education regarding system capabilities and how the system meets their operating requirements and may assist them in executing their duties. Following this is the establishment of a network that will link data contributors and recipients, encourage data contributors to participate and assist in understanding market requirements. Lastly, end user training seminars should be conducted to provide users with an in-depth understanding of the system and the functionalities it has to offer. Training seminars will not only be conducted during this final year before VINCENT becomes operational, but rather will be offered on a rolling basis, with refresher seminars offered at regular time intervals.

12.6.3 The Organizational Component

An essential step for full implementation of VINCENT is the assignment of an agency that will be responsible for the oversight of this system. This does not imply that this agency will necessarily be responsible for Canadian maritime security as part of its mandate, but will rather guarantee that the suitable coordination is provided to ensure the proper and timely development of the system.

Another crucial step for the success of this initiative is the development of programs that will encourage sensor infrastructure development and the associated standards. These programs should have make funds available for organizations interested in becoming data contributors to ensure there is adequate initial funding required for infrastructure development projects of such scope. The standards that will apply to such networks should also be identified at that point.

12.7 Legal/ Privacy Considerations

There are several considerations that must be given to privacy concerns associated with this system concept. The growth and development in recent years in identification technologies make gathering information much easier, given the right technologies are in place. Advanced detection, classification and identification tools can provide data recipients with much more information that is required for crime prevention. Special consideration must be given to *The Personal Information Protection and Electronic Documents Act*. Any information collected via the surveillance tools described in this report must not violate this Act. Recent advancements in video surveillance encryption technology, such as the Secure Visual Coding Solution developed in the University of Toronto, make images of individuals completely obscure and can later be decrypted upon demand for further investigation [UofT2010]. These types of technologies make the use of EO/ IR cameras for detection purposes possible without having to face the legal and privacy constraints.

Law abiding citizens may protest continuous surveillance programs as those may hinder their ability to go about the daily life in a manner they are accustomed to, given that they may feel that the authorities are watching their movements. To counter this, authorities should show that the use of such technology has much greater benefits to the public as a whole that the limitation it enforces on the boating community.

With regards to the data Contributors, organizations that are outside of the government or Crown agencies would have to be cleared with a security screening before being able to participate or ‘plug-in’ to the system. Anyone working with or for the government in a security capacity will need clearance.

Radiation emitted from radars and noise pollution generated from Sonar present ethical concerns. Placement of these sensors must be strategic in order to minimize the effect on the population and marine life. Trade-off studies and cost-benefit analyses must be conducted in order to optimize sensor placement strategy. Assessments should also take place to review the effects that the system will have on the boating community, the general public and the surrounding ecosystem.

13. Policy Considerations

As discussed throughout this report, the key capability gap associated with maritime surveillance in Canada is the system of diffused responsibility and no single governmental body that has the overall accountability for the security program. The output of this study takes into account this fact, and recognizes that such a change in policy is not likely to transpire in the near future. As such, the recommendations of this study are constructed given the current legislative constraints. Technology can be used to complement plans and initiatives, but cannot be looked upon as the sole answer to improved maritime security. As such, the system architecture that is presented in the work was developed given the current organizational construct.

While outside the scope of this study, it is important to note the benefits and impacts on other identified capability gaps and border security in general should systematic organizational changes take place.

Assuming the formation of a centralized body that would oversee all activities pertaining to maritime security and surveillance, proper resource coordination across border enforcement agencies would be accomplished. Funding would also be disbursed with a unified, long-term strategy to enhance border integrity Canada-wide. In addition, a central repository of information and intelligence would enable a more complete Common Operating Picture, streamlining surveillance and interdiction efforts based on maximal situational awareness. For such a change in organization and ease of information sharing to occur, significant legislative changes need to take place.

Other policy considerations can be found in the Strategic Advice Note of this study, included as a separate attachment.

14. Conclusion

The purpose of this study was to support Public Security Technical Program's (PSTP) Border and Transportation Security (BTS) Community of Practice (CoP) via the evaluation of potential technologies and techniques that could enhance Canada's border security, with a focus on persistent small vessel surveillance in the Maritime, Great Lakes, and St. Lawrence Seaway border regions.

Via a systematic and interdisciplinary analysis, three major capability gaps relating to the security of maritime, Great Lakes and St. Lawrence Seaway border regions were identified. The first gap relates to the system of diffused responsibility and jurisdictional approach that introduces hindrances in inter-departmental communication, information sharing, and resource acquisition and deployment, resulting in lack of coordinated intelligence efforts and diminished capacity to protect the integrity of the border. Improving this aspect of the security program could entail the assignment of a single government agency responsible for centralized planning and coordination with other departments to ensure all relevant information is captured in the surveillance strategy.

The second gap relates to availability of resources, both in terms of assets and personnel. In the absence of a leading agency, numerous departments compete for scarce funding to support their mandates. Considering the already tight budgetary constraints faced by most government departments, an effective resource coordination and positioning strategy has to be developed to maximize the effectiveness of such resources.

The third gap relates to sensors and other technologies, where there is a necessity for suitable sensor selection, followed by their strategic placement based on Threat Risk Assessment matrices, and data processing technologies that need to be effectively combined and implemented in the context of small vessel surveillance. This will enable a layered approach to the display of a Common Operating Picture. Currently, these tools vary in their levels of maturity, are scattered across a variety of defence applications, and are not combined together to provide a unified small vessel persistent surveillance capability. The ability to combine these essential small vessel surveillance technologies in a single system is key to prevention and interdiction of asymmetric threats.

In light of the given capability gaps and limitations, a multi-sensor surveillance system that accommodates the various jurisdictional differences that currently exist was designed. The multi-sensor architecture provides a common platform that can be utilized by users with specific departmental mandates and does not necessarily require any government departments to invest in installing and maintaining infrastructure, with non-governmental stakeholders engaged in supplying critical data. Sensor and signal processing technologies were reviewed, and recommendations were made as to which are best suited for the task of small vessel surveillance, and should therefore be considered for inclusion in the system. A Capability Roadmap was also developed, describing the technological, operational and organizational modifications that are required in order to operationilize the system. These outputs are based on the assumption that changes in jurisdictional issues will not occur in the foreseeable future, and as such, the solution aims to mitigate the jurisdictional challenge by the use of operational modifications and technological advances.

References

A STUDY ON MARITIME SECURITY MEASURES FOR NON-SOLAS VESSELS (May 10, 2005), The JAPAN INTERNATIONAL TRANSPORT INSTITUTE (JITI)

Asada A. et al (2007), *Advanced surveillance technology in underwater security sonar systems*, Proc. of Oceans 07, Aberdeen, England (CD-ROM). 061213-002

AUG Signals (2007), *Deployable Web-Based Multi-Sensor ATD/ATR Intelligent System for Real-Time Maritime Surveillance*. Defence Industrial Research Program, DIR # 542, Final Report

Avis, P. (2003). *Surveillance and Canadian Maritime Domestics Security*. Canadian Military Journal (Spring), 9-14

Bar-Shalom, Y., Li, X.R. (1995), *Multitarget-Multisensor Tracking: Principles and Techniques,* YBS Publishing

Barker W., Mori S., Sullinger E. G., Boe M., (1998), *Data Fusion Processing for the Multi-Spectral Sensor Surveillance System*, IRIS proceedings

Brandao, A. (April 2011). *Wireless Connectivity for the Monitoring of Water Quality and Environmental Data from Rural and Remote Sites in Canada*. Draft Version 2. Communication Research Centre Canada.

Blake T.M. (2004). *Development of a rapidly re-deployable hf radar concept*. First EMRS DTC Techn. Conf., Edinburgh

Blackman, S.S. (1986), *Multiple Target Tracking With Radar Applications*, Norwood, MA: Artech House

Blackman, S. (January 2004), *Multiple Hypothesis Tracking for Multiple Target Tracking*, IEEE A&E Systems Magazine, Vol. 19, No. 1

Brooke S.D., Lim T.Y., Ardron J.A., (2010) *Surveillance and Enforcement of Remote Maritime Areas.* Paper 1: Surveillance Technical Options. Marine Conservation Biology Institute, USA. Version 1.2.

Brown, B. (2003). *Threats in N. American Waters*. Transport Canada Security Inspector Course. Transport Canada

Brownstein C. (19 October 2007), *REPORT OF THE DHS NATIONAL SMALL VESSEL SECURITY SUMMIT*, Department of Homeland Security, HSI Publication Number: RP07-12-01

Cai J., Sinha A., Kirubarajan T., (April 2002) *EM-ML Algorithm for Track Initialization using Possibly Noninformative Data*, IEEE Transactions on Aerospace and Electronic Systems, Vol. 38, No. 2, pp. 694—707

Carafano, J. J. (2007). *Small Boats, Big Worries: Thwarting Terrorist Attacks from the Sea. The* Heritage Foundation

CFN Consultants. (2008). *The Maritime and Port Security Demonstration Project Workshop*

Chummun M. R., Bar-Shalom Y., Kirubarajan T. (April 2002), *Adaptive Early-Detection ML-PDA Estimator for LO Targets with EO Sensors*, IEEE Trans. on Aerospace and Electronic Systems, Vol. 38, No. 2, pp. 694-707

Colegrove S. B., (June 1999), *Advanced Jindalee Tracker: Probabilistic Data Association Multiple Model Initiation Filter*, Defence Science and Technology Organisation Technical Report No. DSTO-TR-0659

Corbane C., Marre F. and Petit M. (2008) *Using SPOT-5 HRG Data in Panchromatic Mode for Operational Detection of Small Ships in Tropical Area*, Sensors 2008, Vol. 8, pp. 2959-2973

Crisp D. J., *The State-of-the-Art in Ship Detection in Synthetic Aperture Radar Imagery*, DSTO–RR–0272

Cummins M., Newman P., (June 2009), *Highly Scalable Appearance-Only SLAM - FAB-MAP 2.0*, Robotics Science and Systems

Davey S. J., (November 1998), *A Multi-Target Tracker for the Jindalee Over the Horizon Radar*, Masters Project Report, University of Adelaide

Department of Homeland Security. (2008). *Small Vessel Security Strategy*

DJC. (2010, December 14). Marine Transportation Security Regulations (SOR/2004-144). Retrieved January 8, 2011, from Department of Justice - Regulations: http://laws.justice.gc.ca/eng/SOR-2004-144/20110108/page-1.html?rp18=false

Drummond, O.E., (1997), *Tracklets and a Hybrid Fusion with Process Noise*, in proc. of the SPIE Signal and Data Processing of Small Targets, vol. 3163

Edwards, R. H. (2004). The Future of Canada's Maritime Capabilities: The Issues, Challenges and Solutions in a New Security Environment

Ferriere, D. (n/a). *Using Technology To Bridge Maritime Security Gaps.* National Infrastructure Institute Center for Infrastructure Expertise. Portsmouth: NIICIE

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

Frappier, G. (2002). Marine Security: Canada's New Reality. *Security & Emergency Preparedness.* Vancouver

Frappier, G. (2003). Seaport Security: A Front-Line Update. *Association of Canadian Port Authorities Port / Government Interface*. n/a: G. Frappier, Director General, Security & Emergency Preparedness, Transport Canada

García J. et al (2010), *Robust Sensor Fusion in Real Maritime Surveillance Scenarios*, International Conf on Information Fusion 2010

Garnett, G.L. (2003) The Evolution of the Canadian Approach to Joint and Combined Operations at the Strategic and Operational Level. *Canadian Military Journal*

Gendron A. (December 2010), *Critical Energy Infrastructure Protection in Canada*, DRDC CORA CR 2010-274

Gillis, Matthew. (20 January 2011) *Navies and Coast Guards: Relationships, Mandates, and Options for Reform*. Centre for Foreign Policy Studies Seminar Series.

Giompapa S. et al, (2007)*, Naval target classification by fusion of IR and EO sensors*, SPIE Conf. on Electro-Optical and Infrared Systems: Technology and Applications, Vol. 6737

GLC. (2007, July 11). *Great Lakes Commission*. Retrieved November 30, 2010, from Great Lakes Recreational Boat's Economic Punch: http://glc.org/recboat/pdf/rec-boating-final-small.pdf

Governments of the United States, and Canada. (2007). *Drug Threat Assessment 2007*. N/A: N/A

Graham, R. (2006). *Transformation and Technology: A Canadian Maritime Security Perspective*. Technological Innovation and Maritime Security

Hadzagic M., Michalska H., Lefebvre E., (August 2005) "Track-Before Detect Methods in Tracking Low-Observable Targets: A Survey", Sensors & Transducers Magazine (S&T e-Digest), Special Issue, pp. 374-380

Hammond T., Pelot R., Leadbeater N. (2011*). Sensor Interaction for Small Ship Tracking and Awareness in Harbour*. Public Security S&T Summer Symposium. Conference Proceedings. Pg. 89.

Hammond T. (2006), *The Implications of Self-Reporting Systems for Maritime Domain Awareness*, DRDC Atlantic TM 2006-232

Herselman P. L., Baker C. J., and de Wind H. J. (2008), *An Analysis of X-Band Calibrated Sea Clutter and Small Boat Reflectivity at Medium-to-Low Grazing Angles*, International Journal of Navigation and Observation, Volume 2008

Herselman P. L. and De Wind H. J. (Sept. 2008), "*Improved covariance matrix estimation in spectrally inhomogeneous sea clutter with application to adaptive small boat detection,*" in Radar, 2008 International Conference on, pp. 94–99

Hill, Brian .P. (March 2009). *Maritime Terrorism and the Small Boat Threat to the United States: A Proposed Response*. Master's Thesis, Naval Postgraduate School.

Hill D., Nash P. (2005) *Fibre-optic hydrophone array for acoustic surveillance in the littoral*, Proceedings of SPIE, Photonics for Port and Harbor Security, 5780, pages 1-10

Hobson, B., (2006), *A Technology Maturity Measurement System for the Department of National Defence*, DRDC Atlantic CR 2005-279

Hu J., Tung W.W. and Gao J. B. (2006), *"Detection of Low Observable Targets within Sea Clutter by Structure* Function based Multifractal Analysis", IEEE Transactions on Antennas and Propagation 54, 136-143

Jassemi-Zargani R., Necsulescu D., (December 2002), *Extended Kalman Filter-Based Sensor Fusion for Operational Space Control of a Robot Arm*, IEEE Trans. on Instrumentation and Measurement, Vol. 51, No. 6

Julier, S.J., Uhlmann, J.K. (1997), *A New Extension of the Kalman Filter to Nonlinear Systems*, In Proc. of the 11th Int. Symp. on Aerospace/Defence Sensing, Simulation and Controls

Julier, S.J., Uhlmann, J.K. (2001), *General Decentralized Data Fusion with Covariance Intersection*, in: D.L. Hall, J. Llinas (Eds.), Handbook of Multisensor Data Fusion, CRC Press, Boca Raton, FL, (Chapter 12)

Julier S. J., Uhlmann J. K., (2004), *Unscented filtering and nonlinear estimation*, Proceedings of the IEEE, Vol. 92, No. 3, pp. 401–422

Kinney, L. (2009). Canada's Marine Security. Canadian Naval Review , 4 (4), 15-19

Lampropoulos, G.A., Anastassopoulos, V., Boulter, J.F., (February 1998) *Constant false alarm rate detection of point targets using distributed sensors*, Optical Engineering, The Journal of SPIE, 37(2)

Leung H., Dubash N., and Xie N. (January 2002) *Detection of small objects in clutter using a GA-PBF neural network.* IEEE Transactions on Aerospace and Electronic systems, 38(1):98–118

Li, X.R., (2003), *Optimal Linear Estimation Fusion—Part VII: Dynamic Systems*, in proc. of the Sixth International Conference of Information Fusion, pp. 455–462

Martin, J. (February 2007) *Arab port security tightens*, http://findarticles.com/p/articles/mi_m2742/is_375/ai_n25000767/?tag=mantle_skin;content (accessed May 15, 2011)

McBryan, C. Krasnor, C. (2011). *Evaluation of Wide-area, Covert, Radar Networks for Improved Surveillance, Intelligence, and Interdiction against Watercraft and Low-flying Aircraft.* Public Security S&T Summer Symposium. Conference Proceedings. Pg. 103

Murty, K.G. (1968), *An algorithm for ranking all the assignments in order of increasing cost*, Operations Research, vol. 16, pp. 682-687

NIEM (February 12, 2007). *Introdcution to the National Information Exchange Model (NIEM)*. NIEM Program Management Office. Document Version 3.0. http://www.niem.gov/files/NIEM_Introduction.pdf

Nohara T. J., (2009), *Affordable, multi-mission, radar surveillance networks for marine and port security*, Journal of Ocean Technology, Vol.4, No. 2, pp.29-38

Nohara, T., (2010). *A Commercial Approach to Successful Persistent Radar Surveillance of Sea, Air and Land Along the Northern Border*. IEEE international conf. on Technologies for Homeland Security 2010

Northern Watch TD Project (2010). Defence R&D Ottawa. http://www.ottawa.drdc-rddc.gc.ca/docs/e/rast_274_nw_tdp-eng.pdf

Ponsford, A.M., D'Souza, I.A., Kirubarajan, T. (2009) *Surveillance of the 200 Nautical Mile EEZ Using HFSWR in Association with a Spaced-based AIS Interceptor*, IEEE Conference on Technologies for Homeland Security

Ponsford, T. (2011) *Effective Maritime Domain Awareness Based on Appropriate Layered Surveillance and a Multilevel Decision Support System*, Canadian Tracking and Fusion Group Workshop 2011.

Poore, A., Rijavec N. (August 1991), *Multitarget Tracking, Multidimensional Assignment Problems, and Lagrange Relaxation*, Proc. of SDI Panels on Tracking, pp. 51-74

Rhodes, B.J., Bomberger, N.A., Seibert, M.C.,Waxman A.M. (October 2005), *Maritime Situation Monitoring and Awareness using Learning Mechanisms*, In Proceedings of IEEE MILCOM 2005 Military Communications Conference

Rohling, H. (July 1983), "Radar CFAR Thresholding in Clutter and Multiple Target Situations", IEEE Transactions on Aerospace and Electronic Systems, AES-19, pp. 608-621

Royal Canadian Mounted Police (2007). 2007 Environmental Scan. Ottawa: Government of Canada

Saha, R.K., Chang, K.C. (1998), *An Efficient Algorithm for Multisensor Track Fusion*, IEEE Trans. Aerospace and Electornic Systems. Vol. 34, No. 1

Seibert M. et al (April 2006), *SeeCoast Port Surveillance*, in Proceedings of SPIE Vol. 6204: Photonics for Harbor and Port Security II, Orlando FL, USA

Sinha, A., Peters, D. (July 2010), *New developments in flexible ID association-based tracking algorithm*, Proc. of International Conference of Information Fusion

Sorensen E. et al (2010), *Passive acoustic sensing for detection of small vessels*, OCEANS 2010

Standing Senate Committee on National Security and Defence. (2003). *Canada's Coastlines: The Longest Under-Defended Borders in the World*. Ottawa

Standing Senate Committee on National Security and Defence. (2007). *SEAPORTS: Canadian Security Guide Book - An Update of Security Problems in Search of Solutions.* Ottawa: Government of Canada

Tate J., Lucchese F., Moore R. (2006), "Introduction to Storage Area Networks", IBM Redbooks publication

TC. (April 22, 2005). *Government of Canada Announces New Marine Security Initiatives*. Transport Canada. Retrieved November 30, 2010. http://www.tc.gc.ca/eng/mediaroom/releases-nat-2005-05-gc001ae-3254.htm

TC. (2010, January 15). *Transport Canada*. Retrieved November 30, 2010, from Evaluation Of Transport Canada's Marine Security Initiatives - 2006: http://www.tc.gc.ca/eng/corporate-services/des-reports-2007-marine-305.htm

.

Thomopoulos, S.C.A., Viswanathan, R., Bougoulias, D.C., (September 1987), *Optimal Decision Fusion in Multiple Sensor Systems*, IEEE Transactions on Aerospace and Electronic Systems, Vol. 31, No. 1, pp. 644-653

Transport Canada. (2003). *Update On Canada's Response To Marine Security*. Vancouver

Transport Canada (2010). *Small Vessel Facility: Security Awareness*. Paper copy

Treasury Board of Canada. (2009, April 7). *Marine Security: Plans, Spending and Results. Horizontal Initiatives.* Retrieved November 30, 2010, from Marine Security: http://www.tbs-sct.gc.ca/hidb-bdih/initiative-eng.aspx?Hi=62

US Department of Homeland Security. (2008). *Small Vessel Security Strategy*. US Government

US Department of Homeland Security. (2005). *The National Strategy for Maritime Security*. US Government

US Drug Enforcement Administration, Federal Bureau of Investigations, Royal Canadian Mounted Police. (2006). *Canada / US Organized Crime Threat Assessment.* US / Canadian Government

Vespe M., Sciotti M., Battistello G. (2008) *Multi-Sensor Autonomous Tracking for Maritime Surveillance*, International Conference on Radar, 2008. – P. 525 – 530

Vervecka, M. (2010) *Data fusion algorithms for sea target tracking using coastal radar model*, 11th International Radar Symposium (IRS)

Wang, H., Kirubarajan, T., Bar-Shalom, Y. (January 1999), *Precision Large Scale Air Traffic Surveillance Using IMM/Assignment Estimators*, IEEE Trans. on Aerospace and Electronic Systems, Vol. 35, No. 1

Yang L., Jin R., Sukthankar R., Jurie F., (2008), *Unifying Discriminative Visual Codebook Generation with Classifier Training for Object Category Recognition*, IEEE Conference on Computer Vision and Pattern Recognition

Wehn H., Yates R., Valin P., Guitouni A., Bosse E., Dlugan A., Zwick H., (July 2007). *A Distributed Information Fusion Testbed for Coastal Surveillance*. In Fusion 2007

Willett P., Coraluppi S., (March 2005), *Application of the MLPDA to Bistatic Sonar,* IEEE Aerospace Conference

This page intentionally left blank.

Annex A Project Team

PORTFOLIO MANAGER

Name : Pierre Meunier
Title : Portfolio Manager, Surveillance, Intelligence & Interdiction
Phone : 613-944-4367
Email : pierre.meunier@drdc-rddc.gc.ca

LEAD FEDERAL DEPARTMENT

Department: Communications Research Centre Canada, Industry Canada
Name: Dr. Andre Brandao
Phone: 613-991-3313
Email: abrandao@crc.ca
Website: http://www.crc.gc.ca

OTHER PROJECT PARTICIPANTS

Organization: A.U.G. Signals Ltd. (Lead industry partner)
Contact Individual: Tatyana Litvak
Phone: 416-923-4425, ext. 235
Email: litvak@augsignals.com
Website: http://www.augsignals.com

Organization: Blue Force Global
Contact Individual: Serge Vidalis
Phone: 778-426-2604
Email: svidalis@blueforceglobal.com
Website: http://www.blueforceglobal.com

Organization: CFN Consultants
Contact Individual: John Leggat
Phone: (613) 232-1576
Email: jleggat@cfncon.com
Website: http://www.cfnconsultants.com/

Organization: AKW Global Enterprises Inc.
Contact Individual: Albert Wong
Phone: (416) 301-9909
Email: albert@akwglobal.com
Website: http://www.lampo.com/AKW/index.html

Annex B Stakeholder Data Analysis Report

1.0 General

The purpose of this document is to provide a final report on the findings relative to the Stakeholder response data as it relates to the asymmetric threat from small vessels.

This report is a reflection of the data provided by nine (9) contributing agencies, with differing mandates. The respondents to the questionnaire, though limited in number, provided adequate qualitative and quantitative data that was corroborated, in discussion with marine industry organizations, businesses and persons.

Though 66% of respondents self-identified as possessing enforcement capabilities, the researcher identified only two (2) of nine (9) stakeholders as enforcement capable as it applies to the enforcement of laws, and based upon the respondents place of employment at the time. The following provides a profile of the respondents that contributed to this research based on their current area of employment:

- Police departments – 2
- Port Authorities – 4
- Strategic Centre – 1
- MSOC – 2 (One respondent from Transport Canada, one respondent from RCMP)

2.0 Anecdotal Information

Prior to completing this report, the researcher attended *Canada PortSecure 2011*, Canada's national maritime security conference. Participants included representatives from numerous Port Authorities, RCMP, DND (Navy), CBSA, US Coast Guard, Port Facility Operators, Private Security firms, and many other marine stakeholders.

Armed with the data acquired during the study, the researcher conducted numerous discussions with conference participants that have direct involvement in marine operations, including large port security officials. As with the data reflected in this report, it is estimated that 90+% of those persons spoken with, supported key findings such as:

- Canada's marine security program is not unified and lacks clear leadership;
- Canada's marine security program is prescriptive but does little to solve or address the issues unique to various stakeholders;
- Enforcement and response capabilities are greatly insufficient to address today's security threats and risks, and those emerging threats;
- Canada's marine security community operates in silos, is ineffective in information sharing, and is exclusive to many organizations that have a stake in the marine industry and security.

3.0 Quantitative Data Report

In an effort to provide consistent interpretation of the quantitative data collected during the active research phase of this study, data reported will reflect values based on information provided by respondents that provided data; therefore, “of respondents that provided data”. It must be noted that a number of respondents provided neither positive nor negative responses to many questions.

In consideration of the data collected, it is suggested by the researcher that the variance of responses is a ‘true’ reflection of the differing roles, responsibilities and mandates of each Respondent / Agency. It is therefore suggested that the greatest weight for gauging the value of this data be placed on those Respondents that possess ‘Operational’ responsibilities to conduct marine security functions within their operational jurisdiction. What is evident from the data is the lack of a unified marine security strategy that encompasses common sensors and technologies for the production of shared data for the purpose of mitigating the small vessel asymmetric threat.

Of those respondents that provided quantitative data, the following is a summary of the data reported that addresses the small vessel threat.

Part I: Small Vessel Threat Quantitative Responses

Small Vessel Threat: Of respondents, it was determined that small vessels presented a 65% threat. Specific threats included (derived from Q2 of Questionnaire):

- 90% threat to be engaged in trafficking of controlled substances;
- 70% threat to be engaged in human trafficking;
- 67% threat to be smuggling tobacco, alcohol or commercial goods;
- 63% threat to be engaged in trafficking firearms;
- 52% threat for transporting wanted and or suspected terrorists;
- 46% threat of transporting hazardous or dangerous materiel; and
- 37% threat of being involved in a theft valued over $5000.

Growing Concerns: Of respondents, it was determined that the small vessel represents a growing concern to border security represented by:

- 52% for the transportation of hazardous or controlled materiel;
- 52% for marine thefts valued over $5000;
- 47% for smuggling tobacco, alcohol or commercial goods;
- 40% for trafficking firearms;
- 33% for trafficking controlled substances;
- 33% for transportation of wanted and or suspected terrorists; and
- 17% for human trafficking.

Vessel Types: Of respondents, it was determined that the following vessels presented a threat to commit criminal activities as noted above:

- 26% of pleasure crafts less than 10m in length presented a threat;
- 15% of commercial vessels greater than 10m in length presented a threat;
- 8% of pleasure crafts greater than 10m in length presented a threat;
- 8% of personal motorized watercraft presented a threat;

- 6% of personal non-motorized watercraft presented a threat;
- 5% of motorized pleasure craft presented a threat;
- 4% of sailing vessels presented a threat; and
- 4% of commercial vessels less than 10m presented a threat.

Vessel Construction: Based on the construction material of vessels that present a threat, the following is reflected (and suggests the degree of ease or difficulty in detection):

- 40% constructed with fiberglass;
- 14% constructed with aluminum;
- 10% constructed by rubber or other inflatable material;
- 10% constructed by steel;
- 5% constructed by wood; and
- 2% constructed by other floatation material (ie. Polystyrene).

Environmental Factors: Based on the use of small vessels that threaten border security, the following environmental information was derived:

- The greatest number of offences or incidents relating to border security equally occur between the months of April to June, and July to September. Lesser incidents occur between the months of October to December. It is suggest that this data represents icing of the Great Lakes and St. Lawrence River during the period of January to March, whilst also reflecting the greater boating activity and population during the periods from April to December.
- Most incidents relating to border security occur during night and or reduced visibility.
- Vessels engaged in activity affecting border security will operate in high traffic areas and use public sites.
- Respondents indicated that (based on average of data collected) their jurisdiction is within navigable waters with a line of site of 7.5 nautical miles.

Vessel Modus Operandi: Based on the modus operandi of small vessels suspected or engaged in criminal or border security events, the following is noted:

- Vessels used in trafficking will conceal their cargo, employ parasitic pods affixed to the hull below the waterline;
- Vessels used in border security offences will use encrypted or secure communication, and GPS navigation systems;
- Persons apprehended in border security offences will be local residents or be familiar with the area, and will have local operational and logistical support;
- The use of stolen or owned vessels was deemed to be neutral, as was the use of navigation lights.

<u>Part II: Current Capabilities - Quantitative Responses</u>

Part II of the questionnaire reflected that there exists and emphasis on countering the small vessel threat, and that efforts are being made to tailor surveillance capabilities to enhance preparedness for the small vessel threat.

In consideration of the mandate possessed by the various Respondents, only two Respondents were law enforcement agencies and therefore possessed the capabilities to interdict or respond to border security incidents. Of the two law enforcement agencies that participated in the study, the Ontario Provincial Police represented the greatest capacity, in terms of operational assets. Other Respondents possessed the capacity to engage support by local or regional law enforcement agencies to respond or interdict border security incidents. In order to reflect the imbalance of current capabilities, OPP assets that represent high numeric values will be highlighted.

Current Capabilities and Assets: Based on the data collected from Respondents to reflect current capabilities, the following data is provided:

- Of Respondents, the following number of Patrol Vessels provide response or enforcement capabilities – 149 Patrol Vessels (144 of 149 are OPP assets);
- Of Respondents, the following number of personnel conduct marine patrols – 364 (350 of 364 are OPP personnel);
- Of Respondents, the following number Instructors or Training personnel were recorded – 2;
- Of Respondents, the following number of dive teams were recorded – 3;
- Of Respondents, the following number of fixed or mobile surface surveillance systems were recorded – 38 (35 of 38 operated by the St. Lawrence Seaway Management Corporation);
- Of Respondents, the following number of airborne sensors were recorded – 3;
- Of Respondents, the following number of Operation Centres and or Monitoring Centres were recorded – 11; and
- Of Respondents, the following number of tactical communication systems were recorded – 6.
- Note: the following capabilities were absent: Interdiction vessels, Special Operations Personnel, sonar systems, remotely operated vehicles, autonomous underwater vehicles, and sidescan or multi-beam sonar systems.

Operational Capabilities: Based on the data collected, the following operational capabilities were recorded:

- The average response time to deploy marine security assets was 2Hr and 13.3 Minutes;
- The average marine patrols operate for 6 Hours;
- The majority of Respondents do not operate on a 24/7 basis;
- 33% of Respondents maintain a 24/7 marine surveillance operations;
- 50% of Respondents possess the ability to augment their response capabilities (as a Force augmentation);
- Of those Respondents that have a Force augmentation, the average number of persons available is 5; and
- Where specialized services personnel are required, the average response time is nearly 3 hours (2Hr 45Minutes).

Training: Based on the data collected reflecting the training of personnel involved in marine security duties or functions, the following data is provided based on average of responses. It must be noted, that training requirements particular for Port Authorities is mandated in the Transport Canada Marine Transportation Security Regulations, and that the data reflects the minimum requirements are being pursued.

- 14% of Respondents possess internal sensor or technology specialists (the Respondent was the Canadian Navy Maritime Warfare Centre, and it is suggested that non-military marine security agencies do not possess this specialized capability);
- Marine security training is conducted at least once on an annual basis, and includes two (2) Table Top exercises per year, and one (1) field exercise that is evaluated.

Sensors and Data Processing: Based on the data collected reflecting the current use of sensors and technologies, and the capacity to process sensor data, the following is provided:

- Of the sensors and technologies currently available to mitigate the small vessel threat, terrestrial platforms are utilized (3 of 9 Respondents indicated use of terrestrial platforms) and reflect their method of maintaining Maritime Domain Awareness and persistent surveillance;
- Of Respondents, none possess system interoperability to enhance domain awareness; however, one Respondent possess local data interoperability for domain awareness and persistent surveillance;
- None of the Respondents employ operational sensor specialists for data collection and analysis;
- One (1) of nine (9) Respondents has the capability to data link to patrol assets; and
- Three (3) of Nine (9) indicate the use of automated surveillance systems, yet do not indicated the ability to detect, classify or track.

<u>Part III: Capability and Limitations Gap - Quantitative Responses</u>

Part III of the Questionnaire aimed to capture the Respondent's opinion on the operational and technological limitations and or gaps relating to marine security and persistent surveillance. Of the Respondents that provided data, the following is provided:

- 100% of Respondents that provided data felt that the current surveillance capabilities to counter the small vessel threat was not sufficient;
- 17% of Respondents that provided data believed that the current information coming from sensors is efficient and meaningful for the purpose of detecting, tracking and classifying suspicious small vessels;
- 78% of Respondents that provided data believe that we are not prepared operationally or technologically to mitigate threats from small vessels;
- 66% of Respondents that provided data believe that changes are needed in both long and short term to enhance Canada's preparedness to prevent the escalation of the small vessel threat;
- 78% of Respondents that provided data believe that jurisdictional issues hamper their ability to address the small vessel threat;
- 78% of Respondents that provided data indicate that they would make changes in the way information is shared with other jurisdictions to enhance preparedness and response to the small vessel threat;
- 33% of Respondents that provided data would make changes to the Command and Control system within their jurisdiction. It is imperative to note that these Respondents were Port Authorities that would benefit from the creation of a

combined Command and Control system for all related agencies to benefit in responses to marine security incidents. As not all Respondents possess the same mandate and operational requirements to maintain marine security functions, consideration should be given to this low positive response as not being a reflection of marine security operations being conducted in the field by frontline stakeholders; and

- 50% of Respondents that provided data indicated that they were aware of emerging technologies that would address and improve current capability gaps in countering the existing and emerging asymmetric threat from small vessels.

The qualitative portion of this report assists in capturing the Respondent's experience based on their jurisdiction, mandate, experience, capabilities, limitations and recommendations for the improvement of marine security strategies in mitigating the small vessel asymmetric threat.

As noted in the introductory comments, only a few Respondents possess the mandate of maintaining and exercising a marine security function within their jurisdiction, and therefore greater consideration should be made in the interpretation of the data collected in the study's questionnaire.

The following is a synopsis of the qualitative data collected.

Part II: Respondent Commentary

In relation to efforts underway to tailor surveillance capabilities so as to enhance preparedness for the small vessel threat, the following comments were provided:

- Small vessels are recognized as a potential and real threat. There are several initiatives being explores (ie Transport Canada is researching a small vessel strategy) The USCG has already developed a small vessel strategy. Law enforcement within the Great Lakes is becoming increasingly aware of the small vessel threat and are looking at resource increases and relocation. (ie. the RCMP MSET unit is developing their patrol responses based upon intelligence from MSOC and IBET units). Remote Sensors (ie. motion/camera) are being updated and deployed based upon known intelligence to maximize potential. RCMP and Canadian Coast Guard are generating awareness and information gathering through "Coastal Watch" and "Watchkeeper" programs. Radar capabilities are being studied and developed to maximize their usefulness to law enforcement. MSOC as a whole continues to explore ways of increasing interoperability.

- Surveillance conducted by CCTV, and security patrols by guards. Usually conducted when commercial ships are in and during silent hours, weekends and holidays. Small vessel traffic monitored on a very limited basis.

- Ongoing resource improvements by US (ie. Border Patrol Sensors/Radar/Camera. DRDC Niagara Radar Project.

In relation to operational procedure for detecting and tracking small boats, the following comments were provided:

- No. There are no abilities to detect and track small boats except by land patrol and finding the boats in the MARSEC facilities illegally or landed on private or port property without permission. Therefore the only operational procedure is detected through land patrol which does not occur daily or by marine patrol which occurs April through Oct only.

- There is a security camera network controlled through Port Operations that monitors the movement of all vessels within the port and at anchorage positions. Small craft activity to some extent can be monitored from the PMV Operations Control Room if unusual movements discovered or requested.

- Yes - Security staff alert port authority who contact vessels via VHF or loudhailer. If ignored, there is no way to intervene.

- No - rely on line of sight and or navigational Radar (on the limited number of patrol vessels equipped with radar).

- Limited radar coverage.

- No - Nil Port Procedures.

- No Specifically.

In relation to how pleasure crafts are differentiated from potential threats, the following comments were provided:

- There is no way to differentiate other than the existence of prior intelligence. Some radar patterns can alert surveillance personnel to anomalies and/or inconsistencies but these alone do not indicate threats. Follow-up queries or patrols are required to make any further determinations.

- NO – it is important to note as described above there is very little data (but a great deal of experience based and or anecdotal information) on the small vessel population – by terminology the “pleasure craft” and by population is most often the vessel of choice for criminal exploitation.

- Investigative technique, information gained through sources and vessel stops.

- Visual identification with binoculars.

- Threats are determined as the craft arrives. Advanced intelligence is received from several sources however it has to be known when and where in order to interdict a craft. The differentiation is dependent on the detail level of intelligence involved.

- Unknown.

- No process to differentiate. Assume pleasure craft calling at local yacht clubs are less threat than small commercial fishermen.

In relation to how Respondents address the difference between surveillance for seaborne, inshore, coastal, and river/Gulf traffic:

- We Don't. Major vulnerability and security gap for Prince Rupert PA, and region.

- Areas are divided up and assigned to various MSOCs.

- My area of jurisdiction is the Detroit River only.

- Large vessels: AIS & CCG INNAV. No way to track small vessels.

- We do not do any.

- The issue is one of Proximity! Radar is most beneficial for open water surveillance (ie. radar is line of sight) while cameras, motion sensors etc. are more effective at choke points (ie. river) were time is a contributing factor.

In relation to how weather affects sensor performance, the following comments were provided:

- Effectiveness reduced at night and in inclement weather.

- Weather is a major factor in both electronic and visual means of detection.

- Don't know as they do not have any detection sensors in use. Expect that fog or snow would affect sensors.

- Yes, depending on the type of sensor.

In relation to how useful AIS and LRIT technologies are when applied to surveillance and detection of suspicious small vessels:

- AIS is ineffective for monitoring small boat threat.

- Not very useful as few small vessels carry AIS or LRIT.

- I have used AIS while on base at the USCG for event. I do not have either available to me at my office or mobile.

- Absolutely Nil. Small vessels will have to be regulated by Government of Canada to carry AIS equipment. Can only monitor commercial vessels. Would require financial support to install radar. Request made to TC but denied.

- We are aware of them – would be useful if we had both mandate and direct access.

- At the current time, small vessels do not require AIS and therefore it is not useful. However, it would be of extreme benefit if in fact it was a requirement (ie. SAR purposes). There is often a time delay with AIS, however, this could be mitigated.

In relation to the usefulness of the latest advancements in sensor technologies/data products being utilized for the purpose of small vessel persistent surveillance (e.g., RADARSAT-2, patrol aircraft, the following comments were provided:

- Nil Radar and Aircraft. Boat patrol (daytime only) and wireless canopy network.

- Only Canadian Port Authority in the maritimes WITHOUT full VTMS coverage. Surface radar would be helpful but would need trained resources to support 24/7/365.

- Sensor technologies are utilized by other units however the sheer geographical size of the Great Lakes makes it cost prohibited at this time to attempt any real form of persistent surveillance on the Great lakes. AIS and radar would be the most practical technologies to develop.

- Out of my area of expertise.

- No equipment in Port Authority.

In relation to how reaction / response is coordinated among jurisdictions and how decisions are made in a rapidly developing event, the following comments were provided:

- Prince Rupert Port Security Operations Centre manned 24/7, coordinates local response. PRPA assumes leadership On Scene Commander role. Collaboration is strong and effective.

- Reaction on the river is coordinated by which side of the international GPS line the incident occurred. The lead agency is determined by first on scene. Often law enforcement from other jurisdictions will assist in support. US authorities usually provide protection and security from their side of the GPS line in the event of a CDN event. If casualties or potential victims exceed the capacities of the CDN resources, the USCG will assist.

- Don't know. Indicates that TC, CCG, DND, CBSA, RCMP would be the ones to know (via MSOC).

- All resources are notified though VHF 16 unless communications need to be made over cellular phones.

- Ontario has a robust and functional Emergency Response Plan and Provincial Counter-Terrorism plan.

- Jurisdictions tend to be barriers during routine operations however; on a contingent/emergency basis communication is direct and immediate.

- Incident Command, tactical response, public order etc are standardized (and functionally very interoperable between services) across the Province in a large part to the Police Services Act Adequacy Standards/Guidelines. Investigative units are compelled to interoperability.

In relation to what additional persistent surveillance systems are in place in Respondent's jurisdiction, the following comments were provided:

- No Radar. Coast Guard MCTS control. AIS for 500 tonnes and greater. Motorolla canopy network (cameras). PRPA, RCMP (marine division), Boat patrol daytime only, very limited 24/7 capability.

- Michigan State Police - radar system; USCG AIS; MCTS - CCG Sarnia monitoring of commercial vessel traffic.

- Unknown. Possibly RadarSat or LRIT.

In relation to other ways of adapting existing processes / technologies to provide for better overall area security for small vessel threat in a cost effective manner, the following comments were provided:

- Yes: Radar, AIS integration along with improved on water presence and capability. Integrated C3 (boat - radar- AIS-camera to Port Security Operations Centre, then collaborate and info sharing to RCMD - PRPA- Coast Guard - CBSA.

- There are no existing technologies within the Windsor Port Authority.

- Add port to CCG VTMS including local radar surveillance and VHF.RCMP or CCG locate trained operators and provide response vessels nearby ie. Bathurst, Dalhousie…

- AIS for all vessels. Integrated radar system. Note: Entered by Vidalis: The Great Lakes MSOC and IBET have been working on a project 'Cipitor' intended to collate radar data within their operating area. Status is unkown.

<u>Part III: Respondent Commentary on Capability Limitation and Gaps</u>

The following commentary was provided by Respondents relating the operational and technological limitations and gaps to marine security and persistent surveillance.

In relation to current surveillance capabilities that are insufficient to counter the small vessel threat, Respondents that provided a negative response provided the following comments:

- This requires a continued whole of government focus. The MSOCs are a good start, but specific systems need to be deployed to improve detection capabilities. These systems do not have to be allocated to the navy, but should be integrated into the MSOCs.

- AIS for vessel tracking. CCTV for all docks and vacant properties along the Detroit River. Consistent video surveillance with operator watching will enable quick response to incidents on the river. Sidescan sonar for the police boats as well as night vision to allow law enforcement to continue operating in surveillance after dark. New boats tht provide landing capability as well as speed equal to the law breakers. Clear delineation of the role of the municipal police versus RCMP in relation to patrol and response on the international boundary waters (Detroit River). CCTV monitoring system of the waterway, responsibility and resources for monitoring need to be defined before technology is put in place. Windsor Port Authority is a 3 personnel including CEO, CFO and Harbour Master. Interoperability communication Port Authority and USCG in addition to Windsor Police, OPP and RCMP.

- Fulltime 24/7/365 guard patrols of waterfront and harbour areas combined with waterside patrol vessel enforcement capability with trained operational staff. Consolidation to existing AIS, CCTV systems possibly add on the waterside. Security cameras with nightvision detection capabilities and ??? staff on duty to monitor. Certainly adding radar coverage would be a key item as well. A lot of this would be redundent if CCG provided live MCTS coverage plus RCMP/CCG/TC provided waterside enforcement.

- Infrared cameras along border being monitored 27/7. The only problem is by the time the target is acquired it has already travelled between countries.

- Some effort has been ongoing to acquire/improve surveillance capacity – to what point when there is little (in many locales no) capacity to respond effectively to whatever that technology reveals.

- AIS, Radar.

In relation to data products / signal processing, Respondents provided comments reflecting their efficiency and meaningfulness for detecting, classifying and tracking of suspicious small vessels, the following comments were provided:

- Lack of investment in state of the art technology. Cash for security still a challenge for private companies / Ports. The ROI (return on investment) issues. Government $.50 dollars are key.

- What data we do receive is relatively efficiently utilized through the MSOC construct.

- AIS presently cannot pick up small craft and have no other means like radar…etc. by which to do so.

In relation to operational and technological preparedness to mitigate threats stemming from small vessels, Respondents provided the following comments:

- Vulnerable, nil on water assets, No Real inter-department collaboration.

- There are gaps in our detection and classification capabilities regarding small vessels. However, the threat is not so great that huge expenses would be required to mitigate the threat.

- Information sharing is limited from agency to agency. Not good sharing as a whole. The Port Authority does not have ANY SECURE method of receiving intelligence information. Operationally, Port is limited by seasons to respond to any threats caused by a small vessel. River rarely freezes over and a small craft could launch against critical infrastructure or continue other criminal activity after law enforcement boats leave the river after Oct 30. We need ice capable response craft. Technologically we are not prepared as we have no present capability to profile a vessel due to arrive to the Port or ability to track present locations. Technology sharing between agencies in my opinion is nonexistent. Unknown what capabilities OPP or RCMP may have. Municipal police no monitoring capabilities.

- Complete lack of resources and / or funding by government by which to do so.

- There are very limited marine resources and most police services "emergency responders" have extremely limited ability to function in the marine environment.

In relation as to needed changes in the short and long term to enhance Canada's preparedness for small vessel threats escalating into high consequence public safety / security events, the following comments were provided:

- We are slowly losing control of the marine approaches domain and likely mission creep into the harbours. Criminal success in drug smuggling likely to grow the criminal business to include firearms and people. The fight over territory and criminal control would be bad for the port's commercial business.

- The resources currently assigned are appropriate for the threat. However, special events such as the Olympics and G8/G20 require extra attention and Canada has done so.

- Lack of resources in the area. Port Authority has no monitoring or communication capabilities whatsoever. As a result left to rely on the good relationship with other agencies. When an imminent threat or incident occurs the likelihood of sharing resources will become nil. Need to clarify and educate who is the first response agency to small vessel threats and events. Who is by legislation responsible to provide the response and service and how is that mandate carried out on the river? Who is funded to protect the international boundary? CBSA does not have boats, RCMP are more LE project based and Windsor Police may not have international mandate. Develop marine restricted zones properly and strongly identified and provide enforcement and compliance resources. A penalty aspect must be established or it is irrelevant to have a restricted zone. Likewise on land surrounding port facilities. Currently there are no penalties except trespass which is not well considered within the court system. No deterrent for persons with criminal intent. In order to provide a penalty system, Harbour Masters should be sworn peace officers with ability to write tickets, place fines, or orders to public. Training of the position would be necessary and a system to record offence notices.

- In every discussion attended with TC on the ISPS Code / MTSR issues waterside security capability stands our as the biggest single issue. The shore side has been looked after but not the sea side.

- Small vessels blend with general population and can be used to carry out any number of criminal activities.

- When the big event occurs who is going to respond?

- If an incident was to happen or about to happen all eyes will be turned to MSOC to provide immediate intelligence as to where the threat is and what it is doing.

In relation to whether or not jurisdictional issues hamper or promote the ability to address the small vessel threat, the following comments were provided:

- Today this is an RCMP show, and they do not have the assets to address, so mostly activity is left unchecked and unmonitored.

- Information sharing among departments is still an issue, although the MSOCs are very useful to facilitate this.

- The Canadian law enforcement agencies appear to not be clear who would have jurisdiction in the event of an international boundary event on the river. As the river is patrolled by both municipal and federal police it appears it is not clear who takes jurisdiction or even responds to the event. If a threat comes through intel the information is often not shared with the Port Authority. As a result, we are not on the lookout for persons, activities or vessels. BOLOs are not provided to this office which puts the port and myself at risk during my patrols. The need to know is measured by the agency with the information and not always with consideration of the Port Authority and our knowledge of the Port lands and the persons operating on them. USCG is very open to sharing information with the Port Authority but not so between Canadian agencies to the Port.

- There are no clear rules to indicate which government department or agency has clear priority and superiority over whether in terms of dealing with small vessel threat. Where does Port Authority stand in all of this? Very confusing!!

- Both lack of resources as well as lack of legislated authorities for the very few existing "marine police" to effectively contribute.

- Too many departments with their own agendas/ budgets/priorities and mandates.

In relation to making changes to the way information is shared with other jurisdictions to enhance preparedness and response to the small vessel threat, the following comments were provided:

- Take the Australia approach and make it law that Government agencies share intelligence and information. Establish MSOC Nodes in all Ports (and) co-locate: RCMP, CBSA, Coast Guard, DND, and Port to: share infrastructure costs, share expertise, share info, share the risk, share the success.

- Remove legislative barriers among departments to effective information sharing of potential threat information.

- A secure method is needed by the Port Authority to pass information to agencies such as MSOC. If the rule is MSOC gets the information from the Ports then the Ports should be informed as to whom was the information forwarded to by MSOC. Area Maritime Security Meeting established by the USCG is the most useful method of passing information agency to agency. The rest relies on relationships/ trust person to person.

- RCMP, DND, CCG, TC, CBSA are all part of MSOC yet ports and industry players don't seem to have ability to sit in and / or participate in sharing of information other than reporting and ???. Need to know situation exists ??? and should be changed.

- The majority of forces have small marine divisions. If all divisions worked together under one umbrella. Focused and effective resources could be focused on current situations.

- Police of jurisdiction in Ontario are very sophisticated in how we share both operational information and tactical/strategic intelligence.

- Mandate provincial and federal agencies to coordinate information into a central location such as MSOC.

In relation to making changes to the Command and Control system in place to best link surveillance to operations in the Respondent's jurisdiction, the following comments were provided:

- Once jurisdiction is established, communication by command and control to the Port Authority would be appreciated. At this time there is no communication as to surveillance operations in my jurisdiction or linkage to other activities noted in the Port. As a result, through not knowing the surveillance my patrol could roll into the area and destroy significant amounts of work done during and in preparation of the surveillance. Also I may be put at risk not knowing activities under surveillance as well as place other officers at risk as they now have to protect me during the event.

- Take the Australia approach and make it law that Government agencies share intelligence and information. Establish MSOC Nodes in all Ports (and) co-locate: RCMP, CBSA, Coast Guard, DND, and Port to: share infrastructure costs, share expertise, share info, share the risk, share the success.

- Not at this point only if RCMP, CCG, TC become ??? Involved in ??? With small vessels ???

- Police in Ontario have a very robust and effective command and control structure specific to critical incidents. Application to a surveillance operation would be fairly simple.

- MSOC is not operational. MSOC is a collocation of Federal agencies. Jurisdictions are typically a provincial or municipal ownership.

In relation to emerging technologies that have potential to address the capability gaps and improve Canada’s ability to counter existing/ emerging asymmetric threats, or any innovative efforts underway internationally, the following comments were provided:

- A renewed emphasis on undersea acoustic surveillance within the US Navy that Canada is very interested in.

- Not really since US and Canada seem to be leaders on terrorism threat??? And drive ISPS Code at IMO in the beginning after 9/11. Possibly GPS tracking system similar to what is used in trucking industry.

- Access to various sources of info (camera, RADAR, alarms) etc owned by private industry (often paid for by Transport Canada’s Contribution fund)

List of abbreviations

AES -Advanced Encryption Standard
AIS – Automatic Identification System
ASU - Automated Scene Understanding
AUV - Autonomous Underwater Vehicles
BC - British Columbia
CA - Cell Averaging
CBP – US Customs and Border Patrol
CBSA - Canada Border Services Agency
CCG - Canadian Coast Guard
CCTV - Closed-Circuit Television
CFAR - Constant False Alarm Rate
COP - Common Operating Picture
CoP - Community of Practice
CSIS - Canadian Security Intelligence Service
C3 - Command, Control, and Communications
DEA - Drug Enforcement Administration
DEMUS - Deployable Multistatic Sonar
DES - Data Encryption Standard
DHS - Department of Homeland Security
DND - Department of National Defence
DRDC – Defence R&D Canada
EKF- Extended Kalman Filter
EO – Electro Optical
FLIR - Forward Looking Infrared
FNC – First Nations Communities
GigE - Gigabit Ethernet
GIS – Geographic Information System
GL – Great Lakes
GLSLS - Great Lakes and St. Lawrence Seaway
GPS – Global Positioning System
GSM – Global System for Mobile
GUI - Graphical User Interface
HF – High Frequency
HFSWR- High Frequency Surface Wave Radar
HUMINT - Human Intelligence
IBET - Integrated Border Enforcement Teams
IGSI - Inter-group Shared Information
IMIC3 - Maritime Interdepartmental Integrated Command, Control and Communications
IMM - Interacting Multiple Model
IMO - International Maritime Organization
IPT - Integrated Project Team
IR - Infra-Red
ISPS - International Ship and Port Facility Security Code
ITU - International Telecommunications Union
JORN -Jindalee Operational Radar Network
JPDA - Joint Probabilistic Data Association
LAN – Local Area Network
LRIT –Long-Range Identification and Tracking
LWIR - Long Wave Infrared

MC-IPT - Maritime Capstone Integrated Project Team
MHT-Multiple Hypothesis Tracker
MSOC - Marine Security Operation Centres
MSTT - Marine Small Target Tracker
MTSR - Marine Transportation Security Regulations
NAS-Network Attached Storage
NY- New York
OGD - Other Government Departments
OPP - Ontario Provincial Police
OS - Order Statistic
OTH - Over the Horizon
PDA - Probabilistic Data Association
PPA - Projects and Activities
PSTP -Public Security Technical Program
RCMP-Royal Canadian Mounted Police
RF – radio Frequency
RFMO-Regional Fisheries Management Organizations
SAN-Storage Area Network
SAR – Synthetic Aperture radar
SII-Surveillance Intelligence and Interdiction
SNR - Signal-to-Noise
SOLAS - Safety of Life at Sea Convention
SQ - Sûreté du Québec
TBD - Track-Before-Detect
TC - Transport Canada
TML –Technology Maturity Level
TRL – Technology Readiness Level
UAV – Unmanned Aerial Vehicle
UKF - Unscented Kalman Filter
US - United States
USCG - US Coast Guard
VHF – Very High Frequency
VINCENT - Vessel Intelligence Centre
VMS – Vessel Monitoring System
VTMS – Vessel Traffic Management System
3DES - Triple Data Encryption Standard

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR Defence R&D Canada	2. SECURITY CLASSIFICATION UNCLASSIFIED	
3. TITLE Study on Persistent Monitoring of Maritime, Great Lakes and St. Lawrence Seaway Border Regions		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Leggat, J; Litvak, T.; Parker, I.;Sinha ,A.; Vidalis, S.; Wong, A.		
5. DATE OF PUBLICATION De cember 2011	6a. NO. OF PAGES 90	6b. NO. OF REFS 90
7. DESCRIPTIVE NOTES Contract Report		
9. SPONSORING ACTIVITY DRDC R&D Canada –CSS 222 Nepaen St 11th fl Ottawa, ON K1A 0K2		
9a. PROJECT OR GRANT NO. PSTP 02-341BTS	9b. CONTRACT NO. (	
10a. ORIGINATOR'S DOCUMENT NUMBER PSTP 02-341BTS	10b. OTHER DOCUMENT NO(s). DRDC CSS CR 2011-28	
11. DOCUMENT AVAILABILITY Unclassified		
12. DOCUMENT ANNOUNCEMENT Unlimited		
13. ABSTRACT		

This study employed a systematic and interdisciplinary analysis to better understand the current and arising capability gaps relating to the security of the maritime, Great Lakes and St. Lawrence Seaway (GLSLS) border regions. It examined strategies and technological approaches for persistent small vessel surveillance, and evaluated potential solutions that would address the identified gaps. The approach included a review of the technical literature, a qualitative survey of stakeholders, an analysis of requirements and resulting gaps, and an assessment of potential solutions enabled by new technological approaches and operational procedures.

This evaluation of a variety of potential systems, technologies and techniques resulted in a roadmap designed for a Surveillance, Intelligence, and Interdiction solution which allows persistent surveillance and the accurate, robust and timely identification of small vessels – compliant and non-compliant, while allowing the efficient operation of our maritime border areas.

Cette étude se fonde sur une analyse systématique et interdisciplinaire visant à mieux comprendre les écarts de capacité actuels et en voie de manifester dans le domaine de la sécurité des régions frontalières des Grands Lacs et la voie maritime du Saint-Laurent(GLVMSL). Dans le cadre de l'étude, on a examiné les stratégies et les approches technologiques de surveillance permanente au moyen de petits navires, en plus d'évaluer les solutions qui permettraient de combler les écarts recensés. L'approche consistait à examiner la documentation technique, à faire une enquête qualitative auprès des intervenants, une analyse des besoins et des écarts qui en découlent, ainsi qu'une évaluation des solutions que pourraient apporter de nouvelles approches technologiques et modalités opérationnelles.

Cette évaluation d'un éventail de systèmes, technologies et techniques possibles a donné lieu à la création d'une feuille de route menant à l'adoption d'une solution de surveillance, de renseignement et d'interdiction permettant l'exercice d'une surveillance permanente et l'identification rapide, exacte et fiable des petits navires, conformes ou non, ainsi que la gestion efficace de nos frontières maritimes.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS
Border Security; Maritime Security; Monitoring