Assessing the information content of Maritime Domain Awareness data

Applications to classification guidance

Bruce McArthur
Anthony W. Isenor
DRDC – Atlantic Research Centre

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2015-R207
October 2015

Abstract

The development of Maritime Domain Awareness (MDA) is a multi-faceted and multi-departmental activity within the Canadian Government. In the development of MDA, many data and information sources are brought together or aggregated to help formulate an awareness of vessel activity in and approaching Canadian waters. DND research and development focused on MDA often encounters the issue of data/information distribution to partners or collaborators. In an effort to establish a common understanding of data distribution to partners or collaborators, this report uses several data distribution use cases, combined with an examination of existing security guidelines, to formulate conclusions regarding the distribution of MDA-relevant data/information to partners both internal and external to government. One important conclusion is that distribution of non-real-time Automatic Identification System (AIS) data should not be designated. This work provides the guidance necessary for future data/information distribution especially with external organizations such as academia.

Significance to defence and security

The distribution of MDA data and information is pertinent to the cooperative, multi-departmental formation of MDA in Canada. This document describes several MDA data/information types and the classification that should be assigned when the data/information is distributed to partners.

Résumé

Le développement de la connaissance du domaine maritime est un exercice à volets multiples qui touche plusieurs ministères au sein du gouvernement du Canada. Pour développer la connaissance du domaine maritime, on regroupe de nombreuses sources de données et de renseignements pour permettre l'élaboration d'une connaissance des activités des navires naviguant dans les eaux canadiennes ou qui s'en approchent. Les efforts de recherche et développement du MDN qui se concentrent sur la connaissance du domaine maritime se heurtent souvent au problème de la distribution des données et des renseignements aux partenaires ou collaborateurs. Afin d'établir une compréhension commune de la distribution des données à ces partenaires et collaborateurs, le présent rapport utilise divers cas de distribution des données, combinés à un examen des lignes directrices existantes en matière de sécurité, pour formuler des conclusions relatives à la distribution de données et de renseignements pertinents à la connaissance du domaine maritime aux partenaires à l'intérieur et à l'extérieur du gouvernement. Une conclusion importante établit que la distribution des données du Système d'identification automatique (SIA) en temps non réel ne devrait pas être désignée. Cet ouvrage fournit l'aide nécessaire pour procéder à une distribution future de données et de renseignements orientée surtout vers les organisations externes, comme le milieu universitaire.

Importance pour la défense et la sécurité

La distribution de données et de renseignements en matière de connaissance du domaine maritime se rapporte à la formation coopérative entre plusieurs ministères de cette connaissance au Canada. Le présent document décrit plusieurs types de données et de renseignements ainsi que la classification qui devrait être attribuée lorsque ces données et renseignements sont distribués aux divers partenaires.

Table of contents

List of tables

Acknowledgements

The authors acknowledge the input of Francine Desharnais in multiple discussions related to the distribution of Maritime Domain Awareness data, and her support for the preparation of this document.

This page intentionally left blank.

1 Introduction

Maritime Domain Awareness (MDA) is described as "having true and timely information about everything on, under, related to, adjacent to, or bordering a sea, ocean or other navigable waterway" [1]. In Canada, the development of MDA is a multi-faceted and multi-departmental activity that involves the aggregation of the data and information sources that once combined, help formulate an awareness of vessel activity in and approaching Canadian waters.

In conducting research and development focussed on MDA, one often encounters the issue of data/information distribution to partners or collaborators. The determination of how information is to be managed and to what extent it can be shared is directly affected by the information's sensitivity, and is a key focus of information security.

This report is intended to clarify and provide guiding comments regarding the handling of DRDC maritime data. Specific consideration is given to the sensitivity of information linking a detected object's geo-temporal location with data describing the object's identity. One aspect of this work deals with data collected from Automatic Identification System (AIS), a self-reporting system that can provide both geo-temporal and identity information and that is generally considered to be unclassified. Similar issues, arising from integration of data from multiple sensors or self-reporting systems, are also considered. Data collected by Northern Watch (NW), a DRDC project to demonstrate local-area Arctic surveillance using multiple sensors and self-reporting systems, is presented as a specific example to illustrate these issues.

This scope of this report is limited to data collected by DRDC. It does not apply to data purchased or obtained from partners via data sharing arrangements. In addition, the scope of this report does not include: the sensitivity of information linking a detected object's signature with its identity; the sensitivity of information related to how data is processed (as an example, the processing of AIS signals); or intelligence information.

1.1 Outline

The following report discusses issues surrounding the management and distribution of data and information pertinent to MDA. Section 2 considers data that links a object's geo-temporal location with identity, with focus on data provided by AIS. Section 3 extends the discussion on the linking of contact location with identity to consider, as a specific example, the sensor data types included in the Northern Watch surveillance system.

2 Combining contact data with identity

For the purpose of this guide, contact data shall be defined as follows: the geo-temporal location of a maritime surface or sub-surface object; that is, a geographically-referenced position, such as latitude-longitude, and the date/time at which the contact was located at that position. In turn, identity is defined to be information that is unique to an individual object. The definition of object excludes individual persons; thus, for the purpose of this paper, identity data refers to data about objects, and does not refer to individual persons.

The combining of contact data with identity presents certain difficulties related to the distribution of these data. In particular, an object's identity provides the potential for linking the object (i.e., a vessel) to a passenger or, more generally, to a person onboard the vessel.

Multiple MDA-relevant data sources provide the combination of contact data with identity. For example, the Automatic Identification System (AIS) provides contact and identity data for maritime vessels and the Automatic Dependent Surveillance-Broadcast (ADS-B) system provides similar data for aircraft.

In the case of AIS, vessel identification information can be in the form of a vessel name, or an identifying number (e.g., the Maritime Mobile Service Identity or MMSI). Similarly, in the case of ADS-B, aircraft identification information can be in the form of the call-sign or the aircraft-specific ICAO (International Civil Aviation Organization) number. In other cases, vessel identity can be added to the metadata associated with the contact, this providing the same end result; a vessel's geo-temporal location with identity.

2.1 AIS data

2.1.1 Common reasons for protection

A series of discussions dealing with the designation[1] of AIS data indicated that there were four potential reasons that may lead one to treat AIS data as Protected. These potential reasons were:

1. In terms of a vessel data set provided to a partner, it is possible an identified vessel in the data set is a Government of Canada (GoC) Vessel-of-Interest (VOI);
2. There are possible sensitivities related to publicly stating that DND has collected data from what may have been an announced or unannounced vessel;
3. AIS data may itself contain private information or it may be linked with the names of people onboard a vessel; and
4. IMO guidelines [2] regarding unrestricted release of AIS data.

[1] Information that is Designated is "sensitive in other than the National Interest" and includes "personal information, government business operations, information received in confidence, and advice." The levels of designation are Protected A, Protected B, and Protected C, with Protected A having the lowest level of sensitivity. Information that is Classified is identified as "government information that concerns the defence and maintenance of the social, political and economic stability of Canada." [3].

In the following, arguments are presented that refute the need to designate the data based on the reasons above:

1. Any data set that DRDC may provide to partners could have a GoC VOI present. The larger the data set (i.e., a larger time period) the more likely this is the case. However, any VOI that may be present in the data set is not identified as a VOI. This is considered to be a critical difference.

   This is supported by the lack of issues raised by the aggregation activities being conducted by the Maritime Information Systems (MIS) group. MIS has conducted activities in the areas of maritime data aggregation and archival for approximately seven years. Numerous DND organizations and associated staff have been briefed on these activities. No party has raised any issues related to these activities or related data management practices.

2. Regarding possible sensitivities in publicly announcing the collection of data by DND from what may have been an announced or unannounced vessel:

   a. DND has a mandate to monitor Canadian approaches. The Canada First Defence Strategy [4] states:

      > *"The Forces must also work closely with federal government partners to ensure the constant monitoring of Canada's territory and air and maritime approaches, including in the Arctic, in order to detect threats to Canadian security as early as possible."*

      Clearly it does not say DND is solely responsible for conducting the monitoring. However, collaborative monitoring among the departments, which include DND, is indicated; and, monitoring by DND is not in conflict with the above statement.

   b. In discussions with subject-matter experts within DND, AIS broadcasts were considered to be machine-to-machine exchange; and thus not a form of personal communication. At the time, it was indicated that the legal opinion was that AIS broadcasts could be collected.

      One potential exception was noted. It is possible to add a comment field to AIS message types 6 and 8. Such a comment could be used to communicate a personal message and, in this case, the legal opinion becomes more complex.

3. Whether or not to make publically available the contact with identity is directly influenced by whether or not the vessel identifier is considered personal information. If one considers the contact and identifier to be personal, then the connection is made to the Privacy Act [5].

   Section 3 of the Privacy Act defines personal information "as information about an identifiable individual" [5]. The AIS vessel identifier (whether a ship name or MMSI number) is information about the vessel, rather than information about an identifiable individual. Therefore it can be argued that identity information from AIS should not be regarded as personal information.

   As well, the fact that the Government of Canada endorses the IMO regulation for broadcasting Class A AIS on specified vessel classes[2] would seem to imply that the broadcast information is not in conflict with the Privacy Act. Again, this is interpreted as meaning the

[2] The requirements for AIS usage are based on factors that include tonnage, type of voyage (international or domestic), number of passengers, ship type and ship age.

contact and identity are not considered personal information. This would apply to only Class A AIS, since this is the type of AIS included in the IMO regulation.

Class B AIS, a low-power variant of Class A AIS, is present on some smaller boats such as personal sailcraft, for which there may be a closer link between the identity of a vessel and its operator. At the moment, Class B broadcasts are voluntary. As a result, the captain of the boat is in total control of whether or not the system is broadcasting and by doing so, one can argue that the operator has consented to the release of the information contained in the AIS broadcast.

In the case of passenger vessels and the broadcast of Class A AIS, the passenger list is considered personal information. The privacy of the passenger list would appear to rest with the vessel authority (i.e., the owner or company operating the vessel). However, as the passenger list is not included as part of the AIS broadcast, the release of AIS information does not by itself provide information related to any specific individual on the passenger list.

4. The IMO [2] discourages publication of AIS data as it "could be detrimental to the safety and security of ships". IMO makes no mention to the timeliness of data release, thus implying any release could be detrimental.

   It is recognized that DRDC must be a responsible data custodian. However, DRDC does not provide real-time release of AIS data. In terms of displaying AIS data in a publication, it is suggested that delaying the release of the contact and identity would meet the spirit of the IMO guideline (i.e., the release does not include real-time data).

   In terms of sharing a data set, it is recommended a User Agreement, which includes release restrictions related to data latency, be put in place with the receiving party. For a recipient outside the Government of Canada, the suggestion is a two week data latency. This latency value—representative of the time required for a merchant vessel to transit the Pacific Ocean—is sufficiently long that a vessel could move well away from its last reported position, and should thus allay safety and security concerns associated with real-time release of data[3]. For release to another Canadian Government department/agency, the latency should be negotiated through DRDC Science and Technology External Relations (DSTER).

   Such a User Agreement should provide DRDC with intellectual property and legal protection. If required, this can be enhanced by ensuring the receiving party does not publish identifiers for vessels.

Given the above, the authors consider it unnecessary to protect (i.e., designate) the AIS data collected by DRDC.

2.1.2 Access to information

A second approach to considering the potential sensitivity of AIS data, is to use the perspective of the Access to Information Act (ATIA) [6] and its associated "injury test". In order for information to be exempt from Access to Information regulations, it must fall into one of a specified set of categories (this is termed the "class test") or it must satisfy an "injury test". The injury test determines whether the release of the information could result in an injury to one of the national

[3] The authors were unable to identify any existing national or international regulations on the latency of releasable AIS or related maritime data.

or non-national interests described in the Act. According to the ATIA, the injury test considers whether the injury is:

1. specific: that there is a specific party (i.e., an individual, organisation or nation) who can be identified as being at risk of a specific injury to their interests;
2. current: that the injury can occur at present or in the foreseeable future; and
3. probable: that there is a reasonable probability of the injury occurring.

For information that is exempt from ATIA, the injury test is also applied as a mechanism to determine the level of classification or designation required to protect the information [3]. For designated information, the levels PROTECTED A, PROTECTED B, and PROTECTED C correspond to an "injury", "severe injury" or "extremely grave injury" to interests other than the national interest. Information, whose release will not result in an injury to either national or non-national interests, does not require exemption from ATIA and will be UNCLASSIFIED.

In applying the injury test to the distribution of AIS information, the following three use cases are considered:

1. the release of AIS information for a specific vessel results in the breach of personal information of someone onboard;
2. using released AIS information, Canadian authorities recognise misreporting in the AIS messages originating from a particular ship. The authority decides to investigate and take legal action against the ship's owner; and
3. released AIS information for a specific vessel, combined with correlated data such as images of the vessel, results in the breach of the personal information of someone onboard.

The results of each use case are presented in Tables 1 to 3 (Table 3 occurs in Section 2.3). For each use case, the injury test is applied using the template that was provided as part of DRDC's Security of Information (SoI) 101 training [7]. The template is arranged in three columns, with the first column listing the three injury test criteria, the second column listing questions to be answered in applying each test criteria, and the third column containing the analysis of the test criteria for each use case. The first and second columns are directly from the SoI 101 training. All test cases assume that the release of vessel identity and contact information is not occurring in real-time.

Table 1: *Use Case 1: The release of a ship's AIS data results in the breach of the personal privacy of someone onboard.*

Specific Injury	At Risk Organization	Applies to?
a) What is the specific injury?	Identify the specific individual, organization, nation at risk.	The specific injury would apply to a person onboard the vessel who is identified.
	Identify **who** would cause the injury, **what** would they do, **where** and **when** it could take place, **why** they would do it, and **how** it would happen.	- (who) The injury would be caused by a third party. - (what) The third party would know that the vessel was located at a specific location at a specific time. From this information they could infer the location of occupants of the vessel **if** additional information on ownership, passenger list, etc. was available from another source. - (where, when) The third party could do this at any location and time. - (why) The third party would do this because they were interested in a particular person's whereabouts. - (how) This would happen if the third party was able to combine the location of the vessel with ownership information, or information regarding potential occupants of the vessel.
	Identify how the interest will be injured – the **type of compromise**.	The individual's past location could be known, if the individual were on board the vessel.
b) Is the injury current?	Identify how a specific individual, organization, nation has the capability and intent to cause injury **at this time**.	- For the general individual, there is no reason to assume that a third party would have interest in determining their past location. However, specific scenarios in which such an act might occur can be imagined (for example, tracking celebrities; criminal investigations).
c) Is there a chance/ probability that the injury would occur?	Specify how a specific individual, organization, nation has the **capability** and **intent to use the information** to cause injury.	- (capability) AIS information by itself is insufficient to cause injury. Access to additional information linking an individual to the vessel is required. - (intent) see item (b).

Table 2: *Use Case 2: AIS information is released, and using this information a Canadian authority recognizes misreporting in the AIS message from a particular ship. The authority decides to investigate and take legal action against the ship's owner.*

Specific Injury	At Risk Organization	Applies to?
a) What is the specific injury?	Identify the specific individual, organization, nation at risk.	The authority takes legal action against the ship. The specific injury would apply to the ship owner.
Note: The interests (i.e., the parties) identified under ATIA that could potentially be exempt from providing information based on an ATI request, include federal-provincial governments and their affairs, international affairs, law enforcement, public prosecutors, etc. An individual owning a vessel is not an identified interest in the ATIA. Thus the ATIA would offer no exemption to release of the vessel contact data, since the interest (i.e., the owner) is not listed in the ATIA. With no possible exception through the ATIA, we suggest that no release limitation is possible. In this case, the data could be obtained through ATI request.		
	Identify **who** would cause the injury, **what** would they do, **where** and **when** it could take place, **why** they would do it, and **how** it would happen.	- (who) The injury would be caused by a department within government. We speculate it would be Transport Canada, For the remainder of this use case this is referred to as "the regulatory department." - (what) The regulatory department may have the ability to take legal action (e.g., fine) against the owner. - (where, when) Such action would likely only be taken when the vessel was in the Canadian Exclusive Economic Zone (EEZ; 200 nmile limit). - (why) The regulatory department may take action to deter misreporting of data in the AIS message. - (how) Erroneous data would be recognized by the regulatory department. Using the data, the identity of the vessel would be determined. If appropriate laws exist that deal with misreporting, then the vessel owner could be charged.
	Identify how the interest will be injured – the **type of compromise**.	The owner may experience legal costs or fines.
b) Is the injury current?	Identify how a specific individual, organization, nation has the capability and intent to cause harm **at this time**.	We are not aware of regulatory departments currently investigating or prosecuting the misreporting of AIS data. As well, because the data are not being released in real-time, we speculate this would further reduce the likelihood of action.
c) Is there a chance/ /probability that the injury would occur?	Specify how a specific individual, organization, nation has the **capability** and **intent to use the information** to cause injury.	- (capability) Analysis of the data could be conducted by staff at the regulatory department. Any person with intermediate computer skills could determine if there were errors in the AIS message. However, we speculate that the necessary directives, regulations, or legislation, which would permit action by regulatory departments, do not exist. - (intent) We speculate that the department has little intent to conduct such prosecutions because we know of no such prosecutions and we consider enforcement resources to be too limited for such analyses.

The above use cases present several questions that originate in the injury test template. These questions help guide our thinking to the specifics regarding the injury, the involved parties that might be harmed and cause harm, the capabilities and intent of the party that would cause harm and injury, and the currency of the injury. The use cases presented indicate that the release of vessel identity and historic contact information provides insufficient detail to allow the identification of specific parties, intent and injury, **indicating that designation is not necessary**.

2.1.3 Intellectual Property and use protections

Information sensitivities are one aspect to be considered when releasing MDA-related information. Other aspects to be considered include Crown intellectual property (IP) and warranty associated with the data or information that is being released. The Crown protects the copyright and misuse of the supplied data or information by the receiving party via an agreement established between the Crown and the receiving party. For DRDC, the establishment of such an agreement involves DRDC Science and Technology External Relations (DSTER). It suffices for this document to state that DSTER should be involved in any release of data/information to a third party, with the specifics of the data sharing agreement to be established on a case-by-case basis.

2.1.4 Summary for AIS data

To conclude, for AIS data the authors recommend:

1. When delivering a data set to a party outside of government or another Canadian government department:
    a. that DSTER be involved to establish any necessary data sharing agreement between the parties.
    b. that the data supplier (i.e., DRDC staff) consider agreement restrictions related to the use, presentation, and distribution of the data, such as;
        i. data use is restricted to the specific project for which the data is supplied;
        ii. publication/presentation restrictions be project specific;
        iii. distribution to another party not be permitted unless that party is included in the data sharing agreement; and
        iv. delivery to the parties include release restrictions related to data latency. For a recipient outside the Government of Canada, the suggestion is a two week data latency. For release to another Canadian Government department/agency, the latency should be negotiated through DSTER.
    c. that the data set itself be unclassified and undesignated.
2. When a DRDC report includes AIS data:
    a. that vessel identifiers with or without contact data be permitted in the report, with no protection as a result of inclusion of this particular information.

Note that AIS data purchased by the GoC are different from DRDC collected data. Purchased AIS data comes with distribution stipulations. DRDC is governed by those stipulations, and it is not felt to be necessary to add additional stipulations such as the Protected designation.

2.2 ADS-B Data

Many of the concerns raised with regard to the distribution and management of AIS data (i.e., for vessels), and the arguments made to refute those concerns, can be applied to ADS-B (i.e., for aircraft), which like AIS, is another data source that combines contact data with identity.

As with AIS, there may be concerns that for ADS-B data: an identified aircraft could be a Government of Canada aircraft of interest; that DND is collecting ADS-B data; or that ADS-B data may contain private information. The authors would contend that the arguments made in Section 2.1 for AIS would also apply to ADS-B:

- The argument that it is the VOI label being applied to a vessel that is sensitive rather than the vessel data itself would apply equally to aircraft;
- The argument that DND has a mandate to monitor "Canada's territory and air and maritime approaches" clearly applies to aircraft;
- The argument that identifying aircraft information (call-sign or ICAO number) is not information about an identifiable individual and so is not considered private information as defined in the Privacy Act.

While concerns have been raised in the US over the unrestricted real-time release of ADS-B data (see for example [8]), there is no evidence that national authorities, such as Transport Canada, the US FAA, or international bodies, such as ICAO, plan to impose restrictions on the release of ADS-B data that would be comparable to the IMO guidelines on release of AIS data.

It is also noted that the operation of ADS-B in Canadian airspace is currently voluntary [9]. Therefore any concerns regarding the release of ADS-B data would be under the control of aircraft operators.

2.3 Combining contact data and identity from multiple sources

In addition to considering individual information sources, such as AIS or ADS-B, that provide both contact data and identity, the discussion can be extended to include the following two cases:

- Case A: by aggregating information from other sensors, additional contact or identity data can be added to existing combined contact and identity data; or
- Case B: by aggregating information from multiple sensors that individually provide only contact or identity information, a data output that combines contact and identity is produced.

The integration of imagery with AIS or ADS-B, or radar with AIS or ADS-B, are examples of Case A; adding identity data (e.g., imagery, photograph) or contact data (e.g., radar), respectively,

to existing sources of combined contact and identity data (e.g., AIS, ADS-B). The integration of contact data from radar and identity data from imagery (i.e., Case B) is an example of the production of a data output that combines contact and identity from data sources that individually provide only one of contact or identity.

Assuming that all of these individual sensors and sources and the data they produce are unclassified, i.e., they do not merit exclusion under the ATIA or PA, the integration of an additional source of contact or identity data, with an existing source of combined contact and identity data (i.e., Case A), does not appear, in the general case, to introduce new considerations that would require additional protection of the information[4]. As an example, the extension of use case 1, which deals with a breach of personal privacy, to include the combination of released AIS information together with imagery, is considered below in Table 3. Only if the imagery itself contains identifying information about an occupant of the vessel, would the individual's privacy be violated, and in that case the imagery would already require designation.

Rather, having an additional source of contact or identity data will serve to increase the accuracy or the level of confidence in the resulting data product. For example, because AIS and ADS-B are self-reporting systems (i.e., the vessel or aircraft generates the data message), the contact or identity produced by either of these systems is trusted less than the data provided by a non-cooperative sensor, such as radar.

Case B, involving the integration of data from multiple existing sensors that individually provide only contact or identity, to produce an output that combines both contact and identity, and where data from each of the individual sensors is unclassified, does not, at first glance, appear to be fundamentally different from the case involving a single sensor that provides combined contact and identity data. Consider again the use case involving a possible breach of personal privacy. If the combination of data from two sensors provides contact and identity about a particular vessel, but that information does not identify particular individuals, then release of that data product will not result in an injury to the personal privacy of individuals onboard the vessel.

However, there are specific circumstances where data types that are unclassified when considered independently require designation or classification when combined. Consider, for example, contact data from an unclassified radar. For general non-military vessel types, the radar data, when linked to an unclassified source of identity data, such as an image, will result in an unclassified data product. However, if the vessel was a Canadian military vessel, real-time release of combined contact and identity data would require classification. Other specific circumstances, involving novel and/or unique sensors, methods for information combination, or the circumstances of data collection, might require either designation or classification. It is therefore the authors' opinion that the aggregation of data from multiple sensors that individually provide only contact or identity (i.e., Case B) will have to be examined more carefully than the case where contact or identity information is added to existing combined contact and identity data (i.e., Case A).

[4] It is possible that special cases may exist in which the aggregated information requires additional protection beyond that accorded to the individual sensors or information sources.

Table 3: *Use Case 3: AIS data is released and is combined with third-party imagery of the vessel (Note: this is the more general case of DRDC releasing imagery of the vessel). The combined data results in the breach of the personal privacy of someone onboard.*

Specific Injury	At Risk Organization	Applies to?
a) What is the specific injury?	Identify the specific individual, organization, nation at risk.	The specific injury would apply to a person onboard the vessel who is identified.
	Identify **who** would cause the injury, **what** would they do, **where** and **when** it could take place, **why** they would do it, and **how** it would happen.	- (who) The injury would be caused by a third party. - (what) The third party would know that the vessel was located at a specific location at a specific time. From this information they could infer the location of occupants of the vessel **if** the imagery revealed the vessel's occupants **or if** additional information on ownership, passenger list, etc. was available from another source. - (where, when) The third party could do this at any location and time. - (why) The third party would do this because they were interested in a particular person's whereabouts. - (how) This would happen if the third party was able to combine the location of the vessel with ownership information, or information regarding potential occupants of the vessel.
	Identify how the interest will be injured – the **type of compromise**.	The individual's past location could be known, if the individual were on board the vessel.
b) Is the injury current?	Identify how a specific individual, organization, nation has the capability and intent to cause harm **at this time**.	- For the general individual, there is no reason to assume that a third party would have interest in determining their past location. However, specific scenarios in which such an act might occur can be imagined (for example, tracking celebrities; criminal investigations)
c) Is there a chance/ probability that the injury would occur?	Specify how a specific individual, organization, nation has the **capability** and **intent to use the information** to cause injury.	- (capability) AIS information by itself is insufficient to cause injury. If imagery was able to identify an individual on the vessel, that imagery would be Protected. Otherwise access to additional information linking an individual to the vessel is required.

3 Northern Watch: A case study for combining contact and identity data

In the following section an example application is provided. The ideas presented previously are applied to various DRDC-collected data sets, to determine the resulting classification. The results act as an evaluation of the previous ideas. Data collected as part of the Northern Watch (NW) Project is used in the example.

The Northern Watch (NW) Project is developing and demonstrating a capability to conduct unattended, persistent, local-area surveillance of an Arctic chokepoint, across Barrow Strait on the Northwest Passage, in the vicinity of Gascoyne Inlet, Devon Island, Nunavut. The capability being developed consists of a remote controlled and monitored, unattended Arctic Surveillance Demonstration System (ASDS), to be deployed at Gascoyne Inlet and operated over a commercial satellite communication channel from a Defence Research & Development Canada (DRDC) Southern Control Centre (DSCC) at DRDC Atlantic, in Halifax, Nova Scotia. Based on the original concept for the Northern Watch system [10], a surveillance data output is produced from the integration of data from multiple above-water and underwater sensors and self-reporting systems, including:

- Rutter navigation radar;
- Automated Identification System (AIS);
- Automated Dependent Surveillance–Broadcast (ADS-B);
- Underwater Surveillance System (UWSS), developed by Omnitech for DRDC Atlantic;
- AWAIR (Advanced Wideband Adaptive Intrapulse Receiver) radar intercept system, developed by DRDC Ottawa;
- CANDISS (Canadian Night and Day Imaging Surveillance System) EO/IR system, developed by Obzerv for DRDC – Valcartier Research Centre; and
- a meteorological system.

Following a re-scoping in April 2013, the AWAIR and CANDISS systems were removed as sensors from the project.

In common with the discussion presented in Section 2, the assessment of the sensitivity of NW data, and its appropriate level of classification, must take into account the issues related to the linking of contact location and identity. Data produced by three of the systems—AIS, ADS-B, and CANDISS—can individually link contact location and identity. In addition, the process of integrating information from multiple sensors, may result in either of the two cases considered in Section 2.3: the aggregation of contact or identity information with existing sensor data that combines both contact and identity data; or, the aggregation of data from multiple sensors that individually provide either contact or identity to produce a combined contact and identity data output.

Based on the conclusions of Section 2 and, where necessary, additional sensor-specific considerations, this section first examines the sensitivity of data output by individual NW sensors, with focus on the production of data outputs that combine contact and identity. Specific examples of the integration of information from multiple NW sensors are then considered in Section 3.7.

3.1 AIS

As described in [10], the Northern Watch surveillance system processes position reports and static data reports from Class A and Class B AIS. Consistent with the findings of Section 2.1, these reports, which combine contact and identity data, are considered to be unclassified.

3.2 ADS-B

As described in [10], the Northern Watch surveillance system processes extended squitter reports from ADS-B. Consistent with the findings of Section 2.2, these reports, which combine contact and identity data, are considered to be unclassified.

3.3 Navigation radar

The Rutter radar used by Northern Watch is a commercial X-band navigation radar. As described in [10], the Northern Watch surveillance system processes radar track reports. These include a track number, measurement time, and range and bearing, and as such, constitute contact data. Radar track reports from a commercial navigation radar, considered independently of other data, are unclassified.

3.4 CANDISS (Canadian Night and Day Imaging Surveillance System) EO/IR system

The CANDISS electro-optical/infrared (EO/IR) system [11] is an unclassified system that contains multiple sensors including: narrow field-of-view and wide field-of-view optical cameras; infrared camera; narrow field-of-view active laser imager; laser rangefinder; GPS receiver; and an AIS receiver. As such, CANDISS, independent of other sensors, can provide all of the following combinations of contact and identity data:

1. contact data: time-tagged bearing, from the camera pointing angle, and range, from the laser rangefinder, geo-referenced to the CANDISS system's location;
2. identity data: optical or infrared imagery;
3. combined contact and identity data: from AIS;
4. contact or identity data added to existing combined contact and identity data: AIS with added contact data (camera pointing angle or laser rangefinder) and/or added identity data (optical or infrared imagery); and
5. combined contact and identity data produced from the integration of multiple sensors that provide contact or identity data: contact data (camera pointing angle or laser rangefinder) integrated with identity data (optical or infrared imagery).

Based on the discussion in Section 2, in most cases the contact and/or identity data produced by CANDISS will not require designation or classification. However, special cases do exist. First, for images of vessels taken at sufficiently close range, it is possible that the imagery might include identifiable persons. If combined with contact data[5], it can be argued that such images would contain personal information that requires protection. Alternatively, information identifying persons (for example, faces) could be removed from images. A second case, presented in Section 2.3, involving the real-time release of combined contact and identity data for a Canadian Navy ship, would apply to the combination of contact data (from camera pointing angle and laser rangefinder) and identity data (from imagery) produced by CANDISS.

3.5 AWAIR (Advanced Wideband Adaptive Intrapulse Receiver) Radar Intercept system

For its use within the Northern Watch project, the AWAIR radar intercept system was modified to produce detection, bearings-only tracking and classification data for maritime surface and air platforms, based on detected RF emissions from navigation radars operating in the X and S bands. As described in [10], AWAIR would produce contact data, in the form of time-stamped bearing reports, and radar parameter and classification data. The parameter and classification data produced by AWAIR for Northern Watch do not constitute identity data per se, as they were limited to providing at most a broad classification of ship type.

At the time the System Concept for Northern Watch was developed [10], bearing data from AWAIR, independent of data from other sensors, was considered to be unclassified. This is consistent with the analysis presented in Section 2, given that AWAIR produces contact data which is not combined with identity data. Radar parameter and classification data was also considered to be unclassified, in part because it was limited to navigation radars and also because classification was based on an open source database of navigation radar emitter parameters.

3.6 Under Water Surveillance system (UWSS)

The Northern Watch Underwater Surveillance System consists of two bottom-mounted underwater acoustic arrays and the UWSS Processing and Display System (PDS), a back-end acoustic signal and data processing system that is a variant of DRDC Atlantic's MAPS system. As described in [10], the primary outputs of the UWSS are acoustic bearing reports, for objects detected on either of the acoustic arrays, acoustic cross-fix reports, for objects detected simultaneously on both arrays, and acoustic spectrogram data. Acoustic bearing or cross-fix reports constitute contact data, which is unclassified if considered independently from acoustic spectrogram data or from other sensors.

According to the Maritime Acoustic Security Policy [12], acoustic data will vary in classification level depending on factors such as the type of detected object and the level of analysis performed on the collected data. For example, annotated acoustic signatures of military vessels or vessels of interest are generally classified; otherwise, acoustic signature data is unclassified. Therefore the

[5] Even without the specific contact data described in item 1, imagery, if tagged with meta-data, such as time and camera location, will provide a rough estimate of object location, which constitutes a form of combined contact and identity data.

acoustic spectrogram data produced by the Northern Watch UWSS may be classified in some circumstances. Acoustic spectrogram data, if subjected to a process of acoustic analysis, may result in the production of identity data[6]. However, strictly speaking, the Northern Watch UWSS does not produce identity data because acoustic analysis will occur outside the Northern Watch system.

3.7 Northern Watch Surveillance System

As described in [10], the Northern Watch surveillance system will output surveillance information products produced from the correlated data from all reporting sensors and information sources. The sensitivity of the data output by individual Northern Watch sensors has been considered in Sections 3.1 to 3.6. This section examines additional issues arising from the combination of data from multiple sensors and self-reporting systems.

The combination of sensor data input to the Northern Watch surveillance system will be dependent on the types of objects within the system's surveillance coverage region. Object types that are likely to be encountered in a local-area Arctic surveillance scenario fall into one of the following categories:

- Cooperative surface: commercial vessels that are required to broadcast AIS based on national or international regulations, based on factors such as tonnage, type of voyage, number of passengers, ship type and ship age;
- Non-cooperative surface: vessels that are not required to broadcast AIS. This includes smaller yachts, adventure sailors, and smaller research and exploration vessels. Many of these vessels can be expected to operate AIS in Arctic waters for safety reasons. Military and vessels on government non-commercial service (for example, Coast Guard), while exempt from AIS carriage requirements, can also be expected to operate AIS unless there is an operational reason to remain covert;
- Trans-polar air: commercial jet aircraft on trans-polar routes broadcasting ADS-B;
- Local air: small single-engine aircraft; helicopters; or
- Sub-surface: submarines; unmanned underwater vehicles; towed sources.

For each of the above categories of object, Table 4 summarizes, for each Northern Watch sensor, whether contact or identity data will be generated. Signature data from AWAIR and UWSS is not included in this summary and it is assumed, for the purposes of this discussion, that signature data is not included as part of the surveillance data product.

Using AIS, cooperative vessels will generate a data output consisting of an unclassified combined contact and identity data. As discussed in Section 2.3, because of the cooperative nature of the AIS data, its combination with additional unclassified sources of contact or identity data (see Table 4, Cooperative surface column) is unlikely to create a product which requires designation or classification.

[6] Depending on the uniqueness of the acoustic signature, acoustic analysis may result in classification or identity data.

The detection of non-cooperative vessels may result in combined contact and identity data, created from one or more sources of contact data (radar, AWAIR, CANDISS, or UWSS) and from identity data that originates from CANDISS. As discussed previously, for particular vessel types, such as a Canadian military vessel, this case may generate a classified output. Note that cooperative vessels, if no AIS broadcast is received, would also fall into this category.

Using ADS-B, cooperative commercial aircraft produce unclassified combined contact and identity data, as discussed in Section 2.2.

Finally, local aircraft and sub-surface objects are detected by sensors that produce contact data, with no identity, which is unclassified.

In conclusion, the possible combinations of object types expected in local-area Arctic surveillance, and sensor data types processed by the Northern Watch surveillance system, provides a rich set of examples, which cover the range of previously examined scenarios for aggregating contact and identity data. These examples support the analysis of combined contact and identity data that was presented in Section 2.

Table 4: *Contact and identity data produced by Northern Watch sensors as a function of object type.*

Sensor\Object	Cooperative surface	Non-cooperative surface	Cooperative commercial air	Local air	Sub-surface
AIS	C, I	-	-	-	-
ADS-B	-	-	C, I	-	-
Radar	C	C	-	C	-
CANDISS	C, I	C, I	-	-	-
AWAIR	C	C	-	C	-
UWSS	C	C	-	C	C

C= contact data; I = identity data

4 Conclusion

This report provides guidance on the release of data pertinent to MDA. The guidelines presented will provide clarity and consistency regarding the classification/designation of a maritime data set and because of this, will shorten delivery time of such data sets to partners and collaborators.

As a summary, the report has concluded that when releasing DRDC-collected non real-time AIS or ADS-B data, staff should:

- consider the data to be unclassified and undesignated;
- involve DRDC Science and Technology External Relations to establish any necessary data sharing agreement; and
- consider data use, publication, and presentation restrictions in the agreement.

As well, for a report (i.e., a document) containing AIS or ADS-B data, that vessel identifiers with or without contact data be permitted in the report, with no protection as a result of inclusion of this particular information.

In addition to individual information sources that provide both contact data and identity, the report also considers the aggregation of contact and identity data from multiple sources. It is the authors' opinion that the aggregation of data from multiple sensors that individually provide only unclassified contact or identity must be examined carefully, as there may be specific circumstances which require the designation or classification of the data output.

For the Northern Watch data set, the conclusions are complicated by the diversity of the data types. The reader is referred to the individual sections in Section 3.

This page intentionally left blank.

References

[1] Transport Canada Maritime Domain Awareness (online), https://www.tc.gc.ca/eng/marinesecurity/initiatives-235.htm (Access date: 05 May 2015).

[2] IMO (2004), Report of the Maritime Safety Committee on its Seventy-Ninth Session, (MSC 79/23) International Maritime Organization.

[3] Government of Canada (2002), National Defence Security Instructions (NDSI), Chapter 27.

[4] Government of Canada (2008), Canada First Defence Strategy.

[5] Government of Canada (1980), Privacy Act, (1980-81-82-83, c. 111, Sch. II "1").

[6] Government of Canada (1985), Access to Information Act, (R.S.C., 1985, c. A-1).

[7] Edwards, K. (2014), Security of Information (SoI), 74.

[8] George, F. (2014) "ADS-B Mandate Could Dismantle BARR," Aviation Week, http://aviationweek.com/awin-only/ads-b-mandate-could-dismantle-barr (Access date: 06 May 2015).

[9] Government of Canada (2011), Automatic Dependent Surveillance – Broadcast, Transport Canada Advisory Circular 0700-009, Issue No. 2.

[10] McArthur, B. (2012), "Northern Watch System Concept," DRDC Atlantic TM 2012-119.

[11] Forand, J.L., Larochelle, V., and G. Tardif (2008), "Canadian Night and Day Imaging Surveillance System (CANDISS)," DRDC Valcartier TN 2008-066.

[12] Government of Canada (2011), Maritime Acoustic Security Policy, MARCORD 4-14 (draft).

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

ADS-B	Automatic Dependent Surveillance - Broadcast
AIS	Automatic Identification System
AMAR	Advanced Multi-Channel Acoustic Recorder
ASDS	Arctic Surveillance Demonstration System
ATIA	Access To Information Act
AWAIR	Advanced Wideband Adaptive Intrapulse Receiver
CANDISS	Canadian Night and Day Imaging Surveillance System
CSEC	Communications Security Establishment Canada
DFO	Department of Fisheries and Oceans
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DSCC	DRDC Southern Control Centre
DSTER	DRDC Science and Technology External Relations
EEZ	Exclusive Economic Zone
EO	Electro-Optical
GoC	Government of Canada
ICAO	International Civil Aviation Organization
IMO	International Maritime Organisation
IR	Infrared
MDA	Maritime Domain Awareness
MIKM	Maritime Information and Knowledge Management
MMSI	Maritime Mobile Service Identity
NW	Northern Watch
PA	Protected A
RCMP	Royal Canadian Mounted Police
SoI	Security of Information
UWSS	Underwater Sensor System
VOI	Vessel Of Interest

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

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 report, or tasking agency, are entered in Section 8.)

DRDC – Atlantic Research Centre
Defence Research and Development Canada
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Assessing the information content of Maritime Domain Awareness data: Applications to classification guidance

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

McArthur, B.; Isenor, A.W.

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

October 2015

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

32

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

12

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

Scientific Report

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

DRDC – Atlantic Research Centre
Defence Research and Development Canada
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7
Canada

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

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-RDDC-2015-R207

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

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

Public release

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

Public release

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.)

The development of Maritime Domain Awareness (MDA) is a multi-faceted and multi-departmental activity within the Canadian Government. In the development of MDA, many data and information sources are brought together or aggregated to help formulate an awareness of vessel activity in and approaching Canadian waters. DND research and development focused on MDA often encounters the issue of data/information distribution to partners or collaborators. In an effort to establish a common understanding of data distribution to partners or collaborators, this report uses several data distribution use cases, combined with an examination of existing security guidelines, to formulate conclusions regarding the distribution of MDA-relevant data/information to partners both internal and external to government. One important conclusion is that distribution of non-real-time Automatic Identification System (AIS) data should not be designated. This work provides the guidance necessary for future data/information distribution especially with external organizations such as academia.

Le développement de la connaissance du domaine maritime est un exercice à volets multiples qui touche plusieurs ministères au sein du gouvernement du Canada. Pour développer la connaissance du domaine maritime, on regroupe de nombreuses sources de données et de renseignements pour permettre l'élaboration d'une connaissance des activités des navires naviguant dans les eaux canadiennes ou qui s'en approchent. Les efforts de recherche et développement du MDN qui se concentrent sur la connaissance du domaine maritime se heurtent souvent au problème de la distribution des données et des renseignements aux partenaires ou collaborateurs. Afin d'établir une compréhension commune de la distribution des données à ces partenaires et collaborateurs, le présent rapport utilise divers cas de distribution des données, combinés à un examen des lignes directrices existantes en matière de sécurité, pour formuler des conclusions relatives à la distribution de données et de renseignements pertinents à la connaissance du domaine maritime aux partenaires à l'intérieur et à l'extérieur du gouvernement. Une conclusion importante établit que la distribution des données du Système d'identification automatique (SIA) en temps non réel ne devrait pas être désignée. Cet ouvrage fournit l'aide nécessaire pour procéder à une distribution future de données et de renseignements orientée surtout vers les organisations externes, comme le milieu universitaire.

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.)

maritime domain awareness; data distribution; aggregation