SMARTracIn -- A concept for spoof resistant tracking of vessels and detection of adverse intentions

Sten F. Andler*[a], Mikael Fredin[b], Per M. Gustavsson[c], Joeri van Laere[a], Maria Nilsson[a], Pontus Svenson*[d]

[a]University of Skövde, Box 408, SE-54128 Skövde, Sweden; [b]Saab Microwave Systems, Storgatan 20, SE 54130, Skövde, Sweden; [c]George Mason University, 22030, Fairfax, VA, U.S.A.; [d]Swedish Defence Research Agency, SE 164 90 Stockholm, Sweden

ABSTRACT

The aim of maritime surveillance systems is to detect threats early enough to take appropriate actions. We present the results of a study on maritime domain awareness performed during the fall of 2008. We analyze an identified capability gap of worldwide surveillance in the maritime domain, and report from a user workshop addressing the identified gap. We describe a SMARTracIn concept system that integrates information from surveillance systems with background knowledge on normal conditions to help users detect and visualize anomalies in vessel traffic. Land-based systems that cover the coastal waters as well as airborne, space-borne and ships covering open sea are considered. Sensor data are combined with intelligence information from ship reporting systems and databases. We describe how information fusion, anomaly detection and semantic technology can be used to help users achieve more detailed maritime domain awareness. Human operators are a vital part of this system and should be active components in the fusion process. We focus on the problem of detecting anomalous behavior in ocean-going traffic, and a room and door segmentation concept to achieve this. This requires the ability to identify vessels that enter into areas covered by sensors as well as the use of information management systems that allow us to quickly find all relevant information.

Keywords: Maritime domain awareness, tracking, information fusion, early warning

1. INTRODUCTION

We present the results of a study on maritime domain awareness (MDA) financed by the Swedish Emergency Management Agency (as of 1 Jan 2009 subsumed by MSB, the Swedish Civil Contingencies Agency) during the fall of 2008. The purpose of the study was to investigate how information-fusion and anomaly-detection methods can be used to facilitate worldwide surveillance of maritime activities. The specific goal of the project was to determine how to reduce one of the technology gaps identified at a Nordic Vigilance workshop carried out in Sweden during the spring of 2008. The detailed contents of this capability gap are summarized in section 6 below.

The findings of the study can be summarized as follows: Today's surveillance systems and data sharing initiatives within the maritime domain offer an opportunity to collect huge amounts of data on vessels worldwide; This opportunity doesn't necessarily mean that all data are, in fact, available, permitted or true; There is a need to develop intelligent data processing functionality that highlights unusual behaviors and inconsistencies in the large dataset; Interesting events or threats are often camouflaged and hidden in regular traffic patterns, which means that available data mostly appears quite uneventful to the user; To remedy this, we need to increase the level of automation at higher fusion levels, which aims to support operators with limited resources by giving them early warnings about worldwide approaching threats.

In order to reach the goal of early warnings (alerts) of worldwide approaching threats, it is necessary to exploit as much available information as possible. Data sharing in this context means that all forms of available data is combined – not only radar and AIS data but also data from registers and information databases regarding vessels, harbors, crews, etc. We will refer to these other sources of information as *intelligence sources*.

* sten.f.andler@his.se
* ponsve@foi.se

Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense VIII, edited by Edward M. Carapezza, Proc. of SPIE Vol. 7305, 73050G · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.818567

We introduce the concept system SMARTracIn – Surveillance of Maritime Activities by Robust Tracking of Information – with an aim to track vessels worldwide using *all available information* – or smart tracking of information. By including information from ship and crew records, cargo details, records of ship ownership and details about the activities of ship-owners as well as intelligence reports about the ships, it is possible to track all existing information about the vessel rather than just its geographical position. This enables information-fusion and anomaly-detection methods to discover more threats, at an earlier time, than a purely position-driven approach. Today's MDA systems often focus on detecting threats in coastal regions [1]. SMARTracIn, in contrast, explicitly aims at allowing users to follow vessels ocean-wide, and to detect suspect behaviors globally. While this makes the project more challenging scientifically and technically, it also allows for a larger increase in user effectiveness than focusing merely on coastal regions.

This paper is outlined as follows. In section 2, we describe the gap and the analysis undertaken in our project to further describe it, as well as some previous approaches to anomaly detection for MDA. Section 3 reports on the stakeholder workshop performed by us, while section 4 describes our concept solution (SMARTracIn) and section 5 present a system architecture for the solution. The paper ends with a summary and some suggestions for future work in section 6.

2. CAPABILITY GAP IN WORLDWIDE TRACKING OF VESSELS

The Swedish Emergency Management Agency (as of 1 Jan 2009 subsumed by MSB, the Swedish Civil Contingencies Agency) and the U.S. Department of Homeland Security (DHS) have identified a number of capability gaps related to Maritime Domain Awareness (MDA). The pre-study reported in this paper addressed one of the identified capability gaps, namely M-2, described as [7]:

The problem is to ***track vessels*** *in order to* ***detect anomalies*** *using* ***available information*** *from* ***information-, transponders- and sensor systems****. Coverage from radar, cutters and aircraft is limited in area and time coverage and does not fill the gap of information. Transponder systems such as AIS demands co-operative systems onboard vessels. Any* ***hampering or spoofing makes such systems unreliable****.*

Therefore, a support to the operational pictures and analysts ashore for a more efficient capability to detect, track and identify the intention of adverse activities worldwide in near-real time is needed for the planning of appropriate action.

The desired outcome of addressing M-2 is: Continuous awareness of identity, location, behavior of all vessels.

In order to define more exactly what the gap description of MSB involves, two main activities were performed in the preliminary research study executed in autumn 2008. These were a literature/document study of previous research and engineering activities related to worldwide Maritime Domain Awareness and a brainstorming workshop with 16 key stakeholders (described in section 3).

Technology of today does not allow continuous tracking of all vessels at sea. Cooperative methods for detection and identification such as AIS[1], and LRIT[2], are restricted to vessels of a certain size, and non-cooperative methods such as radar are mainly limited to coastal areas. Furthermore, even though the dynamic behavior of vessels captured by sensors is known worldwide it would not be enough to identify adverse intensions in general, since the threats often are associated with cargo details, crew records and port history logs etcetera.

No single system or sensor has a complete view of all vessels within a certain area and within a certain time frame – there are no super sensors that provide us with all necessary information. This unavoidable fact motivates the numerous maritime data sharing initiatives that have appeared lately, e.g. MSSIS [6] and the Europe-wide sharing of vessel traffic

1 Automatic identification system

2 Long-range identification and tracking

data under SafeSeaNet[3]. However, the existence of huge amounts of data collected on vessels worldwide does not necessarily imply that all data are available, allowed or true.

Moreover, just having a huge amount of data does not make the identification of anomalies or early warnings self evident. There are no standard information fusion techniques for modeling data from multiple heterogeneous sensors and data bases and fuse it. There is thus a need to develop such models and methods, as well as intelligent data processing functionality that highlights unusual behaviors and inconsistencies in large data sets. Today, most interesting events or threats are to a large extent camouflaged and hidden in the regular traffic, and on the surface the data is mostly quite uneventful to the user. Using information fusion and combining sensor data with intelligence records will enable the creation of computer systems that help the user detect more such hidden threats.

3. WORKSHOP ON EARLY WARNINGS (BASED ON ANOMALIES)

In order to align the SMARTracIn work according to real user needs, a workshop was performed. The focus of the workshop was "What early warnings do we need in the future?" Participants from different stakeholders such as the Swedish Armed Forces, Swedish Coast Guard, Department of Fisheries Control, Port of Gothenburg Swedish Customs, Lloyds and Swedish Emergency Management Agency were present at the workshop, as well as several researchers involved in SMARTracIn. In total, the workshop had about 25 participants, some 10 of which came from the Swedish Armed Forces.

The goal of the workshop was to collect user requirements regarding what anomalies are of most interest. During the workshop 75 early warnings were identified. A vote aimed at selecting the most interesting ones resulted in identification of 31 early warnings. These 31 early warnings (see. Figure 1) were discussed in more detail regarding the following questions:

- What information is needed to detect this early warning?
- Where can that information be found (sources, systems, organizations)?
- How can one tamper with this information, and how can that be prevented?
- How can this information be fused (methods/algorithms)?
- What is the added value of fusing compared to the existing situation?

[3] A European platform for exchange of maritime data. See http://ec.europa.eu/idabc/en/document/2282/5637 for information.

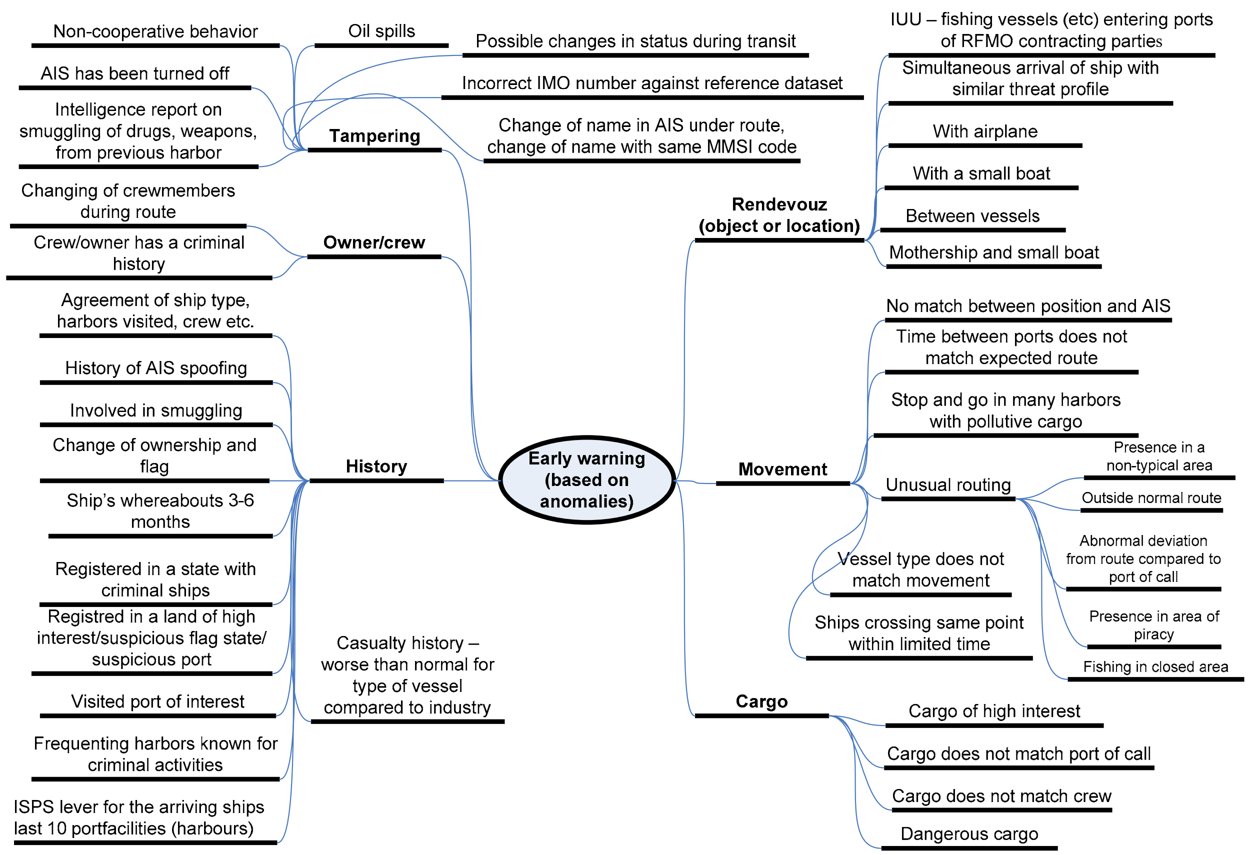

Figure 1. Classification of anomalies as they were produced during the workshop on early warnings. Note, for example, the high interest in ownership and flag history of the vessel.

Over 200 comments were collected in the in-depth discussion. Many of the early warnings identified in the workshop combine information regarding radar and AIS information. In follow-up discussions after the workshop, this was identified as a possible "defense-biased" conclusion of the workshop, caused by the large number of participants from the Swedish Armed Forces. According to non-defense participants, such as the Swedish Customs, the Port of Göteborg and the Swedish Coast Guard, there is also much information gathered in various databases kept by them and by other organizations such as the Swedish Maritime Administration, the Swedish Board of Fisheries etc. Fusion of these kinds of data is a challenge, since most information gathered in the databases does not regard movements and position. Also, it was emphasized that these warnings should cover vessels that enter as well as leave Swedish water. See Figure 1 for a classification of anomalies identified during the workshop on early warnings.

After the workshop, a technical review has been carried out by government, university, and research institute representatives to ensure the relevance of the outcome of the workshop for potential U.S. partners. A conclusion from the review session is that the U.S. and Sweden stakeholders and potential partners have very similar interests in the area of maritime domain awareness.

4. SMARTRACIN – ROBUST TRACKING OF INFORMATION

The ultimate objective of SMARTracIn is to provide users, like ports, the navy, or the coast guard, with early warning of worldwide approaching threats, like smuggling or terrorism. The main focus of this project will be to develop methods (e.g. fusion algorithms) that will derive such early warnings by combining various kinds of information from many different sources, such as data bases, responder and sensor systems (AIS, LRIT, intelligence reports, registers/databases of vessels, harbors, and crews). Such early identification and monitoring of vessels of interest (VOI), or on a more detailed level, cargo or persons, may enable public, private and defense organizations to plan response operations (for example, interception of VOI in coastal waters or inspection of VOI in port).

The goal of SMARTracIn is to demonstrate that it is possible to achieve better maritime domain awareness by fusing information from both sensors and intelligence records and using this information in advanced anomaly detection methods to create early warnings that will alert operators and decision-makers to possible threats and suspect vessels.

Since we will, at least for the foreseeable future, will not have continuous sensor coverage over all oceans, it will never be possible to track vessels using only position data. Instead, we will have partial positional tracklets from different areas ("rooms") of sensor and transponder coverage. In our proposed fusion architecture, these tracklets will be associated with each other and fused with information from other sources, such as crew and ship history records, cargo details, and ownership records. We will also fuse with open source information from, e.g., newspapers, web sites, and blogs devoted to maritime traffic.

By exploiting *all* available information, it will be possible to track smarter (track information rather than sequences of positions) and provide users with more detailed and earlier warnings about vessels of interest.

This early detection of vessels of interest (VOI) will enable operators to plan response operations, e.g., to intercept VOI in coastal water or inspect VOI in port. It will also be possible to send platforms with better sensors to inspect VOI without boarding (e.g., if the early warning is about terrorist activities, we can send sensors that detect explosives aboard the ship).

An added bonus of fusing information from various sources is that it enables us to get tamper and spoof resistant early warnings: by exploiting the heterogeneous information available and not relying only on one kind of sensor, it will be possible to detect some deception attempts.

No single system or sensor has a complete overview of all vessels within a certain area, but MDA can be improved by:

- Combining the information gathered from different surveillance systems in use by different authorities with information from intelligence records
- With a heterogeneous set of sensors, using different physics to sense:
  - fewer vessels will be missed, independent on its cooperation or not
  - more attributes can be collected on individuals
- Different sensor systems cover different areas around the globe
  - enabling the long term behavior to be studied

The increase in situation awareness of operators in the maritime domain that is the goal of SMARTracIn will be achieved by integrating the information from all sources, enabling operators to quickly get all relevant information about a vessel or area that they are interested in and then fusing the information gathered in the information management system to enable anomaly detection at all fusion levels. This will help decision makers focus more on threat analysis than normal situations, thus facilitating enhanced situation awareness in the maritime domain.

To enable situation awareness in the maritime surveillance, operators must be supported in detecting anomalous behaviors. There are factors that speak in favor of attempting to automate the detection of activities and not to depend solely on operators to observe a situation manually. Operators have limited cognitive ability and this makes it hard to be observant of small changes in a situation. The second factor is that different people tend to understand situations differently, which leads to different views on situation awareness, e.g., they notice issues differently from each other. This means that just a data driven approach is not sufficient by itself: it needs to be complemented with a knowledge driven approach, where knowledge from Subject Matter Experts (SME), results from previous observations and the kind of threats that are needed to be detected in a certain area of interest are used.

In order to reach the goals outlined above, it is necessary to perform research in modeling and fusing of heterogeneous information, anomaly detection at different fusion levels (e.g., object as well as situation), information management systems, and develop an architecture suitable for distributed fusion of the heterogeneous information sources.

The distributed fusion architecture should use geo-fencing concepts (similar to the economic or territorial zones), where the oceans are divided into rooms with doors between them, and where we assume to have differing degrees of sensor coverage in different rooms. The SMARTracIn project will perform user studies in order to ensure that the developed methods are useworthy. Further investigations of what information sources are available now and in the near-future must be performed and the results incorporated into the system. Different approaches for modeling the heterogeneous information (such as using random sets) must be investigated.

In order to identify vessels that enter into areas covered by sensors, it is necessary to store information about previously seen vessels as well as about normal or expected traffic. Whenever a new object is seen, relevant information about it (e.g., its home port, known motion patterns etc) must be extracted from a database of background knowledge. By making use of semantic technology [5] for such information extraction, it is possible to formulate general information needs that could be used even if very little information is known about the new object. For instance, if a new vessel appears whose identity cannot be determined or where the database lacks specific information about it, information regarding the movement patterns of vessels of similar size and other characteristics could be extracted from the database and used as input to the anomaly detection algorithms.

SMARTracIn will develop information fusion and anomaly detection methods and algorithms that use these heterogeneous information sources to reduce the ability of vessels with harmful intent to spoof or tamper with the fused worldwide tracking information. Information management methods that enable both operators and computer algorithms to quickly find the information that is relevant to them will be developed.

User experiments will be performed to test the systems developed by SMARTracIn. This requires a prototype that can be used in demonstrations and user tests. The results of experiments with this prototype will influence the final versions of all algorithms and systems developed. At the end of the SMARTracIn project, a final concept demonstrator will be developed and tested. This concept demonstrator will also be used to evaluate the project.

The identified gap related to worldwide tracking of vessels can be addressed by expanding the traditional tracking concept: smart tracking of information rather than using only sequences of positions High-level fused tracking uses aggregated information collected from sources of varying types distributed all over the world. The high-level fused tracking concept uses highly heterogeneous data, in several senses:

- Sensor data as well as intelligence data.
- Dynamic as well as static and voyage related data
- Current and historic as well as future (predicted) data.

In this sense we track information rather than sequences of positions. The high-level fused tracking concept requires methods for modeling heterogeneous information and advanced algorithms that fuse it. Developing such methods and an architecture that allows distributed fusion and anomaly detection at all levels will be a significant scientific contribution of the SMARTracIn project.

The identified gap related to tamper and spoof resistant tracking can be addressed by using information fusion techniques and by doing anomaly detection at all fusion levels .The are many advantages to fusing heterogeneous information. By using overlapping sensor data fewer vessels will be missed, independent of their cooperation or not and more complete information can be collected on individuals which enables more complex threats to be detected. Using different sensor systems covering different areas around the world and other sources of local information enables the long term behavior of vessels to be studied.

Developing intelligent data processing functionality such as anomaly detection increases the level of automation at higher fusion levels, which aims to support operators with limited resources by providing early warning of worldwide approaching threats.

Maritime domain awareness has been a focus of research for some time. However, most of the work has been related to coastal surveillance rather than the ocean-wide perspective advocated by us. Some interesting work is presented in [3], which describes a system where a human operator fuses tracks that refer to the same object. Another paper which also deals with coastal surveillance is [8], which describes a framework for distributed fusion for coastal surveillance. A very interesting paper that describes a concept system for fusing AIS data with radar data is [2]. It would be very interesting to combine the approach suggested in that paper to also include intelligence data such as in this paper.

5. SMARTRACIN – SYSTEM ARCHITECTURE

Figure 2 shows the system architecture, involving Information Fusion and Anomaly Detection using the Common Information Set. Information Fusion and Anomaly Detection processes are performed at several levels of abstraction (according to the JDL model [4]) as well as geographically distributed, and interact with various existing systems at information suppliers and end users.

The focus should be on providing information about generalized tracks. These tracks, which contain more information than just sequences of positions, can be described as:

- The track for a specific vessel contains aggregated information collected from sources of varying types distributed all over the world, including both sensors and intelligence records (e.g., crew and cargo details, ownership history)
- The track consists of dynamic, static and voyage related attributes
- The tracks are heterogeneous
    - the sample rates for specific attributes varies locally
    - the sample rates for different attributes differs by many orders of magnitudes
    - the number of attributes associated with a specific track depends on the availability of data which varies locally
    - the resolution and accuracy for specific attributes varies locally
    - the number of attributes depends on the vessel type

There is a need for the anomalies detected by the system to be displayed to decision-makers at different levels as well as to the analysts actually performing the anomaly detection. A related challenge is to develop algorithms and methods for detecting the anomalous behaviors. Before this can be done, the system needs to align the data in space and time, a non-trivial problem in itself, and establish the quality of the available data.

The potentially very large amount of information available to a monitoring node needs to be automatically filtered and sorted for efficient usage. To this end, metadata and semantic tags aligned with the shared ontology can be exploited to query available sources for relevant information. Semantic technologies could be useful here. An important research challenge is how to automatically generate the correct semantic queries that would give the anomaly detection system the information it needs to distinguish normal traffic patterns from the interesting patterns.

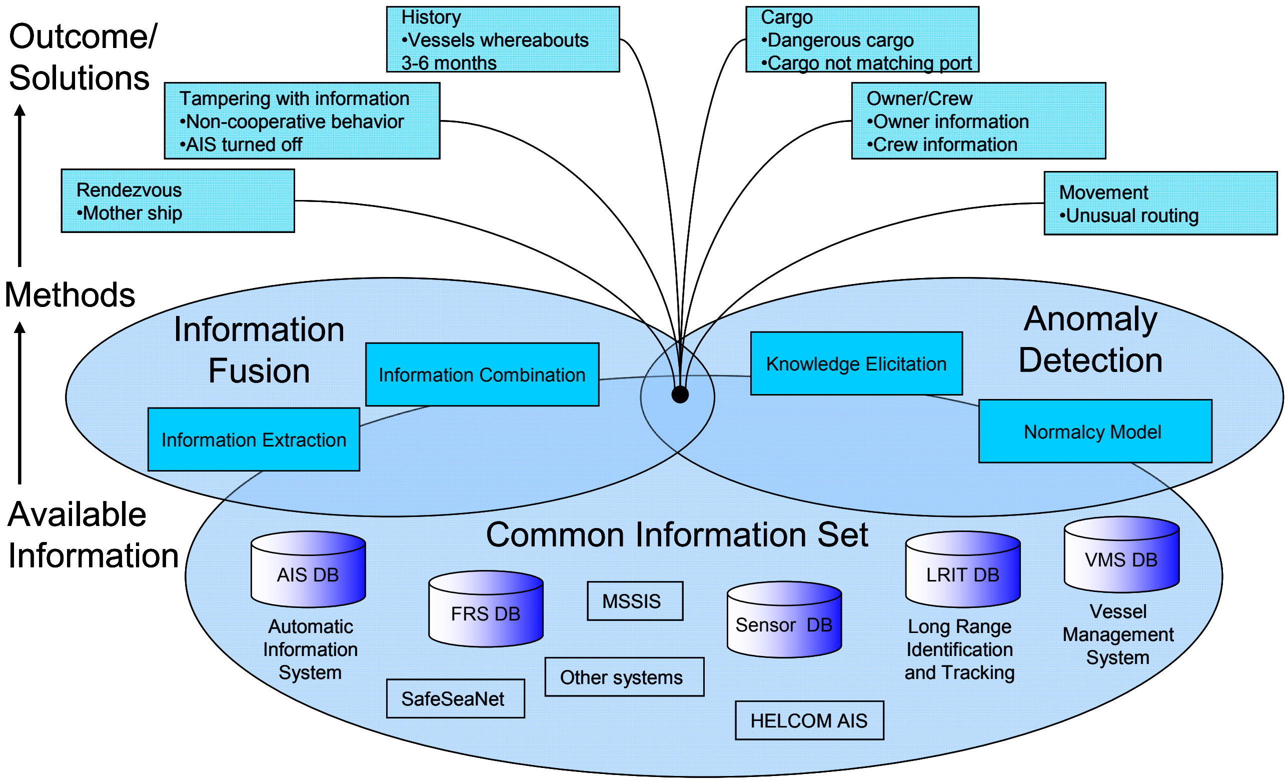

Figure 2. System architecture (Information Fusion, Anomaly Detection, and CIS)

6. SUMMARY

We have presented the results of a study on maritime domain awareness performed during the fall of 2008. Results from an analysis of an identified capability gap, and a user workshop addressing the identified gap "world-wide tracking of maritime activities" were given. We have outlined the SMARTracIn approach and a proposed architecture, with system components for an information workbench that helps users track information about ocean-going vessels, even when there is no continuous sensor coverage.

There are ample opportunities for work in information fusion within the application area of maritime domain awareness. In addition to implementing the system architecture outlined in this paper, there also need for research on algorithms for anomaly detection, information flow mechanisms using semantic technology, and user experiments to determine the correct way of presenting information to the users of the information workbench.

SMARTracIn will make significant scientific contributions to the field of information fusion by developing methods for modeling and fusing information from heterogeneous information sources such as sensors and intelligence records,. The combination of knowledge-based and data-driven anomaly detection methods at all fusion levels is an innovative application of information fusion. We plane to take advantage of geo-fencing and develop information fusion methods that fuse results from anomaly detection at different levels and regions, using the proposed architecture. To help mediate between machine-based anomaly detection and human-centered threat analysis, we may develop visual analytics, and information management methods to help user rank information and detect spoofs.

REFERENCES

[1] BORTEC, "A Frontex study on technical feasibility of establishing a surveillance system", Warsaw, December 2006.

[2] C Carthel, S Coraluppi, P Grigman, "Multisensor Tracking and Fusion for Maritime Surveillance", Proc. International Conference on Information Fusion 2007

[3] C Helleur, M Mathews, N Kashvap, J Rafuse, "Track-to-track Fusion by a Human Operator for Maritime Domain Awareness", Proc. International Conference on Information Fusion 2007

[4] M. E. Higgins, D. L Hall, J. Llinas, Handbook of Multisensor Data Fusion: Theory and Practice, CRC Press 2008

[5] C. Mårtenson, A. Horndahl, "Using semantic technology in intelligence analysis", Proc. Skövde Workshop on Information Fusion Topics 2008

[6] R. B. Pirie, D. A. Whelan, The 1,000 Ship Navy: Maritime Security Partnerships. The National Academies Press. Washington, DC. 2008. Available at: http://www.nap.edu/catalog/12029.html. [Downloaded: 2008-11-03]

[7] Swedish Emergency Management Agency, 2008, Ref: 1831/2008

[8] P Valin, A Guitouni, E Bossé, H Wehn, R Yates, H Zwick, "Testbed for large volume surveillance through distributed fusion and resource management", Proc. SPIE 6578, 657803 (2007)