



The Impact of Self-Reporting Systems on Maritime Domain Awareness

Tim Hammond, Mark McIntyre, Liesa Lapinski, Dave
Chapman

11th International Command and Control
Research and Technology Symposium



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada

Canada



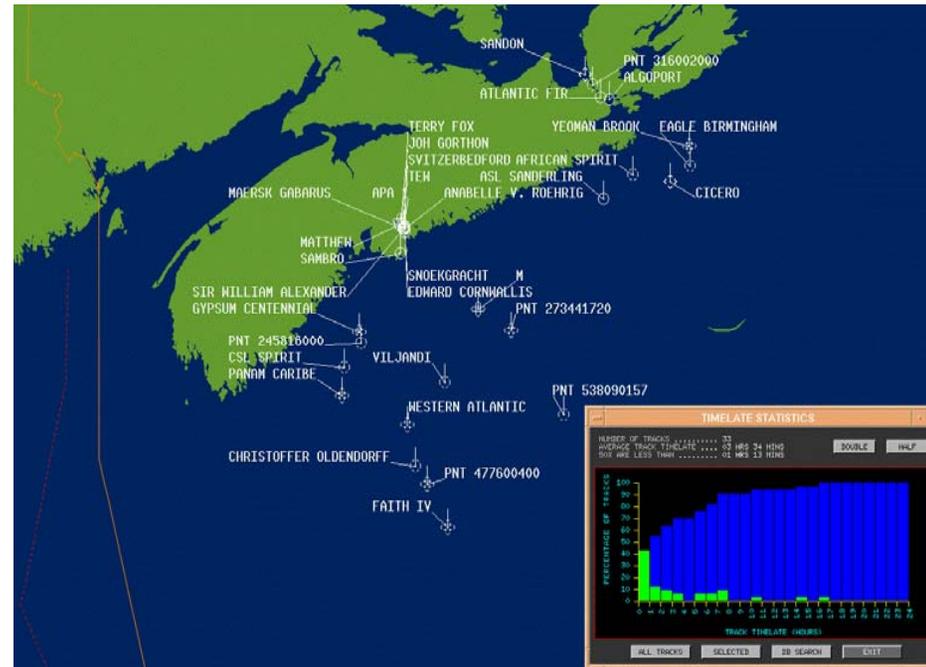
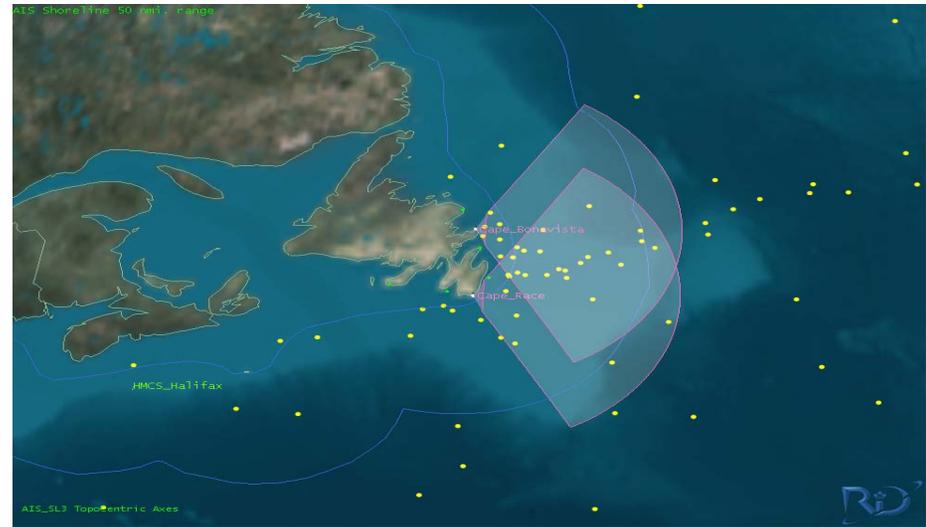
Maritime Domain Awareness (MDA)

- *Maritime Domain Awareness* is much like *situational awareness* or *battlespace awareness*.
- The term MDA was coined by the USCG, however, so it tends to have more of a civilian safety and security focus.
- MDA is the effective understanding of anything associated with the maritime domain that could affect a country's security, safety, economy, or environment.
- This talk focuses on awareness of civilian shipping activity.



The Rise of Self-Reporting Systems

- In the last few years, there has been a big increase in the apparent quality of the RMP.
- Before, it was easier to **locate** a ship contact than to **identify** it, leading to the “yellow dot problem”.
- Since the rise of self reporting systems, far more ships are identified in the RMP.





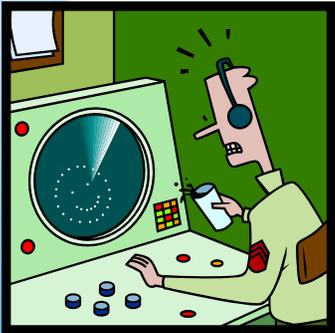
What is a Self-Reporting System?

- A self-reporting system (SRS) is one where an entity (like a ship) may report its own identity and position in a conventional format.
- SRS become useful for security purposes, if government authorities
 - are the intended recipients of the self reports,
 - obtain the self report by various means
- Identity information is very specific- down to the serial number of the unit, not just to type
- Accuracy of position reports tends to be higher than what can be obtained from conventional sensors.



New Considerations in ISR

- SRS are different from traditional surveillance sensors (like RADAR) for several reasons:
 - The value of a SRS depends on the participation level.
 - The quality of the information from a SRS depends on the goodwill of participants.
 - Self reports are currently easy to spoof
 - Understanding an SRS is less about physics and engineering and more about social psychology.
- In developing trust in a SRS, 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 information.





Encouraging active participation

- There are only two ways to get people to participate in an SRS: the carrot or the stick.
- The carrot is much better at preserving goodwill, so a good SRS should reward participants.
- Unfortunately, the benefits of a SRS tend to come more from the reports *of others* than they do from a participant's own. Thus, there is a temptation to take the benefits of the system without contributing (passive participation).
- The stick, of course, is much better than the carrot at discouraging passive participation.



Preserving Goodwill

- Three things can destroy the goodwill of mariners:
 - Raising their costs
 - Invading their privacy in a way perceived to be unjustified
 - Letting their competitors obtain sensitive information
- Privacy concerns can arise when security agencies use self report information even though they are not the intended recipients of the reports.
- Participants need to trust authorities to use self-reports with discretion.



Evaluating Self-Reporting Systems

- So, let's look at some self-reporting systems that are in current use and ask:
- Who is bearing the cost?
- Are there benefits to the mariner or is it a legal requirement?
- How easy is spoofing?
- How easily can bad guys get access to the data?
- To what extent are expectations of privacy being violated in using the data for security.
- Who owns the information?



The Automatic Identification System (AIS)

- Ships with AIS make self-reports every 2-10 seconds by VHF radio and receive these reports from other vessels.
- International Convention for the Safety of Life at Sea (SOLAS) mandates that AIS must be fitted to:
 - all new ships on international traffic since 2002
 - all passenger (12+ passengers) ships since 2004
 - all ships over 300 tonnes on international traffic since 2004
 - all ships over 500 tonnes by 2008



Mariners bear the costs, but AIS helps ships avoid collisions.



Fishing boats have to carry VMS

- DFO uses satellite tracking to monitor the activities of fishing fleets.
- Since January 1, 2001, all vessels fishing for groundfish or shrimp in the NAFO Regulatory Area were required to be equipped with a vessel monitoring system (VMS). These systems cost the ship \$1500 to \$5000 + calls
- VMS allows for the tracking of vessels by satellite.
- Fisherman are very concerned that their fishing locations remain private. Any sharing of the data, even within the Canadian government, is likely to worry them.



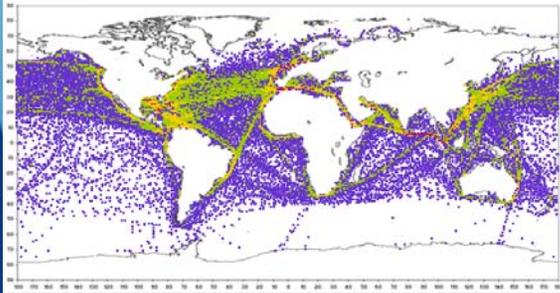


VMS Report Card

- VMS would have a dramatic impact on the RMP, though it is not as rich a data source as AIS.
- Due to legal concerns about who owns the data, VMS has not had the impact in Canada that it has had in other countries.
- VMS provides little if any benefit to the fishermen and increases their costs. Resentment can be expected.
- VMS is nearly as easy to spoof as AIS.
- It is relatively hard for bad guys to get the data.



AMVER –(Automated Mutual-Assistance Vessel Rescue)



- All mariners are obligated to respond to distress calls from their fellows, but they do lose time and money in doing so.
- AMVER, run by the USCG, promises to reduce the time spent responding to distress calls, by diverting only the closest, most suitable vessels to an emergency. In exchange, vessels have to provide regular self-reports of their position.
- Ships from 148 nations participated in AMVER in 2005: on an average day, 3004 ships reported their position.
- Information sent to AMVER is “protected and used only in a bonafide maritime emergency.”



AMVER report card

- Clearly, AMVER data would be useful to the RMP.
- Mariners are unlikely to resent a system that saves them money, though US flag ships use AMVER mainly to fulfill legal reporting requirements.
- It's hard for bad guys to get the data.
- Spoofing would be possible, but seems to provide more risks than benefits.
- AMVER seems to provide an ideal security system, but for that inconvenient promise only to use the data in a “bonafide emergency”. How upset would participants be if this promise were broken?



Conclusions

- SRS can have a big impact on MDA. They focus attention on remaining unknown targets.
- SRS should be used in such a way as to preserve the goodwill of participants.
- Trust is essential. Operators need to trust SRS participants to report accurately and participants need to trust operators to use data appropriately.
- Where there are privacy concerns it is wise to justify the use of self reporting data for security purposes *before* starting to use them for those purposes.
- Broadcast SRS, like AIS, are particularly attractive for security because the frequent position reports can be monitored passively.

DEFENCE



DÉFENSE