Categorization of Maritime Anomalies for Notification and Alerting Purpose

Jean Roy
Defence R&D Canada – Valcartier
2459 Pie-XI Blvd. North, Quebec (Quebec)
Canada, G3J 1X5
jean.roy@drdc-rddc.gc.ca

Michael Davenport
Salience Analytics Inc.
87 West 41 Ave, Vancouver, BC
Canada, V5Y 2R8
mrd@salienceAnalytics.ca

Abstract - *Automated anomaly detection systems in the maritime domain typically generate large numbers of unorganized alerts of various types which must be reviewed by human analysts. When the volume of reports becomes very high, and when the reports cannot be structured and/or prioritized, there is a greater risk that analysts/subscribers will reject the whole data stream. Efficient mechanisms are thus needed to make the reports more palatable to the analysts and/or the partner agencies on a network who may subscribe to an anomaly-reporting service. Such mechanisms require a categorization of the anomalies that is well-matched to the implicit operational models of the end-users. This paper presents such a categorization, based on a taxonomy of the maritime situational facts involved in anomaly detection identified and validated through knowledge acquisition sessions with experts. The paper begins with a review of domain challenges, knowledge-based (expert) systems, and the knowledge engineering process that was used. Highlights of results from knowledge acquisition sessions with maritime domain experts are presented; these results are the foundation of a proposed taxonomy of maritime situational facts of interest. This taxonomy is then used as a mechanism to categorize maritime anomalies.*

Keywords: Maritime Domain Awareness, Maritime Situational Awareness, Anomaly Detection, Expert System, Knowledge Representation, Automated Reasoning

1 Introduction

Maritime domain operators/analysts around the world typically have a mandate to be aware of all that is happening in maritime approaches. This mandate is based on the need to protect from attack, defend sovereignty, detect illegal activities, and support search and rescue activities, and it became more challenging in the past decade, as commercial shipping became a potential threat.

Operators and analysts maintain 24/7 watch over the oceans in support of the mandate. They do so by extracting and analyzing situational facts from a variety of sensor data streams and analysis tools. The main challenges facing them are not a lack of data – in some ways they are drowning in data – but rather:

- The data has often been degraded by ambiguities and data-entry errors, requiring operators to spend large amounts of time cleaning up the data to reveal the underlying situational facts.
- The data has too often been delivered to the operators as individual dots on screens, each from a different moment in time, rather than being first resolved into tracks.
- A huge fraction of the information presented to the operators is mundane, from platforms going about normal, legitimate activities, and no attempt is made to draw attention to the non-mundane.

1.1 Detection of maritime anomalies

Regarding the last bullet above, the search for automated ways to sift through mundane maritime surveillance tracks and contacts and extract a smaller number of anomalous events that are worthy of an operator's attention was discussed in [1]. Recent work analysing knowledge management and exploitation requirements [2] identified anomaly detection as a high priority. Further studies characterized the types of anomalies that are of interest [3] and candidate algorithms for detecting one class of anomalies [4].

1.2 Requirement for support systems

To achieve their mandate, maritime domain operators and analysts are constantly searching for situational facts. Many facts of interest can be observed (although only imperfectly) using their observation assets (e.g., sensors, self-reporting systems) but many cannot, sometimes because they are intrinsically unobservable [5]. This is especially true of highly abstract types of situational elements (e.g., the intent of a human actor in the situation), and also of some of the relationships between the situational elements. Facts that cannot be directly observed must be inferred from what can be observed, i.e., derived as a conclusion from other facts or premises, or by reasoning from evidence. Human operators/analysts thus use their knowledge of the maritime domain and their reasoning faculties to infer many important facts – and they are experts at doing this. Unfortunately, they are also often overwhelmed by the large amount of data and information that they have to process

and that might be important. Automated reasoning tools could thus support them.

Recognizing that operators/analysts are invariably far better than computers at understanding what surveillance data *means*, our recent research efforts seek not to replace them, but rather help them to prioritize their work by marking data as either "probably normal" or "possibly anomalous." Such a data analysis task fits automated reasoners pretty well because they can do the same task over and over again without getting bored and tired.

1.3 Anomaly notification and alerting

An emerging problem is that recent automated anomaly detection systems for maritime situational awareness (MSA) typically generate a huge number of alerts of different types, without any structured grouping. The high volume and lack of structure have been described by the operators and analysts as a real showstopper for such systems. The developers of these systems thus now need to develop a more efficient notification and alerting mechanism to communicate anomalies to system users, or to publish information about anomalies to network partners.

Ideally, such a mechanism would be based on a rich categorization of the anomalies so that notifications and alerts could be adapted, for example, to:

- the missions and mandates of the analyst agency (sovereignty, search and rescue, drug smuggling, illegal immigration, etc.),
- the roles of each operator or analyst (surveillance officer, intelligence officer, etc.),
- variable confidence in each data feed,
- insights gained in previous analyst assessments.

To support such adaptations, this paper presents a taxonomy of the maritime situational facts relevant for anomaly detection.

1.4 Organization of this paper

The paper is organized as follows. Knowledge-based systems, with emphasis given to expert systems, are introduced in Section 2. Then knowledge engineering is briefly described in Section 3. One key step of knowledge engineering is knowledge acquisition. This is discussed in Section 4 that first provides a high-level summary of the initial small-scale knowledge acquisition and elicitation session conducted to capture the anomaly detection know-how of some maritime domain experts, followed with an introduction to recent additional efforts with SMEs to validate and expand the initial results. Highlights of the new results of these more recent elicitation efforts are presented in Section 5, along the perspectives of maritime threats, risks, and actionable events. Then, Section 6 focuses at the actual maritime anomalies that were also identified and documented.

As facts play a key role in the knowledge-based approaches being considered for anomaly detection, a long (but non-exhaustive) list of maritime situational facts is provided in Section 7 to illustrate the wide variety of these situational facts. Based on a review of many such facts of interest that can be identified from the knowledge collected from the SMEs, a taxonomy of maritime situational facts is proposed in Section 8. Then, Section 9 shows how this taxonomy can be used as a mechanism to categorize maritime anomalies for notification/alerting purpose. Finally, some concluding remarks and recommendations for future work are provided in Section 10.

2 Knowledge-based systems

Automated reasoning with computers is not new; it has been studied extensively for decades in the field of Artificial Intelligence. It requires 1) domain knowledge encoded in a suitable format [6], and 2) sound inference procedures [7]. Until the mid-sixties, a major quest of artificial intelligence was to produce intelligent systems that relied little on domain knowledge and more on powerful methods of reasoning [8]. By the early 1970's, it had become apparent that domain knowledge was the key to building machine problem solvers that could function at the level of human experts.

A knowledge-based system is a computer system that represents and uses knowledge to carry out a task. An expert system is an intelligent computer program that uses knowledge and inference procedures to solve problems that are difficult enough to require significant human expertise for their solution [8]. As the applications for the technology have broadened, the more general term *knowledge-based system* has become preferred by some people over expert system because it focuses attention on the knowledge that the systems carry, rather than on the question of whether or not such knowledge constitutes expertise [9].

Figure 1 illustrates the basic concept of a knowledge-based (expert) system.

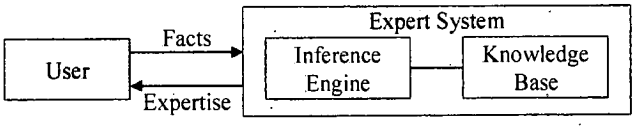

Figure 1. Basic concept of a knowledge-based (expert) system function [8].

The user supplies facts or other information to the expert system and receives expert advice or expertise in response [8]. Internally, the expert system consists of two main components (Fig. 1). The inference subsystem is the part that reasons its way to the solutions of problems, with its search guided by the contents of the knowledge base [9]. Traditionally, colourfully, and colloquially, this part of a knowledge system has been called the inference engine. The knowledge base contains the knowledge with which the

inference engine draws conclusions [8]. These conclusions are the expert system's responses to the user's queries for expertise.

Along this line of thoughts, a number of research initiatives related to the application of knowledge-based systems technologies to the support of situation analysis, with emphasis on maritime anomaly detection, have been conducted in recent years. One goal of the research activities reported in [10] and [11] is to cover a broader spectrum of anomalies through the exploitation of different knowledge representation and reasoning approaches [17].

3 Knowledge engineering

The development of a knowledge-based system begins with organizing the knowledge in the target application domain [5]. Knowledge engineering, illustrated in Fig. 2, has been discussed in [12]. It is the process of building a knowledge base for a knowledge-based system [13]. It deals with knowledge acquisition, knowledge representation, knowledge validation, inferencing, explanation and justification, and maintenance.

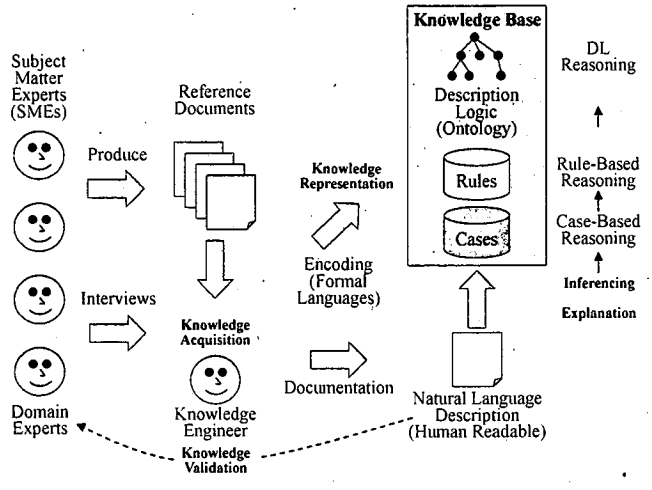

Figure 2. Knowledge engineering.

A knowledge engineer is someone who investigates a particular domain, determines what concepts are important in that domain, and creates a formal representation of the objects and relations in the domain. Often, however, the knowledge engineer is trained in representation, but not an expert in the domain at hand. The basic model of knowledge engineering thus portrays teamwork in which a knowledge engineer interacts with one or more human experts of the domain of interest in building the knowledge base [14]. It is the expert's job to provide knowledge about how he/she performs the task that the knowledge-based system will support or perform.

4 Maritime knowledge acquisition

The development of knowledge-based systems necessarily includes the participation of experts from the application domain, i.e., the Subject Matter Experts (SMEs) in Fig. 2. Actually, the development process begins with the identification of SMEs from the operational community.

Expertise is a specialized type of knowledge that is known only to a few [8]. It is not commonly found in public sources such as books and papers. Instead, expertise is the extensive, task-specific and implicit knowledge of the expert that is acquired from training, reading, and experience, and that must be extracted and made explicit so it can be encoded in an expert system. An expert is a person who has (or is recognized by peers as having) expertise in a certain area [8]. One actually talks about degrees or levels of expertise [14]. In general, the term *expert* connotes both specialization in narrow problem-solving areas or tasks and substantial competence [9] [14]. An expert can solve problems that most people cannot solve, or can solve them more efficiently (but not as cheaply) [8].

Knowledge acquisition is the process of collecting, extracting, transferring, accumulating, structuring, transforming and organizing knowledge (e.g., problem-solving expertise) from one or more knowledge sources (human experts, books, documents, sensors, or computer files) for constructing or expanding a knowledge base [14].

A commonly used form of knowledge acquisition is face-to-face interview with SMEs. It is an explicit technique and it appears in several variations. It involves a direct dialog between the expert and the knowledge engineer. Information is collected and it is subsequently transcribed, analyzed, and coded. In the interview, the expert is presented with a simulated case or, if possible, with an actual problem of the sort that the expert system will be expected to solve. The expert is asked to "talk" the knowledge engineer through the solution.

Unfortunately, acquiring knowledge from experts is a complex task. This process has been identified by many researchers and practitioners as a (or even as *the*) bottleneck that typically constrains the development and construction of expert systems and other AI systems.

4.1 Maritime anomaly detection workshop

Reference [1] describes a small-scale knowledge acquisition and elicitation session, a maritime anomaly detection workshop (MADW), which we initially planned and conducted to identify, capture and document some of the anomaly detection know-how of maritime domain experts.

The discussions at this MADW began with considerations about what is actually meant by the term *anomaly*. One "dictionary" definition of this term that was formulated and that seems to be appropriate in the context of maritime domain situation awareness is: *"Something peculiar (odd, curious, strange, weird, bizarre, atypical) because it is inconsistent with or deviating from what is*

usual, normal, or expected, or because it is not conforming to rules, laws, or customs." Taking into account all of the discussions, some consensus emerged from the workshop participants that a good, simple working definition of the term anomaly would be as "*a deviation from the expected.*"

4.2 Initial taxonomy of maritime anomalies

One of the sub-objectives of the MADW was to identify a classification scheme for anomalies. This was indeed one of the most important aspects of the MADW. Hence, a significant portion of the limited time available for the MADW was devoted to this issue. During the workshop, brainstorming was the technique used to help generate ideas.

A draft taxonomy of maritime situation anomalies was produced at the MADW and was presented in [1]. At the highest level, maritime situation anomalies were categorized as static or dynamic. Static anomalies include things related to the name, IMO number, international radio call sign (IRCS), ship control number (SCONUM), license, etc., of a vessel. Dynamic anomalies were further decomposed into kinematic and non-kinematic anomalies. The kinematic category represents those anomalies related to the location, course, speed and manoeuvres of vessels. Sensor/source reporting anomalies, when these are related to kinematic aspects, were also attached to this category. Such anomalies appear to be kinematic but are actually due to reporting errors (e.g., a ship position that is reported on dry land or in non-navigable waters). The non-kinematic category includes aspects such as crew, passengers, and cargo.

The efforts reported in [1] represent a first cut at developing a taxonomy of anomalies in the maritime domain. This taxonomy has been further documented in [3].

4.3 Recent knowledge acquisition sessions

There may be inconsistencies, ambiguities, duplications, or other problems with the expert's knowledge that are not apparent until attempts are made to formally represent the knowledge in a knowledge-based system [8]. The process of developing such a system thus has an indirect benefit since the knowledge of human experts must be put into an explicit form for entering into the computer. Because the knowledge is then explicitly known instead of being implicit in the expert's mind, it can be examined for correctness, consistency, and completeness. The knowledge may then have to be adjusted or re-examined, which improves its quality [8].

Along this line of thought, the first attempt to exploit the maritime domain knowledge acquired at the initial MADW revealed some weaknesses of various kinds. This was sufficient to trigger significant additional efforts with SMEs to validate and expand the initial results. Hence, five additional workshops were recently conducted at three different locations, involving 17 SMEs overall, for a total of over 100 SME hours. Once again, the objectives were to: 1) validate the knowledge collected in previous R&D activities, and 2) acquire new knowledge to expand our knowledge base. Information was collected in different ways; information from previous studies was reviewed, and maritime domain subject matter experts were interviewed on both coasts in Canada. Using all sources of information, including previous anomaly description tables, detailed descriptions of anomalies and related facts were developed. They were then validated with subject matter experts, and new anomaly tables were produced. References [15] and [16] document these knowledge acquisition sessions. These two reports:

- describe the workshop discussions,
- provide an analysis of the collected knowledge,
- describe data feeds to the RJOCs,
- provide tables describing threats,
- identify "actionable events",
- identify "intermediate facts", and,
- characterize anomalies.

These reports describe our current understanding of anomaly detection in the Canadian context.

5 Threats, Risks, and Events

The anomalies tabulated in [3], [4] and [16] repeatedly refer to "illegitimate reasons" for anomalous behaviour. The term "illegitimate" here refers to behaviour that would mandate immediate attention from the operators, if identified. Analysts are interested in these anomalies because they indicate either:

- **An impending threat:** such as an attack on infrastructure or sovereignty infringement.

- **A noteworthy event:** such as a regulatory infraction, or the departure of a VOI.

5.1 Impending threats and associated risks

In [16], the sets of events and threats that RJOC analysts have in mind when looking for anomalies are extracted. Seven tables are provided, describing threat situations along the notions of capability, opportunity, intent and risk. These tables document the threats of:

- illegal fishing,
- smuggling or illegal immigration,
- piracy or attack on a high value vessel,
- attack on seafloor infrastructure,
- attack on above-water infrastructure,
- illegal information gathering, and,
- Hidden agenda (bomb in a box).

Table 1 is an illustrative example of the contents of the threat tables.

Table 1. Example Threat Table: Threat of piracy or attack on a high value vessel (Table 4-3 of [16])

Description: Pirates or terrorists, using a ship of opportunity, may plan to intercept, attack, or take a "High Value Vessel" (HVV) that has perceived value to them.
Capability: • Does the potential attacker (PA) have adequate manoeuvrability to intercept the HVV? • Is the potential attacker equipped to take or cause major damage to the HVV?
Opportunity: • Is the current location and heading of the PA consistent with a threat to the HVV? • How will the positional opportunity change with time based on current location of the PA and (to a lesser extent) on course? • When must the PA "make a move" else opportunity will be lost? Given available sensors, when would we see evidence that the move occurred or not? • Is there a media presence that would amplify or reduce the value of the HVV? • Is there a probable perceived invulnerability to getting caught? • When will surveillance aircraft fly over?
Indicators of Intent: • Would an attack on the HVV be beneficial to PA? • Is the PA well known to us? • Are there indications and warnings? • Is the track and speed of the PA consistent with its declared commercial interests? • Has the PA changed speed or heading in a manner indicative of an interception? • How probable is it that an attack is planned?
Risk: • How soon must we act to have enforcement assets on-scene in time to prevent the attack, if one is planned? • What is the impact (e.g. on national security, infrastructure, morale, productivity, defense capability, political reputation) if an attack is planned and not prevented?

5.2 Actionable events

The perspective of « actionable events » is another point of view that was considered during the analysis of the knowledge acquired. In this regard, Table 2 lists events that might require a response, but are not considered threats because they have already happened. These differ from the anomalies because they represent the events that cause the anomalies. In a sense, actionable events are what makes the anomalies interesting.

Table 2. Actionable events (Table 4-8 of [16])

Sovereignty Infraction: • Sovereignty has been challenged by navigating a vessel through a controlled zone without required permits • Example Action: Send a ship or MSA to investigate or intervene.
Foreign Warship: • Foreign navy ship (e.g. submerged sub) in within 12nm limit without permission. Observation may be e.g. from shore or by maritime surveillance aircraft. • Example Action: Send a ship or MSA to investigate or intervene.
Zone Infraction: • Vessel is in an excluded zone, or is engaged in an activity not allowed in a zone. • Example Action: Request investigation, inform most concerned agency, add ship to watch list.
Missing or Erroneous Call-In or Paperwork: • Ship appears to be headed into a port but has not called in or submitted pre-arrival information as required. • Example Action: Inform Coast Guard or concerned agency, add ship to watch list
Rendezvous: • Two or more ships have rendezvoused • Example Action: Request investigation, inform concerned agency.
Ship Sinks or has Major System Failures: • A ship sinks or ceases all emissions. • Example Action: Inform concerned agency, request investigation.
Ship Enters Dangerous Zone: • A ship enters an ice zone, or fails to avoid a dangerous weather event • Example Action: Inform concerned agency, ask agency to contact the ship.
Ship is Spoofing • Signals from a ship's AIS, LRIT, or VMS are being spoofed to report false information • Example Action: Request investigation, inform concerned agency, ask ship to clarify

6 Maritime anomalies

Once again, the main objectives of the most recent knowledge acquisition sessions with the maritime domain expert were to: 1) validate the knowledge collected in previous R&D activities, and 2) acquire new knowledge to expand our knowledge base. The resulting domain

knowledge for all maritime anomalies was encoded using a table format template that summarizes the key descriptive attributes of each anomaly. For example Table 3 reproduces Anomaly #24, concerning the coincidence of cargos that together are dangerous. The final box of the table would normally indicate approval from a specific Subject Matter Expert.

Table 3. Example Anomaly Table: Coincidence of cargos that together are dangerous (Table 5-24 of [16])

Short Name: Bad Cargo Coincidence	
Description: Two or more cargos, which when put together would represent an unusual threat, arrive at nearby locations.	
Illegitimate reasons for behaviour:	**Corroboration questions:**
Terrorist plot	Who are the addressees? Were cargos inspected at source?
Legitimate reasons for behaviour:	**Corroboration questions:**
Coincidence	Legitimate addressee? Did ships ask for berth change?
Best information sources to detect this anomaly: Pre-Arrival Information Report (PAIR) CBRN reports (via CBSA)	
Information errors that might spoof this anomaly: Incorrect berth maps for terminal	
Ship classes for which this would not be an anomaly: HMC/CCG/DFO; RCMP/Pilot, Fishing, Passenger	

Detection Rule:
Given ship *A* has cargo *AC* **and** ship *B* has cargo *BC*
Given ships *A* and *B* were assigned berths *Q1* and *Q2*
Then
if cargos *AC* and *BC* when combined represent a threat **Then**
if berth Q1 is adjacent to berth Q2 **Then**
if *A* and *B* will be in port at the same time **Then**
Anomaly	

Detection Challenges: Inter-agency information firewalls	
Comments: Example 1: Ammonia and bleach Example 2: Diesel oil and fertilizer	
SME Approval:	

A total of 28 anomalies were characterized and documented in [16] (down from the 37 initially documented in [3] as a result of the first maritime anomaly detection workshop). Although there are fewer anomalies documented in the end, there is actually more knowledge available now that has been captured and made explicit in references [15] and [16].

7 Maritime situational facts

Facts play a key role in the knowledge-based approaches being considered for anomaly detection ([10] and [11]). In this regard, reference [16] explicitly lists maritime situational facts that the analysts consciously or unconsciously use to help interpret the maritime situation. Aside from these explicit statements, a careful review of all the knowledge acquired and documented for all of the knowledge acquisition sessions conducted so far about anomaly detection in our research program allows for the identification of a large number of maritime situational facts of interest. The following non-exhaustive list of over a hundred examples illustrates the wide variety of these situational facts:

- Ship X is conducting activity Y
- Ship X is involved in activity Y
- Ship X is emitting emergency signal Y
- Ship X goes radio silent
- Ship X is at location Y
- Platform X is being relocated at location Y
- Ship X has actual destination Y
- Ship X has declared destination Y
- Ship X has changed its destination
- Ship X and Ship Y have the same destination
- Track X ended at location Y
- Ship rendezvous occurred at location Y
- Ship X is in proximity of ship Y
- Ship X is in proximity of infrastructure Y
- Ship X has rendezvous with ship Y
- Group of ships X-Y-Z has rendezvous at location L
- Ship X is inside/outside route Y
- Ship X is following a great circle route
- Route X is consistent with destination Y
- Ship X is inside/outside zone Y
- Ship X has distance Y inside/outside zone Z
- Zone X is closed to natural resource Y
- Ship X is approaching infrastructure Y
- Ship X is moving away from country Y
- Ship X is drifting
- Ship X is entering zone Y
- Ship X is exiting zone Y
- Ship X is heading inbound/outbound
- Ship X is heading towards port Y
- Ship X is heading into danger
- Ship X is heading towards a port that can handle its cargo
- Ship X is loitering
- Ship X has changed heading
- Ship X has changed speed

- Ship X is slowing/has slowed down
- Ship X is passing through zone Y
- Ship X is going around obstacle Y
- Ship X has speed too high for ship class Y
- Ship X has speed too high for activity Y
- Ship X has stopped
- Ship X has (voyage) plan Y
- Ship X has current berth Y
- Ship X has requested berth Y
- Ship X has declared cargo Y
- Ship X has bad cargo coincidence Y
- Port X can handle cargo Y
- Ship X has equipment Y
- Crew list of ship X includes person name Y
- Passenger list of ship X includes person name X
- Ship X has supply Y
- Person X is in control of ship Y
- There is a storm (in zone X)
- Event X is accidental
- Ship X has arrived port Y
- Ship X is departing port Y now
- G8 meeting is happening now
- There is a SAR event (in zone X)
- Ship X has current flag Y
- Ship X has historical record of activity Y
- Ship X is quarantined
- Ship X is involved in criminal act Y
- Ship X has felony warrant Y on it
- Ship X is involved in criminal infraction Y
- Ship X is involved in terrorism
- Ship X is being inspected
- Ship X is compliant to regulation Y
- Ship X is involved in regulation infraction Y
- Ship X has permit Y
- Business circumstances are changing
- Ship X has current owner Y
- Ship X has visited port Y
- Ship X (voluntary) reports to be in location Y
- Ship X is reporting false location
- Ship X has changed IMO number
- Ship X is within/beyond range of active radar
- Data X has been mis-entered
- Ship X has AIS set up incorrectly
- Ship X has AIS failure
- Ship X has navigation radar failure
- All contacts of ship X are in one location
- Ship X and ship Y have the same IMO number
- Moving distance X in time Y requires impossible speed
- Ship X has mismatch between reported speed and calculated speed
- Data X arrived late
- Ship X has not submitted required report(s)
- Ship X is late with 96 hr call-in
- Track X has ended
- Reporting on track X has stopped
- Ship X is missing on display
- Database X is outdated
- Data X has been validated
- Ship name X is on ship analyst defined list
- Ship name X is on ship COI list
- Ship name X is on ship MSC list
- Ship name X is on ship VOI list
- Ship name X is on ship warm and fuzzy list
- Ship name X is on ship watch list
- Ship X is more than 20 years old
- Ship X has mechanical problem Y
- Ship X has reported equipment failure
- Ship X is stuck in ice
- Ship X has medical problem Y
- Ship X has destructive capability Y
- Ship X has capability to intercept ship Y
- Ship X is a high-value vessel
- Behaviour X is indicator of intent Y
- Indicator X matches activity Y
- Ship X has opportunity to intercept HVV Y
- Ship X has hijack opportunity
- Infrastructure X has vulnerability Y
- Ship X presents risk Y
- Ship X is at location Y in time interval Z
- Ship X goes to country Y every month
- Ship X has estimated time of arrival (ETA) Y
- Ship X arrives at time Y and departs at time Z
- Arriving late is commercial advantage to ship X
- Ship X arrives before ship Y
- Ship X and ship Y will arrive at the same time
- Ship X is of type Y
- Ship X is over X tons
- Ship X is a submarine

Many of the facts above refer to some « activity X » for a particular ship/vessel. Some examples of such activities of interest to the maritime operators/analysts are given below:

Attacking	Attending	Avoiding	Boarding
Breaking the law	Broadcasting	Causing an accident	Clustering
Collecting intelligence	Coordinating with others	Counterfeiting	Cutting cables
Dealing arms	Deceiving	Defying	Delivering
Deploying	Dragging	Drifting	Dropping-off
Exchanging	Exercising	Exporting	Evacuating
Fishing	Frauding	Gathering information	Grabbing and dashing
Handling off	Harvesting resources	Hiding	Hijacking
Hitting	Importing	Informing	Inserting
Intercepting	Loitering	Lying	Medevac
Navigating	Patrolling	Picking up	Pirating
Poaching	Polluting	Positioning	Protesting

Recovering equipment	Rescuing	Researching	Responding
Returning	Sailing	Searching	Servicing
Sheltering	Sightseeing	Sinking	Smuggling
Stealing	Supporting	Switching mode	Terrorizing
Threatening	Touring	Trading	Trafficking
Trans-boarding	Transiting	Transporting	Trawling
Waiting	Whaling		

Many of the facts previously listed refer to some « zone X ». Some examples of such zones of interest to the maritime operators/analysts are given below:

Analyst defined	Anchorage	Area of interest	Area of responsibility
Closed (to activity)	Danger	Drug producing	Drug smuggling
Economic Exclusion Zone (EEZ)	Economically depressed	Exclusion	Exercise
Extreme weather	Fishing	Fishing grounds	Heavy shipping
High traffic density	« Hot »	Ice-covered	Ice hazard
Interdiction	International water	NAFO-controlled	Natural resource
Non-navigable	Pirate hazard	Quarantine	Recreation
Refugee	Replenish-ment	Restriction	Scenic location
Search	Sensor black-out	Submarine operations	Territorial waters
Traffic-managed	Weather hazard	Whales	With/without a specific feature

Finally, a close look at the maritime situational facts also reveals that a computer-based fact management system would have to manipulate a number of lists of different maritime items of interest. Examples of such lists are lists of:

Activities	Bad cargo coincidences	Berths	Cargo attributes
Commercial advantages	Emergency signals	Equipment	Exceptions
Financial problems	Intents	Infrastructures	Locations
Permits	Person types	Ports	Canadian ports
Regulations	Regulated reports	Shipping lanes	Ship types/classes

8 A taxonomy of maritime facts

Although the list of maritime situational facts presented above is very long, it represents only a subset of all the facts of interest that can be identified from the knowledge collected from SMEs. Based on a careful review of all these facts, the authors propose the taxonomy shown on Fig. 3 to categorize the facts of interest into a convenient, manageable number of classes. The wide diversity of maritime situational facts that one eventually has to consider to cover the overall spectrum of anomalies in the maritime domain is well illustrated with the proposed taxonomy. One can easily imagine how complex it quickly becomes to manage these facts and anomalies without such a taxonomy.

9 Maritime anomalies categorization

The authors have mapped the current set of anomalies documented in [16] onto the taxonomy of Fig. 3. The result is shown on Fig. 4. It really was an easy exercise to categorize the 28 anomalies using the proposed taxonomy. It is believed that many other anomalies could as easily be categorized in the future, as our knowledge base in this domain further expands. An additional advantage of the proposed taxonomy is that it could be used as some sort of « check list » in future discussions with the maritime domain experts to identify the next set of anomalies to be considered for automatic detection in our situation analysis support systems.

10 Conclusions

A mechanism to categorize anomalies in the maritime domain was presented in this paper as a step towards the efficient management of the communication of such anomalies to the operators/analysts, or their publication to partners on a network. It is based on a taxonomy of the maritime situational facts of interest that are involved in anomaly detection. This taxonomy was carefully derived from a review and analysis of results from various knowledge acquisition sessions with maritime domain experts; the knowledge collected during these sessions really constitutes the foundation of the proposed taxonomy.

Further work will be required to actually use the taxonomy in some concrete « anomaly filtering » mechanism, which would be configured by the analyst according to his/her preference(s) or role(s) in the intelligence organization, to modulate the presentation of the alerts on the display of some computer-based situation analysis support system. Future work will also include the use of the taxonomy for the definition of a data exchange model for maritime anomalies (which could actually be an extension to an existing standard model). Such work would contribute to the development of an appropriate notification/alerting mechanism to be used across a network, on a publish/subscribe service oriented architecture for example, to exchange anomaly information among partners.

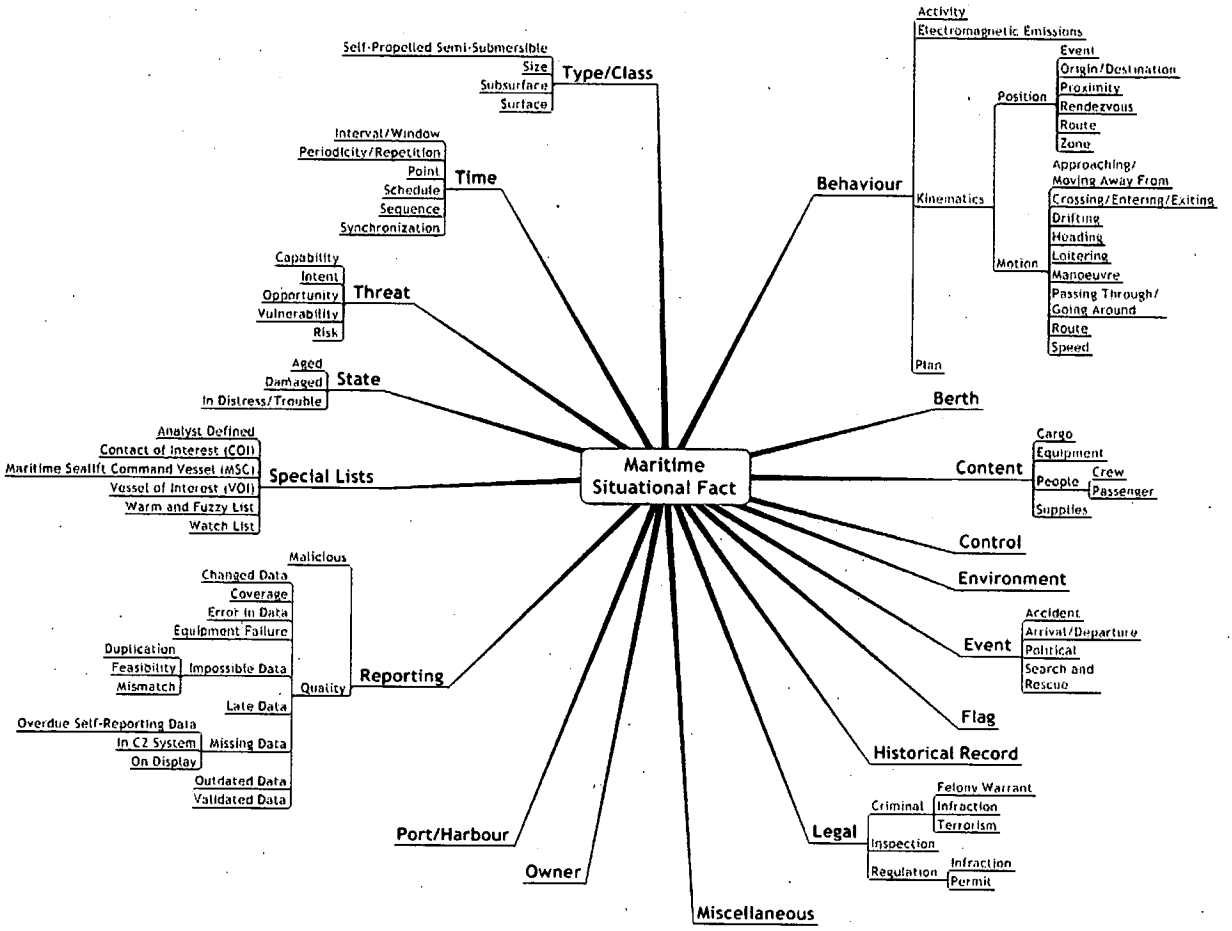

Figure 3. A proposed taxonomy of maritime situational facts

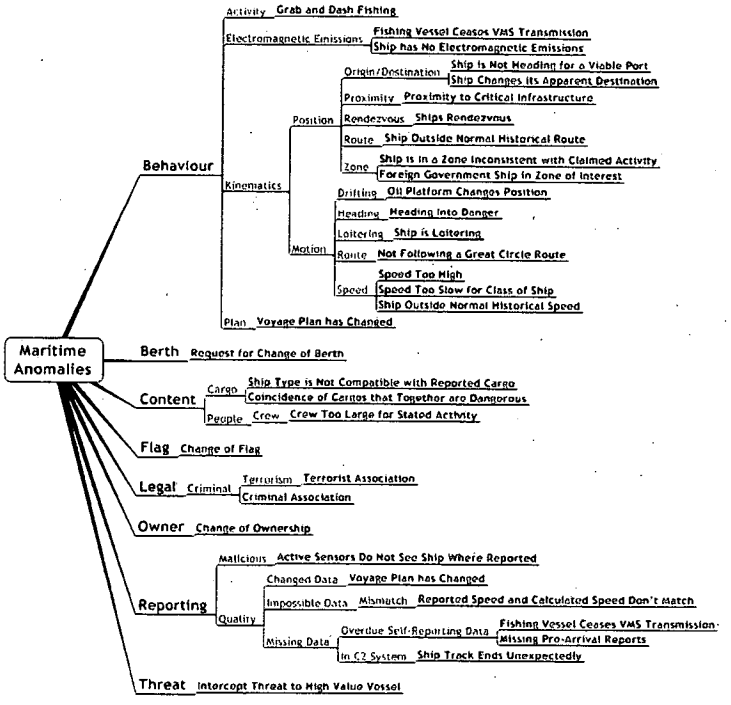

Figure 4. Using the maritime situational fact taxonomy to categorize maritime anomalies

References

[1] Roy, J., *Anomaly Detection in the Maritime Domain*, Proceedings of Technologies for Homeland Security and Law Enforcement/Maritime Security Technology 2008: Challenges and Solutions, SPIE Defense and Security 2008, Orlando, Florida, 16-20 March 2008.

[2] Davenport, M., *Maritime Domain Awareness Knowledge Management Requirements*, MacDonald Dettwiler and Associates Ltd., DRDC Scientific Authority: Jean Roy, DRDC Valcartier CR 2007-174, 20 July 2007.

[3] Davenport, M., *Maritime Anomaly Detection Workshop Report and Analysis*, MacDonald Dettwiler and Associates Ltd., DRDC Scientific Authority: Jean Roy, DRDC Valcartier CR 2008-275, 31 March, 2008.

[4] Davenport, M., *Kinematic Behaviour Anomaly Detection (KBAD) – Final Report*, DRDC Scientific Authority: Neil Carson, DRDC CORA CR-2008-002, April 2008.

[5] Roy, J., *Combining Elements of Information Fusion and Knowledge-Based Systems to Support Situation Analysis*, Proceedings of Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006, SPIE Symposium on Defense and Security, Orlando, Florida, 17-21 April 2006, 14 pp.

[6] Roy, J. and Auger, A., *Knowledge Representation Concepts, Paradigms and Techniques for Use in Knowledge-Based Situation Analysis Support Systems*, DRDC Valcartier, TM 2006-755, October 2008.

[7] Roy, J. and Auger, A., *Reasoning Processes, Methods and Systems for Use in Knowledge-Based Situation Analysis Support Systems*, DRDC Valcartier, TM 2006-756, October 2008.

[8] Giarratano, J. and Riley, G., *Expert Systems - Principles and Programming*, PWS Publishing Company, Boston, 1998.

[9] Stefik, M., *Introduction to Knowledge Systems*, Morgan Kaufmann Publishers, San Francisco, California, 1995.

[10] Roy, J., *Automated Reasoning for Maritime Anomaly Detection*, Proceedings of the NATO Workshop on Data Fusion and Anomaly Detection for Maritime Situational Awareness (MSA 2009), NATO Undersea Research Centre (NURC), La Spezia, Italy, 15-17 September 2009.

[11] Bergeron Guyard, A. and Roy, J., *Towards Case-Based Reasoning for Maritime Anomaly Detection*, Second IEEE Symposium on Computational Intelligence for Security and Defense Applications - Detecting and Adapting to Emerging Threats, Ottawa, Canada, 8-10 July 2009.

[12] Roy, J. and Auger, A., *Knowledge and Ontological Engineering Techniques for Use in Developing Knowledge-Based Situation Analysis Support Systems*, DRDC Valcartier, TM 2006-757, October 2008.

[13] Russell, S. and Norvig, P., *Artificial Intelligence - A Modern Approach*, Prentice Hall, New Jersey, 1995.

[14] Turban, E. and Aronson, J.E., *Decision Support Systems and Intelligent Systems*, Fifth Edition, Prentice Hall, New Jersey, 1998.

[15] Davenport, M., Gerbrecht, R., Kraft, J. and Aikins, G., *Knowledge Acquisition Sessions for Maritime Anomaly Detection – Volume 1: Methodology and Interview Data*, DRDC Scientific Authority: Jean Roy, DRDC Valcartier CR 2009-XXX, 31 March 2009.

[16] Davenport, M., *Knowledge Acquisition Sessions for Maritime Anomaly Detection – Volume 2: Anomaly and Threat Tables*, DRDC Scientific Authority: Jean Roy, DRDC Valcartier CR 2009-XXX, 31 March 2009.

[17] Roy, J., *Automated Reasoning for Maritime Anomaly Detection*, Proceedings of the NATO Workshop on Data Fusion and Anomaly Detection for Maritime Situational Awareness (MSA 2009), NATO Undersea Research Centre (NURC), La Spezia, Italy, 15-17 September 2009.