The Implications of Self-Reporting Systems for Maritime Domain Awareness

Hammond, T.; McIntyre, M.; Chapman, D.; Lapinski, L.; DRDC Atlantic SL 2006-123; Defence R&D Canada – Atlantic; June 2006.

Hammond, T.; McIntyre, M.; Chapman, D.; Lapinski, L.; Proceedings of the 11th ICCRTS, Command and Control in the Networked Era; Cambridge 2006.

1. Introduction

The term *domain awareness* has its origin in the safety and security community and it appears to be analogous to the term *battlespace awareness* in the military command and control community.[1] Battlespace awareness has always been key to military decision making. Commanders must maintain a current picture of the geographic disposition and capabilities of the forces under their command as well as allied military forces. They must understand the physical environment in which they operate and they need to understand how to employ their forces to best advantage in those environments. Moreover, commanders must employ all available sensors, intelligence and information sources to maintain an accurate and timely picture of all adversarial forces as well as neutral and non-combatant actors. (A closely related term in military parlance is *situational awareness*.) Similarly, those charged with national security rely on domain awareness as a basis for decision making associated with national security missions. We provide a more complete definition of domain awareness in the maritime domain below.

An important distinction between national security scenarios and traditional blue-on-red military scenarios is the relative importance of "white" situational awareness. White situational awareness is an awareness of the non-military components of the battlespace or mission space. In traditional scenarios with a well-defined adversary, there is an assumption that the adversary (red force) will employ all necessary measures to ensure that the blue force cannot gain and maintain red-force situational awareness. Such measures include management of their physical signatures to reduce detectability, protection of the communication channels used (including the information that flows on those channels), and maintaining secrecy regarding plans and intentions. In such scenarios, awareness of civilian infrastructure and non-combatant personnel is a necessary subcomponent of blue-red situational awareness. However, in public security missions, where the adversaries are terrorists or other criminals, awareness of non-military actors and infrastructure is critically important because adversaries will often choose to masquerade as innocent civilians and exploit the vulnerabilities of civilian infrastructures for their purposes.

Another characteristic of traditional military scenarios is that both blue and red forces rely heavily on their own sensor systems for surveillance, reconnaissance and targeting.

[1] See "DOD Dictionary of Military Terms" at http://www.dtic.mil/doctrine/jel/doddict/

Adversaries are, almost by definition, non-cooperative in such scenarios. Using a mix of passive and active sensor systems at acoustic, radio-frequency, and electro-optic wavelengths, military commanders attempt to detect, track and identify red forces. Based on an understanding of the attributes of the various sensors, experienced commanders develop a level of trust in the information derived from these physical sensor systems. In security scenarios, however, a great majority of the traffic under surveillance is cooperative (or at least not uncooperative) and makes little attempt to conceal movement or intentions. In fact, many mobile entities will openly publicize their identities, intentions, and precise positional information, which raises the question as to whether additional information is needed from physical sensor systems.

Below, we discuss the important role that new self-reporting systems (SRSs) are playing in maritime domain awareness (MDA). We define maritime domain awareness and self-reporting systems and suggest what characteristics of SRSs are important to MDA. We contrast self-reported information to traditional sensor-based domain awareness information. In particular, we discuss self-reporting systems for ships, such as the Automatic Identification System (AIS), Voluntary Observing Ships (VOS), Vessel Monitoring Systems (VMS) and Long Range Identification and Tracking (LRIT) systems. We review the contribution that these sources have made to the Canadian Recognized Maritime Picture (RMP) and speculate on what characteristics of AIS have made it emerge as the dominant contributor. We discuss the social and public policy dimensions of the SRSs, especially the challenge of encouraging responsible participation. Finally, we speculate about the impact such systems will have on maritime command decisions.

2. Maritime Domain Awareness and Self-Reporting Systems

2.1 Maritime Domain Awareness

Maritime Domain Awareness is a term coined by the US Coast Guard to refer to "…the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States".[2] They go on to define the maritime domain as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances." This broad definition includes such activities as long-range vessel tracking and identification, maintaining awareness of cargo and crew aboard vessels, maintaining current meteorological predictions for safety at sea and maintaining detailed awareness of critical marine infrastructures in maritime hubs, such as sea ports or fresh water seaways like the St. Lawrence. MDA encompasses everything that a decision-maker may need to be aware of to make effective decisions in the maritime domain.

2.2 Self-Reporting Systems

[2] "National Plan To Achieve Maritime Domain Awareness for the National Strategy for Maritime Security," (2005), retrieved June 2006, from http://www.uscg.mil/mda/MDA_Plan.pdf

Self-reporting systems offer the potential to significantly improve maritime domain awareness. Modern satellite navigation systems have revolutionized our ability to locate people and objects in space and time in a common global reference system. Furthermore, global communication systems have revolutionized our ability to share this position and time information among widely dispersed parties. Roughly, SRSs are communication systems that enable sharing of such position and time information. In more detail (but not formally), we define self-reports as messages, in some pre-defined format, that include at least identity, position, and velocity information about some entity. Other status or intention information could be — and often is — included in self-reports.

A self-reporting system is characterized by the form of its reports in conjunction with a defined communication system used for passing these messages between participating parties. Typically, defining a communication system involves defining a communication channel together with a protocol for passing the messages. A simple example is one whereby operators on a ship at sea complete a paper form and FAX the form to a central site that requires the information at regular intervals. We use this highly manual example to motivate the following section where we discuss the characteristics of more automated SRSs that are relevant to MDA.

2.3 Self-Reporting System Characteristics

There are many characteristics of SRSs that are of interest to those maintaining MDA and are, therefore, worth investigating and understanding. To make the discussion here more concrete, we assume that we are interested in maintaining MDA over a broad maritime area of interest at some centralized location referred to as a Security Operations Centre (SOC). There are examples of security operations centres that focus on maritime security. They tend to be located in strategic locations and are given wide areas of responsibility that cover the open-ocean regions, the coastal and inland waterways, and the ports of strategic interest to the nation and its allies. At these SOCs, decision-makers from various government departments and agencies are responsible for different aspects of MDA within their respective mandates. An important component of MDA, at these SOCs, is maintaining an accurate picture of the identity, position, track, and intentions of all vessels in their Area of Responsibility (AOR). It is this component of MDA that will be the focus of the remainder of the paper.

One characteristic of SRSs that is of interest to a SOC is participation. The question of interest is: How many vessels in the AOR are employing an SRS of some kind? Two other important SRS characteristics are spatial and temporal coverage. The questions of interest are: For those vessels self-reporting within the AOR, (i) are they reporting regardless of where in the area they are operating? and (ii) how often are they reporting? For example, in protected marine areas or high-traffic areas, such as ports, there may be a requirement to report much more frequently than in other areas within the AOR. Another characteristic of SRSs that will affect the utility of self-report information is time delay. The question of interest is: what is the delay between the time the report is authored and the arrival of the information at the SOC? There are many factors that can increase this delay, including the report authoring process, report review procedures, and the report communication path. Also, the body that manages or sets-up the SRS may have a ruling on how often the self-reports are allowed to stream into the SOC or may have the ability to start and stop the flow of information at their discretion. In the manual case above, the time taken to manually complete a form, to have it reviewed for correctness and completeness, and to FAX it to the SOC via satellite all add significant delay at the SOC end. These spatial and temporal characteristics can be incorporated into the general characteristic of availability. How available is the self-report information to the SOC?

All of the SRS characteristics mentioned above are quite technical; however, there are less technical SRS characteristics that are equally significant. These characteristics are the access rights that the SOC has to the SRS information and the trust one can place in the self-report information. Investigating access rights refers to establishing what "need to know" information may be shared between the owner of the SRS reports or the sender of the self-reports and the SOC. The access rights can be governed by policy and legislation, depending on the nature of the information. Trust in the information itself is probably the most subjective characteristic. It is related to two questions: (i) Do decision-makers at the SOC believe SRS information to be correct? (ii) Do those providing SRS information trust the authorities to use it responsibly? (Eroded trust could lead to resentment and ultimately affect the information quality.) Availability, accessibility and trust are all discussed later on. Availability and accessibility are brought up in conjunction with the various SRSs described in Section 3 and the two trust questions are examined further in Sections 5 and 4, respectively.

3. Examples of Self-Reporting Systems

Examples of ship-related SRSs are described in this section.

3.1 Vessel Monitoring Systems (VMS)

Vessel monitoring systems, whereby vessels self-report to a central location via satellite links, have been in use world-wide by commercial companies for some time now.[3] They have moved away from the manual reporting we discussed earlier towards highly automated systems that are capable of reporting continuously on a fixed schedule or responding to requests for reports on demand from the central site. For commercial companies in the business of moving goods by sea, it is in their best interest to have good knowledge of the location of their ships at any time on all shipping routes that they frequent. So, the carriage of a commercial VMS is typically limited to ships under one owner. The coverage of the SRS will be determined by the satellite (or fixed) system chosen, which would need to have communication coverage over all areas of business interest. The update rate for a commercial SRS will be determined by the owner's desire for accurate information balanced by the increased communication costs of more frequent updates. Access to this information would clearly be under the control of the company that owns the ships, pays the communication costs for the self-reports, and stores and

[3] For example, Pole Star Space Applications Limited, http://www.purplefinder.com

manages the self-report information in some centralized data base. While it is very unlikely that a commercial company would offer this information to competitors, it would be in the company's interest to share at least some self-report information with an SOC under the proviso that it would not be shared further. So, both availability of the self-reports and access rights to the self-report information would be a subject of negotiation between the SOC and the SRS owner, and a level of mutual trust would have to be established.

Another interesting example of a VMS is that used for tracking fishing. Government agencies around the world are increasingly using VMSs to monitor commercial fishing fleets. These systems use satellite communications to report the positions of active fishing boats on a regular basis (typically hourly). The information provided is generally limited to identity and position. For example, since January 1, 2001, all vessels taking groundfish or shrimp in the North Atlantic Fisheries Organization (NAFO) regulatory area have had to be equipped with a VMS. This carriage is mandated by NAFO but the costs to the fishing vessel—$1500 to $5000 for the initial system and about $50 per month in satellite phone calls—are paid by the fisher. So, while the coverage and temporal resolution issues of these VMS systems would be similar to those for commercial ships, the availability and access rights to the fishing boat self-reports have the potential to be much more complex.

The intent of fisheries VMSs is to improve fisheries management. They can, for example, provide some reassurance that fishers— especially foreign ones—are not fishing in restricted areas, they can provide insight into the distribution of fishing effort, and they can provide data on the connection between fishing effort and commercial catch. Depending on the system chosen, a VMS may provide the fishing vessel with additional two-way communications capabilities. There may also be a search & rescue benefit. While fishers may value such improvements, confrontations between fishers and their government regulators have been known to happen. Even when relations are amicable, the financial benefits of these intangible improvements are very hard to measure. It is probable, therefore, that VMS costs would be perceived by many fishers to provide little return. Few would participate in the system were they not compelled to do so.

Fishers are often very protective of their favourite fishing spots, lest they be discovered by others. Although VMS does not typically indicate when the fishing gear is in the water, access to the positions of successful vessels would nonetheless be very useful to less experienced crews, as illustrated in Figure 1. Therefore, fishers may be very concerned about who has access to their VMS position reports. For this reason, there are typically restrictions on data distribution. Due to concerns about data distribution and to distributed management of VMS systems in Canada, VMS has not had the impact on the Canadian RMP that it has had in some other countries.

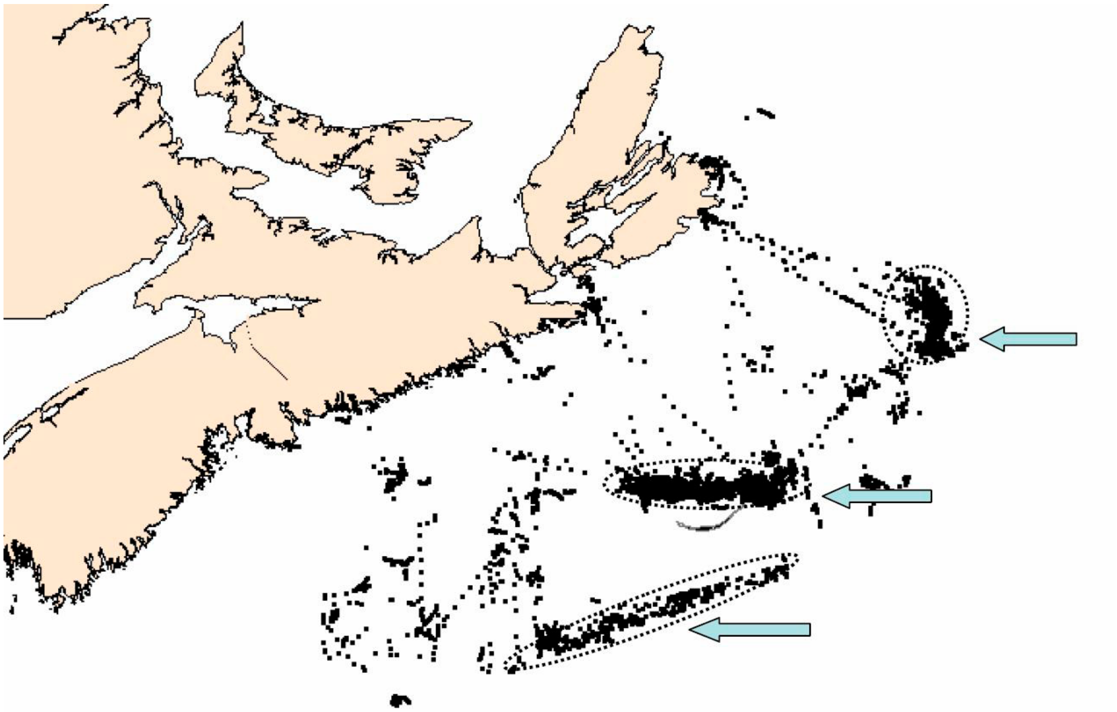
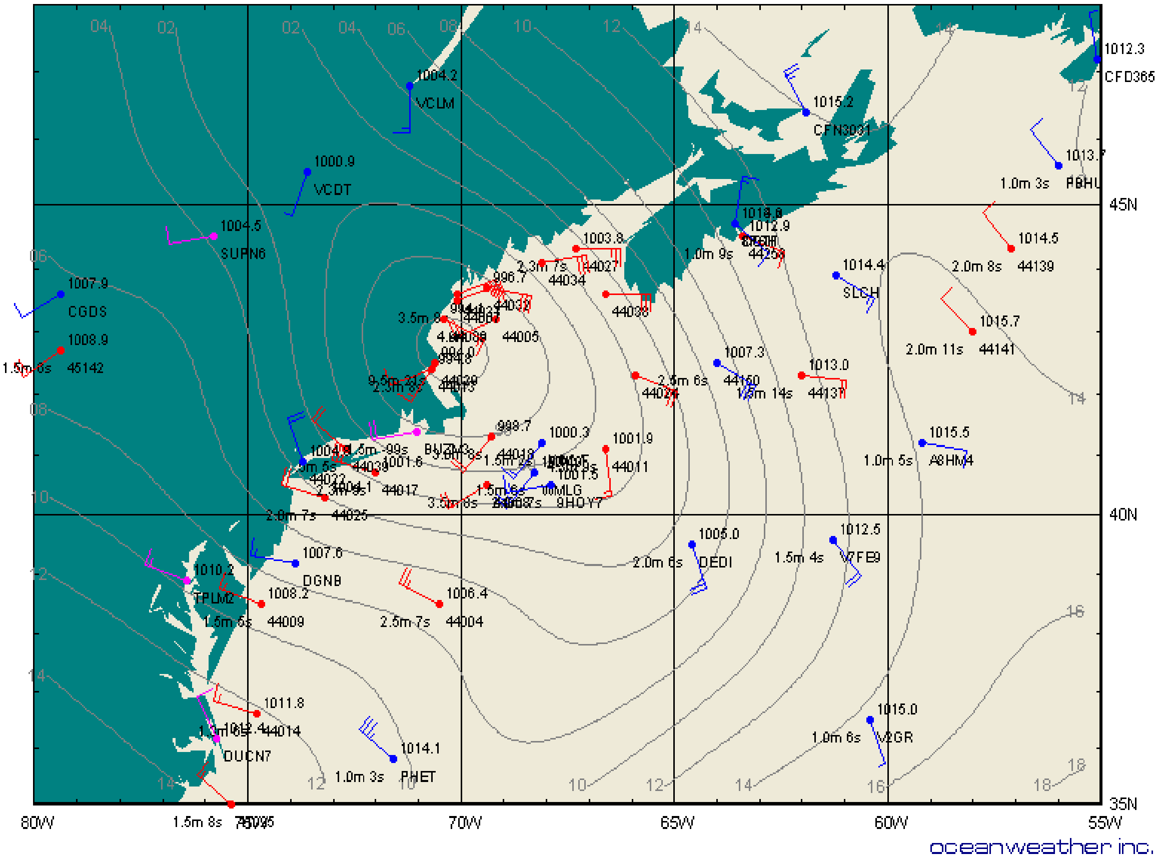


Figure 1. Vessel Monitoring System (VMS) data from 35 vessels of the Snow Crab fishery off the coast of Nova Scotia, showing areas of concentrated effort with arrows[4]. Black dots indicate position reports.

3.2 Voluntary Observing Ships

The World Meteorological Organization (WMO) collects weather reports from about 4000 Voluntary Observing Ships (VOS) when these vessels are at sea. These ships report the weather in their vicinity four times daily. They send their weather reports to one of forty-nine National Meteorological Services (NMSs), and then the NMS forwards them to the WMO for compilation. Ships participate in order to improve the WMO's knowledge of weather conditions at sea; knowledge which the WMO claims has made considerable contributions to operational meteorology, to marine meteorological services, and to global climate studies. Reports are also used in the preparation of forecasts and warnings, including those for the Global Maritime Distress and Safety System (GMDSS).

[4] Fisheries and Oceans Canada, "Vessel Monitoring System (VMS)," (2005), retrieved June 2006, from http://www.glf.dfo-mpo.gc.ca/fm-gp/cp-cp/vms-ssn/vms_presentation-e.pdf



Marine Observations Valid for April 04, 2006 18 GMT
Model Pressures Valid for April 04, 2006 18 GMT (6 Hour Forecast)

Figure 2. A graphical representation of ship locations and local weather for April 04, 2006, collected from the WMO's VOS program[5]. Weather buoys are red and ships are blue. The wind barbs indicate the wind direction and speed (long = 10 knots, short = 5 knots).

Ships pay no communications costs for reporting the weather in this scheme and usually employ INMARSAT C [6] satellite communications. Some meteorological services provide free software to automate much of the process. In some cases, port meteorological officers provide ships with the equipment necessary to take observations, and install it free of charge. They also ensure that observations are taken using consistent methodology. With regular update rates and a global coverage, VOS is potentially a valuable source of information for SOCs as long as there is an agreement with the participating vessels that some of the information can be shared for MDA and security purposes. Having said that, the truth is that VOS information is actually freely available on the internet, as can be seen in Figure 2; therefore, merchant ship positions can be obtained without the consent of the vessels to support a SOC.

Since the free VOS system is getting easier to use all the time and contributing to mariners' ability to avoid bad weather, one might expect that ships would join in large numbers. Unfortunately, the number of participating vessels has declined steadily since the peak of 7700 participants in 1984. We can only speculate on the reasons: (i) the

[5] From Ocean Weather Inc., http://www.oceanweather.com/data/

[6] See Inmarsat C, http://maritime.inmarsat.com/services/c_minic.aspx

increasing availability of satellite weather information, which may have led some mariners to the erroneous belief that weather reports are no longer needed; (ii) mariners have learned that security agencies are exploiting the data; (iii) mariners are content to benefit from the weather reports of others but do not see a need to participate.

3.3 Automated Mutual-Assistance Vessel Rescue (AMVER)

All mariners are obliged to respond to distress calls from their fellows, but to do so costs time and money. AMVER, which has been run by the United States Coast Guard (USCG) in various guises since 1958, promises to reduce the time, fuel, and payroll costs spent responding to distress calls by diverting only the closest and most suitable vessels to an emergency. In exchange, vessels provide regular reports of their position. Vessels participating in AMVER submit a sailing plan to the USCG that must contain sufficient information to predict the vessel's position to within 25 nautical miles at any time during the voyage. If they deviate from the submitted plan, they are expected to send a deviation report as soon as possible. Within 24 hours of leaving port, and at least every 48 hours thereafter, vessels are expected to send in a position report. The communication is free for the vessel. Software named AMVER/SEAS [7] is available to automate the process and can also file weather reports.

Ships from 148 nations participated in AMVER in 2005: on an average day, 3004 ships reported their position (Figure 3). Participation levels appear to have held steady in recent years. AMVER also shares data with the Japanese Ship Reporting System (JASREP), the Australian Ship Reporting System (AUSREP), the Chilean Ship Reporting System (CHILREP), and the U.S. Maritime Administration Reporting System, so reports need only be made to any one system with an option to approve information sharing.

Mariners are unlikely to resent AMVER, as it is intended to facilitate search & rescue and to save mariners money. Some US-flagged vessels also use AMVER to satisfy legal reporting requirements, and it doesn't cost them anything. Mariners are assured that the information they provide is "commercial proprietary" and that it is released only to national search & rescue authorities in an emergency. These assurances help create strong expectations of privacy posing an interesting dilemma: AMVER reports would be very useful for MDA purposes if not for these promises; however, it might be the promises that encourage participation.

[7] See SEAS, http://seas.amverseas.noaa.gov/seas/

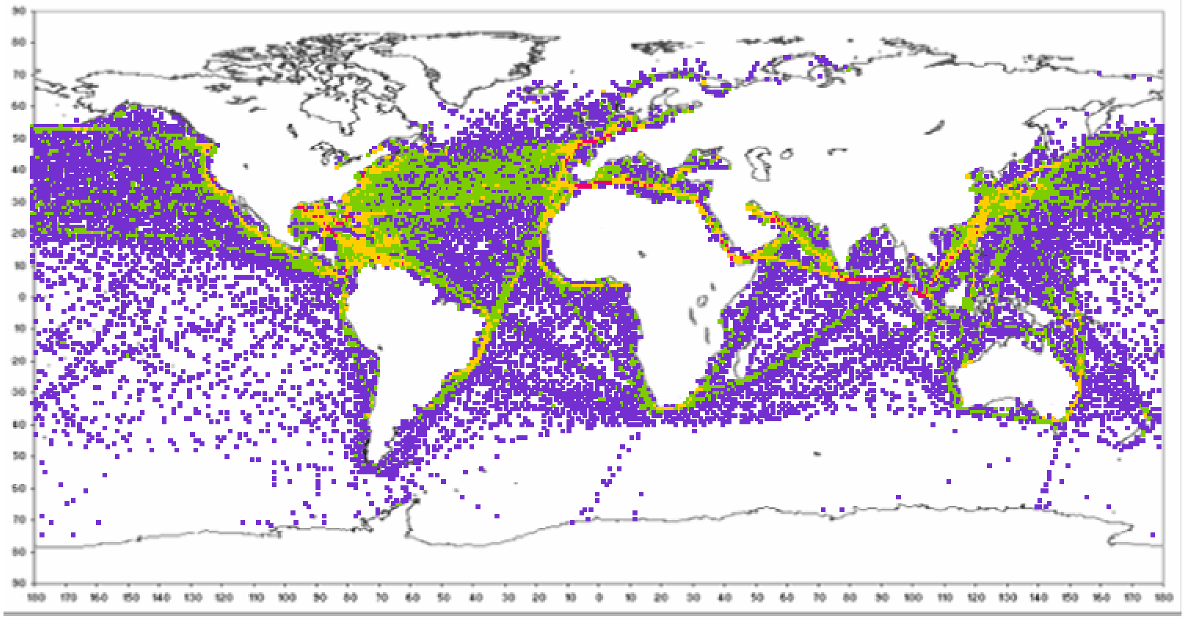


Figure 3. The portions of the ocean covered most effectively by AMVER in 2005. Blue pixels indicate areas traversed by one to four AMVER-equipped vessels in a month, while red areas are traversed by more than 50 in a month. Orange areas are more visited than green ones, but both are intermediate between red and blue. White areas are unvisited.

3.4 Long Range Identification and Tracking (LRIT)

LRIT stands for Long Range Identification and Tracking. It is a self-reporting system proposed for world-wide adoption and is being aggressively promoted by the Canadian and US Coast Guards. It would closely resemble AMVER in form and function, the primary difference being the purpose. Like AMVER, it would make automated position reports using communications equipment that vessels already carry, such as INMARSAT C. As well, it would use software to program the INMARSAT C terminals to report automatically and the communications would be free for the ship. So, the carriage, coverage, and reporting rate characteristics of LRIT would be similar to the first three SRSs discussed above. It is considerations of availability and access rights to the self-report information that differentiate LRIT from other SRSs.

Unlike AMVER, the planned purpose of LRIT is to support MDA primarily for national security purposes. Also unlike AMVER, participation would be compelled rather than solicited. The final form of LRIT is yet to be determined, but three classes of users are envisaged: flag states, port states, and coastal states. The first two users are generally accepted; the last is controversial. It is generally agreed that flag states have the right to require that vessels flying their flag report their position regularly. A port state, by which we mean the nation that owns the port to which a given ship is headed, is also allowed to demand regular position reports from an incoming vessel. This is seen as a natural extension of the 96-hour reports currently required of all vessels approaching US and

Canadian ports. However, allowing coastal states[8] to force a vessel in transit to report its position is said to interfere with the longstanding right of innocent passage. The International Mobile Satellite Organization (IMSO) has offered to oversee the LRIT program. It plans to poll all internationally bound vessels continuously using whatever satellite communications they have on board (generally INMARSAT). It would send countries the information about a vessel when they qualify to know about it under one of the three user classes. This plan, however, has met with considerable international opposition, in part out of concern that it too greatly empowers the IMSO. Most likely, therefore, the US and Canada will have to content themselves with national LRIT systems that poll only their own vessels and those bound for their ports. Even so, the system will likely provide a strong improvement to the RMP.

3.5 Automatic Identification System (AIS)

Automatic Identification System (AIS) is a self-reporting system for sea-going vessels that originated in Sweden in the early 1990s. It was designed primarily for safety of life at sea (SOLAS) and proposed as an automated system for ships to exchange high-accuracy navigational data. When two ships are within radio reception range of each other, they exchange identity, position, course, and speed information across a VHF data link using the self-organizing time-division multiple access protocol upon which AIS is based. Because of the requirement for self-organization, it is based on a continuous broadcast of self-report information every 2 to 10 seconds depending on vessel speed. Once two or more ships are within VHF radio horizon of each other, they form a network amongst themselves to share information to ensure safe passage. The AIS protocols and radio standards have been refined and accepted by the International Telecommunications Union (ITU) as an international standard and the AIS system has been mandated by the International Maritime Organization (IMO) for carriage by a broad class of large ocean going ships world wide.[9] Over 400,000 ships with AIS are listed in a database maintained by the ITU.[10]

The AIS system is fundamentally different from the previous SRSs discussed here in that it is based on a broadcast (or simplex) protocol for self-reports rather than a duplex protocol where the destination of the self-reports is pre-defined. This means that coverage, availability, and latency of self-report information to a SOC can be determined by deploying receiving systems in locations of interest rather than by relying on other organizations to provide the information. This is one aspect of AIS that makes it an appealing source of information for MDA. The positional accuracy of the self-reports can be better than estimates provided from primary sensor systems, such as passive or active radar. Furthermore, with updates at a rate of every 2-10 seconds, which again is better than many primary sensor systems, AIS provides the potential for very high fidelity

[8] According to the US definition, coastal states are nations whose coastline has at least one point within 2000 nautical miles of a given ship.

[9] See Automatic Identification System Overview – U.S. Coast Guard Navigation Center, http://www.navcen.uscg.gov/enav/ais/default.htm

[10] See Maritime mobile Access and Retrieval System (MARS) – International Telecommunication Union, http://www.itu.int/ITU-R/terrestrial/mars/index.asp

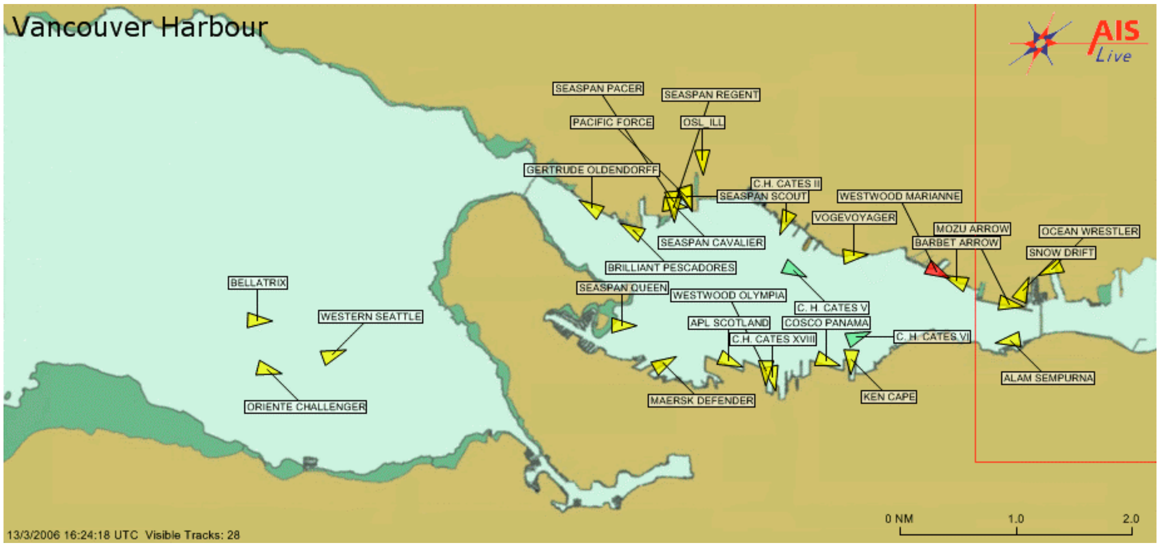


Figure 4. The positions of AIS-equipped vessels in Vancouver harbour on March 13th, 2006 are shown using isosceles triangles labelled with the vessel name.[12]

vessel tracking in regions of interest to the SOC. Finally, because AIS is broadcast to an unknown audience, access to the information is not a barrier to its use by a SOC. There may, however, be public policy considerations, as illustrated in section 4.3 below.

AIS transmissions are very easy to intercept, if one can get within VHF radio range of the ships making them. Thus, AIS data has had a dramatic impact on the Canadian RMP, particularly since fisheries surveillance aircraft started to carry AIS receivers. The ease of interception is not limited to security agencies. Indeed, private companies have started to publish current pictures of AIS traffic in harbours around the world on the internet (Figure 4). This suggests that terrorists and criminals have ready access to considerable amounts of AIS data.

While AIS information has the potential to be an extremely valuable information source for a SOC, current implementations of the AIS system have a major drawback. That is, the self-report information is prone to human error and potential malicious altering and the system itself was not designed with these vulnerabilities in mind.[11]

3.6 Automated Dependent Surveillance – Broadcast (ADS-B)

Automated Dependent Surveillance – Broadcast (ADS-B) is a self-reporting system for commercial aircraft that is under development as a basis for automated airborne collision avoidance. It promises to provide similar benefits for the airborne component of MDA that AIS provides for the surface vessel component. Similar to AIS, it is a broadcast protocol where aircraft navigational data is broadcast as frequently as once a second and data exchange networks are automatically formed between aircraft that are in close

[11] Shwu-Jing Chang, “AIS Applications as an Efficient Tool for VTS: Identifying and Coping with Discrepancy between Ideal Cases, Standard and Real Situations,” Sea Technology 47(3): 15-18 (2006).
[12] From Aislive.com, www.aislive.com

proximity. Although it uses a different data link protocol than AIS, namely Mode-S, and operates above the VHF band to allow for higher data rates, it has basically the same advantages as AIS as a source of domain awareness information. Namely, the spatial accuracy of the GPS-based self-reports is substantially better than the location and speed information that could be derived from time-of-flight and bearing estimates from a primary sensor system such as radar. Also, because it is a broadcast protocol, it is possible to receive passively the information that is transmitted.

The potential benefits of evolving systems, such as ADS-B, for maintaining awareness of civilian air traffic by the military has been recognized for some time.[13] However, the benefits of ADS-B for MDA in general are only now being widely recognized as it gains acceptance in the aviation community. This system shares the same potential pitfalls of a broadcast-based system as those discussed for AIS above.

3.7 Enhanced Position Locating and Reporting System (EPLRS)

In addition to the SRSs discussed above that were developed for and are evolving in the commercial world, we include a military example for comparison. Self-reporting is common in military systems to maintain blue-force situational awareness among allied decision-makers. One example is the Enhanced Position Locating and Reporting System (EPLRS) used by the US Army and Marines for about 20 years.[14] It provides near real-time, GPS-based position and force movement information among individual soldiers and both land and air vehicles. It employs time-division multiple access and operates in the UHF band to provide tactically and operationally useful coverage in both ground-to-ground and ground-to-air applications. Unlike the other self-report systems discussed here, the EPLRS self-report information is provided by military forces for other national and allied military forces. As a result, availability and the access given to others are strictly controlled.

It is critically important that military self-report information not be available to adversaries. Hence it needs to be protected using cryptographic techniques, both at the information level and transmission level and strong authentication is required from new participants in a military self-reporting network. Access to the information is protected based on these strong authentication techniques. In contrast to commercial systems, the coverage of a military system like EPLRS is focused at the tactical and operational levels, but detailed information regarding coverage characteristics as well as self-report latency information and update rates are guarded as sensitive information.

4. The Social and Policy Dimension of Self-Reporting Systems

[13] G.A. Van Sickle, "Allied Air Identification," Proceedings 4th Annual Symposium and Exhibition on Situational Awareness in a Tactical Air Environment, Piney Point Maryland, 8-9 June 1999.
[14] See Enhanced Position Locating and Reporting System - (EPLRS), http://www.marcorsyscom.usmc.mil/sites/pmcomm/EPLRS.asp

While the previous sections focused on the five “W” aspects (who, what, where, when and why), this section deals with the more human aspects of SRSs, as related to MDA. In this realm, important concerns related to SRSs are ensuring that there are as many self-reporting participants as possible and ensuring that the information collected is accurate. This section reflects on how to satisfy these requirements by dwelling on topics such as privacy and trust, proposed methods of getting people to participate in SRSs, and proposed public policy.

4.1 Privacy and Trust

In democratic societies, there exists the concept of the *right to privacy*. Although it’s hard to get collective agreement on a precise definition of privacy, who should expect it, and under what conditions, it is generally agreed that the extent of an individual’s right to privacy must necessarily be restricted to some degree for the greater good of society.[15,16] Expectations of privacy are dependent upon culture, location, time of day, and a myriad of other factors. What makes someone want to keep a piece of information private? Fear, shame, mistrust, simply not wanting to share – the reasons are many and complicated. In recent years, advances in information technology have improved the efficiency of delivering goods & services and at the same time permitted intrusion into our private lives. The relationship between self-reporting systems and maritime domain awareness reflects this general trend in society. The intent of homeland-security surveillance is to detect threats to the country. The surveillance required to achieve that end can include the monitoring of innocent civilian activity. To build accurate maritime domain awareness, monitoring innocent civilian activity is definitely required to build a complete awareness of the domain. Nevertheless, people tend to want to keep what is going on in their own lives, or in their company, private, or at least confine the information to a group of people who they know and trust. Many people are not inclined to voluntarily share information they deem to be “their own business”. This is part of the information quality problem in the context of self-reporting systems helping to build MDA: the more people who share information, the better the MDA.

The presence of trust, mentioned above, is actually a very important aspect of requesting, giving and receiving private information. On several levels, the concept of “trust” permeates the concern of using SRS information for MDA. On the technical level, there is trust in the communication channel and trust in the processing and storage of the information. On the social and public policy level, there exists mutual trust between participants: the authorities collecting the information trust the self-reporters not to intentionally corrupt the information or mislead; on the other hand, the individuals providing the information trust the authorities to use the information only for the intended purpose and to respect their privacy. A breakdown of trust between authorities and self-reporting individuals could compromise the information quality and quantity.

[15] Andrew J. Charlesworth, “Privacy, personal information, and employment,” Surveillance & Society 1(2): 217-222 (2003), http://www.surveillance-and-society.org

[16] David Lyon, ”Surveillance Studies: Understanding visibility, mobility, and the phonetic fix,” Surveillance & Society 1(1): 1-7 (2003), http://www.surveillance-and-society.org

Table 1: The Social Characteristics of Self-Reporting Systems and their Relevance to Maritime Domain Awareness

Key Characteristic	Related Factors
Who pays the costs of equipment and communications?	Level of participation in the system and potential for errors or spoofing (where there is resentment).
Is it voluntary or a legal requirement?	Level of participation in the system and potential for spoofing (where there is resentment).
Are there benefits to those who self-report?	Level of participation in the system
Are there expectations of privacy or restrictions on distribution?	Level of participation and availability of information to security agencies
How hard is it to intercept the communications.	Availability of information to security agencies. Availability of information to enemies (terrorists).
Is the data available on the internet	Availability of information to security agencies. Availability of information to enemies (terrorists).

This social dimension is significant in self-reporting systems to a degree not seen with traditional sensors. An attempt to understand a self-reporting system is necessarily an attempt to understand the motivations and attitudes of participants, whereas an attempt to understand radar (for example) does not so strongly pull one away from physics and engineering. One wonders why self-reports are being sent, how the senders regard the system, whether they would care if the information were wrong, and who they think is able to receive the transmission or view the information. Considerations like these belong to the realm of social psychology. We propose that certain characteristics of a self-reporting system determine the attitudes of participants towards it; that is, they encourage or discourage people to provide the private information that is wanted. By extension, the attitudes of the participants will largely determine the SRS's impact on MDA.

4.2 Social Characteristics of Self-Reporting Systems

Some characteristics of SRSs that are relevant to the social domain are listed in Table 1. Several of these involve the extent to which the system is likely to build resentment in the participant, as rising resentment could lead to decreased participation, to pervasive errors in reported data, or even to intentionally generating false reports, also known as spoofing. We suggest that characteristics of a self-reporting system that raise costs for participants or that are perceived to unreasonably invade people's privacy naturally lead to resentment and, therefore, would not be an incentive to participate.

We propose that there are but two ways to obtain the cooperation of potential participants in a self-reporting system: incentives and penalties. By incentives, we mean that participation has benefits. By penalties, we mean that lack of participation has costs. Some systems use both. Incentives and penalties help encourage a person or organization to release their private information by making it worth something to participate. When it comes to preserving the goodwill of participants, incentives are much preferred. This is

Table 2. Social Characteristics of Various Self-Reporting Systems

System	Cost to participant?	Benefit to participant? (a)	Participation compulsory?	Participants know data may be used for security?	Ease of report interception (b)	Data readily available to terrorists? (c)
AIS	Yes	Great	Yes	Probably	Easy	Yes
ADS-B	Yes	Great	Not yet	Probably	Easy	Yes
LRIT	No	No	Not yet	Yes	Hard	No
EPLRS	No	Great	Yes	Yes	Very Hard	No
VMS	Yes	Marginal	Yes	Probably not	Hard	No
AMVER	No	Yes	No	Promised not to	Hard	No
VOS	No	Yes	No	Probably not	Hard	Yes

(a) participant benefits from the self-reports of others
(b) how easy is it for an unintended recipient to receive and understand a self-report
(c) current self-report data is generally available on the internet or other public place

important because in self-reporting systems the quality of the data always depends on the goodwill of participants. Table 2 provides an overview of the systems considered above and summarizes their social characteristics for ready comparison. Table 2 suggests that AIS, ADS-B, AMVER, EPLRS and VOS, which invite participation with benefits, will generally yield better data than VMS and LRIT, which must force compliance.

Though self-reporting systems that provide incentives should typically provide better data, without some penalties for non-compliance, participation can be expected to dwindle. There is a very good reason for this: the benefits of self-reporting almost always come from the reports of others much more than they come from the participant's own, although EPLRS may provide something of an exception. This means that there is a temptation to be a free-rider, to take the benefits without taking the trouble to contribute. Unless the free-riders are curtailed in some way, or unless ways are found to reward active participation, self-reporting systems will slowly wither, as we see with the VOS system. This insight may also suggest why ADS-B, which provides all the benefits of AIS to participants but lacks the carriage requirements, has yet to make a contribution to domain awareness.

4.3 Public Policy and Self-Reporting Systems

Recognizing the social implications of using SRS information for security purposes, and the subsequent impact on the quality of information, it seems prudent for authorities to work with self-reporters towards a common understanding of surveillance and privacy in connection with security. This would instil in those concerned a sense of trust, which, as mentioned earlier, is an issue that can permeate the apprehension of using SRS information for MDA. Following the lead of Charlesworth,[17] we propose that some set of

[17] Andrew J. Charlesworth,"Privacy, personal information, and employment," Surveillance & Society 1(2): 217-222 (2003), http://www.surveillance-and-society.org

general principles be considered by those tasked with legal and regulatory oversight. The following is a suggested starting point:

- **A. Legitimate purpose** ~ authorities must identify a purpose for any privacy-intrusive measure, and only use the information in accordance with that purpose. Wherever possible, this should be publicized in advance of application of the measure.
- **B. Proportionality** ~ authorities should demonstrate that the privacy cost of the measure is outweighed by the gain in social benefit, and should ensure that the least privacy-invasive measure be adopted.
- **C. Fair, lawful, and equal** ~ measures should be considered fair, be subject to law, and apply equally to all.
- **D. Transparency** ~ the public must be informed about the purpose of any measure, and of the steps that authorities have taken to ensure the forgoing principles have been upheld.

These suggestions are probably in general accord with the society that most of us wish to live in, and may not be a panacea, but moving in this direction would certainly be preferable to ignoring the social and policy dimensions of the issue and forging ahead, with the probable loss of public trust and information quality that would ensue.

5. Impact of SRSs on Command Decision Making

Decision-makers dealing with national security and military commanders responsible for military missions other than war in busy maritime regions will be impacted by the information available from SRSs. This will be especially so for broadcast SRSs such as AIS and ADS-B. In this section, as we look at the impact of increased use of SRSs for decision making, we again assume that the decisions discussed are in support of a centralized security operations centre (SOC) where either military commanders or non-military leaders are responsible for the conduct of some security mission.

The first impact to be examined is from non-SRS using vessels being highlighted in the minds of decision-makers. Compared to traditional sensor-based contact information, modern SRSs have the potential to provide higher quality information, better update rates and lower latencies; not to mention they could give the receiver control of the update rate and latencies. These attributes will naturally increase the reliance that decision-makers place on SRSs and allow the decision-makers to focus on non-SRS using vessels. Knowledge of the self-reporting marine traffic helps a decision-maker sort out the total marine picture in that it helps reduce the number of unknowns so that more effort can be placed on sorting out the unknown vessels, if the information can be trusted. For example, there is currently no requirement for small pleasure craft to utilize a system such as AIS, although there are proposals for a similar system to be adopted by small craft. In a busy seaport environment, with a mixture of both commercial and pleasure craft, knowledge of the large craft based on self-reporting allows attention to be focused on those vessels that do no have an SRS installed.

As mentioned above, the level of trust that decision-makers have in SRS information will also impact their decisions. That level of trust a decision-maker places on SRS information becomes increasingly important as the availability and use of self-report information increases. How much can the decision-maker trust all those SRS contacts so that the decision-maker can focus on learning more about vessels of interest, such as non-SRS using vessels? If vessel awareness in the AOR for the SOC has traditionally been based on sensor systems, such as radar or electro-optic systems employed by the centre itself, then the trust in that sensor information is usually based on experience with the sensor in the operating area coupled with an understanding of the basic physics of the sensor. For example, if a SOC employs a long-range surface surveillance radar, over time operators learn the effects of weather and season on sensor performance and develop a basic understanding regarding the sizes and types of vessels that will be detected, tracked and potentially identified by the radar. With information such as self-reports, however, trust is based on the ideas of information-trust put forward by the information & network security community. That is, trust in self-report information as it arrives at the SOC is based on trust in the original source of the information itself, trust in the communication and network paths between the source and the SOC and trust in any computation or manipulation that is conducted on the information en route to the SOC.

Systems like AIS are still quite new to the maritime world and there is a growing realization that there are situations where one cannot rely on AIS information without reservation.[18] For example, criminals and terrorists can exploit self-reporting systems, by either obtaining or spoofing information. Spoofing is only to be expected: any system which gives individuals the ability to send a report also gives them the opportunity to lie. Spoofing can have severe negative impacts on MDA, particularly if too much trust is placed on self-reports. However, if the decision-makers are aware that spoofing is occurring, then it also poses opportunities to catch the culprit in the act. Assuming that spoofers are up to no good, then spoofing detection could lead to the early identification of criminals and terrorists. Trust in self-report information like AIS can be improved through a good understanding of the information vulnerabilities of the system coupled with an understanding of how to reduce or eliminate those vulnerabilities. Also, one needs to develop an understanding of the sources of misinformation, both accidental and malicious.

Finally, another important impact SRS information can have on decision-makers evolves from the information sharing policies under which the information is provided. These policies could be determined by those managing the SRS or by government legislation. The information sharing policies can impact a decision-maker in their ability to make collaborative decisions, if the information cannot be shared openly in the collaboration process. This is typically not a problem for sensor derived information, such as radar contacts, since the SOC will usually control the distribution of the information. However, since self-reports originate outside an SOC, information sharing can become more complicated. An interesting example of this complication arises when military ships are

[18] Shwu-Jing Chang, "AIS Applications as an Efficient Tool for VTS: Identifying and Coping with Discrepancy between Ideal Cases, Standard and Real Situations," Sea Technology 47(3): 15-18 (2006).

asked to become active participants in an SRS. The decision to openly share accurate navigational data with non-military vessels and SOCs is one that military commanders do not take lightly and will likely be done only when absolutely required or when it is in the best interest of the commander.

6. Concluding Remarks

Self-reporting systems have been in use by the commercial and non-military world for some time now. However, their impact on decision making related to maritime security and defence has been limited by their infrequent update rates, their long latencies and the potential difficulties associated with sharing self-report information. These sharing issues usually arise because the self-report information is collected at some central location that is not controlled by the SOC. The growing use of broadcast SRSs such as AIS and ADS-B, which provide very accurate navigational information at very high update rates with potentially low latency, has peaked interest in these SRSs by those interested in MDA. Because they are broadcast systems, the availability and timeliness of this information to a SOC is more under the control of the SOC and very high-quality information can be obtained for some maritime area of interest, if receivers can be properly positioned and appropriate communication links can be established between the receiver(s) and the SOC. However, even with modern broadcast SRSs, there could still be potential use and sharing issues.

Unlike traditional sensors that have been used for establishing MDA, there is a strong human element to SRSs. For example, in order for SRSs to be useful in helping build an MDA and ultimately helping decision-makers make good decisions, as many people as possible have to be using the system and they have to provide accurate information in their self-reports. People need incentives to participate and provide accurate information. One of those incentives is trust between the people providing the information and the people using the information. From the decision-maker’s point of view, there needs to be trust in the information as well; i.e., trust that it has not been tampered with or accidentally altered.

The modern SRSs are poised to be very valuable in maintaining maritime domain awareness. Will the existence of SRSs one day do away with the need of additional information from physical sensor systems? Probably not until nearly every ship participates in an SRS and the information is generally accurate and tamper-proof. Until then, corroboration will be needed. However, SRSs definitely can provide information traditional sensors have not been able to provide and in a timely manner on top of that. Command decision making will be greatly helped by SRSs.

Acknowledgements

The authors thank their colleages at DRDC Atlantic, Dr. Jacqui Crebolder and Ms. Tarra Penney for resources and discussions regarding the social psychological aspects of this work and Mr. Bill Campbell for his valuable comments and discussions on this topic.

DOCUMENT CONTROL DATA

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

1. ORIGINATOR (The name and address of the organization preparing the document, Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's document, or tasking agency, are entered in section 8.)

Publishing: DRDC Atlantic
Performing: DRDC Atlantic
Monitoring:
Contracting:

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification is indicated by the appropriate abbreviation (S, C, R, or U) in parenthesis at the end of the title)

The Implications of Self−Reporting Systems on Maritime Domain Awareness (U)
(U)

4. AUTHORS (First name, middle initial and last name. If military, show rank, e.g. Maj. John E. Doe.)

Tim Hammond, Mark McIntyre, Dave Chapman and Liesa Lapinski

5. DATE OF PUBLICATION (Month and year of publication of document.)

September 2006

6a NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

20

6b. NO. OF REFS (Total cited in document.)

18

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of document, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Literature

8. SPONSORING ACTIVITY (The names of the department project office or laboratory sponsoring the research and development − include address.)

Sponsoring:
Tasking:

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant under which the document was written. Please specify whether project or grant.)

11hf

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document)

DRDC Atlantic SL 2006−123

10b. OTHER DOCUMENT NO(s). (Any other numbers under which may be assigned this document either by the originator or by the sponsor.)

ICCRTS Paper I−093, DRDC TM 2006−232

11. DOCUMENT AVAILABILITY (Any limitations on the dissemination of the document, other than those imposed by security classification.)

Unlimited distribution

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11), However, when further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited announcement

DOCUMENT CONTROL DATA

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

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

(U) Self−reporting systems based on GPS−quality navigation information that is sent using widely−accepted standards and protocols, offer the potential to greatly improve important components of Maritime Domain Awareness (MDA). The purpose of this paper is to provide an overview of some existing and evolving Self−Reporting Systems (SRSs) and to characterize them in order to discuss their relative impact on MDA. We argue that broadcast−based SRSs, such as Automatic Identification System (AIS), offer significant advantages over traditional sensor−based vessel tracking and that availability of information from SRSs will impact how command decisions related to MDA are made in the future. The social and public policy dimensions of using SRSs information for MDA are explored, especially encouraging people to participate in SRSs. Also, we discuss some of these impacts and raise the question of how much trust decision−makers should place in self−report information.

(U) Les systèmes d'auto−signalisation (SAS), qui utilisent de l'information de navigation de qualité GPS transmise selon des normes et protocoles largement adoptés, offrent la possibilité d'améliorer considérablement des éléments importants de vigilance dans le secteur maritime (VSM). Le présent document donne une vue d'ensemble de certains systèmes d'auto−signalisation existants et en évolution, et il en expose les caractéristiques dans le but d'évaluer leur impact relatif sur la VSM. Il avance que les SAS à diffusion, comme le système d'information automatisé (SIA), offrent des avantages significatifs comparativement à la poursuite des navires par détecteur ordinaire et que la disponibilité de l'information en provenance des SAS influera sur la façon dont les décisions de commandement relatives à la VSM seront prises dans l'avenir. Le document examine les dimensions sociales et publiques que comporte l'utilisation de l'information des SAS pour la VSM. Il aborde aussi l'impact de la prise des décisions de commandement et soulève la question de la fiabilité que les décideurs devraient accorder à l'information d'auto−signalisation.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

(U) self−reporting systems, AIS, maritime domain awareness