Redefining Situation Awareness for the Maritime Information Warfare Domain

Anna-Liesa S. Lapinski
Defence Research and Development Canada, 9 Grove Street, Dartmouth, NS, Canada B3A 3C5

ABSTRACT

Maritime Situational Awareness (MSA) is generally understood in the physical world. The challenge is achieving it, not understanding the concept. However, what does situation awareness (SA) mean in the Maritime Information Warfare (MIW) domain? An ongoing project at Defence Research and Development Canada is addressing that question. Stepping back from the maritime domain, it can be observed that Information Warfare (IW) overlaps with all other warfare areas, but as a warfare area in itself, the concept of SA should still exist. In an effort to ultimately understand what SA in MIW means, this paper first breaks down the information battlespace into four key components: content, content generator, conduit, and repository. These are posed as sub-battlespaces in the information battlespace, analogous to above water and underwater sub-battlespaces. Then, the types of SA elements are proposed: physical, digital, and human. This is important because while one warfare activity might be heavily human centric, another might be technology centric. However, to adequately conceptualize SA for any warfare activity, there should be cognizance that all three types could exist. The paper concludes with a proposed definition of SA in IW that could be translated to the MIW domain.

Keywords: Information Warfare, Maritime Information Warfare, Situation Awareness, Situational Awareness, IW, MIW, SA

1. INTRODUCTION

On April 1, 2018, Defence Research and Development Canada (DRDC) started a new project in the Maritime Information Warfare (MIW) program: Maritime Information eXploitation (MIX). Part of the MIX project is to recognize the elements of the information environment that must be catalogued to achieve the required situation awareness (SA) for activities within the MIW domain.

To conduct activities in any warfare environment, awareness of the elements surrounding and affecting the activities are required. The accumulation of the necessary awareness is a key step in achieving SA. One of the questions MIX is meant to answer is: what does the term "situation awareness" mean in the MIW domain? However, before that can be answered, it seems logical to take a step back and answer the question: what does the term "situation awareness" mean in the Information Warfare (IW) domain? Once a general understanding is attained of the meaning of SA in IW, it can be translated to answer the original question. After SA in MIW is understood, the next step will be to isolate the elements that need to be catalogued to achieve SA in MIW.

To understand what SA in IW means, this paper begins by breaking down the information battlespace into parts. It then identifies the common categories of elements that contribute to SA in the IW domain. A generic definition of SA in IW is then proposed.

1.1 Information Warfare

In an article in which a commander within Directorate of Naval Information Warfare (DNIW) in Ottawa, Canada is interviewed on IW [1], IW is defined as "the provision, assured use and protection of information, processes, systems and networks, and limiting, degrading and denying that of adversaries to achieve operational advantage across the battle space." The IW domain, therefore, is seen as touching many aspects of warfare; e.g., communications, cyber operations, electronic warfare, information operations, and intelligence. MIW is therefore information warfare as it relates to the maritime domain.

1.2 Situation Awareness

A popular definition of SA is by Endsley [2] which states that "situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." This definition was actually developed within the context of pilot cognition. The question is then, how does that definition translate into the information battlespace?

To begin to answer that question, it is useful to divide Endsley's definition into three parts: cataloguing (i.e., perceiving), comprehension, and predicting. Arguably, in Endsley's definition of situation awareness, comprehension and anticipating the future cannot be achieved until "the elements in the environment within a volume of time and space" begin to be catalogued; therefore, the first part of the definition is critical to attaining the second and third parts of the definition. This paper will focus on that first step: the cataloguing of the required elements as this is a key step to fully attain SA.

In IW, to catalogue the elements it is first required to acknowledge that at the most general level "space," in the Endsley definition, is the information battlespace. In the information battlespace, there may be "inform and influence" operations (within the psychological realm) as well as technical operations (within the technical realm), as Porche et al. [3] proposes. For example, spreading propaganda is an "inform and influence" operation, while disabling an adversary's communication infrastructure would be a technical operation. Porche et al. [3] provide examples of a large variety of specific types of activities under these two operation types.

It should also be pointed out that the IW SA needed to carry out a specific activity will be smaller in scope than the all-encompassing SA for the entire IW domain. Whether for the smaller scoped IW SA or the all-encompassing SA aimed at the entire IW domain, it is useful to understand the information battlespace prior to building SA. The next section attempts to do this by breaking down the information battlespace into parts.

2. BREAKING DOWN THE INFORMATION BATTLESPACE

The following presents an argument that the information battlespace is made up of four smaller battlespaces: content battlespace, content generator battlespace, conduit battlespace, and repository battlespace (these battlespaces are a revision of what was proposed in Hazen et al. [4]). Dividing the information battlespace into smaller battlespaces is analogous to dividing the ocean battlespace into above water and underwater. Within each of these smaller battlespaces, both offensive and defensive activities can take place. In the same way ocean activities can span both above water and underwater battlespaces, activities in the information battlespace can span more than one of these smaller battlespaces. The following explains the smaller battlespaces, with examples.

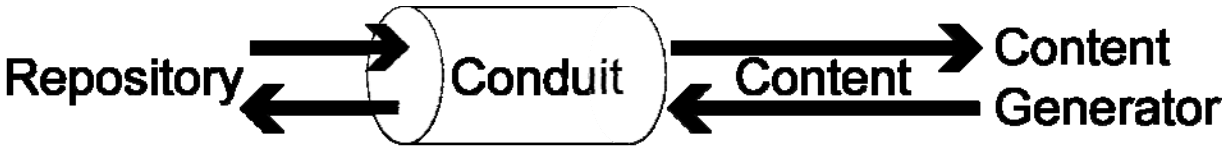

Figure 1. The information battlespace divided into parts; i.e. smaller battlespaces.

Content is an all-encompassing term that represents the information in the IW domain. Content could be a thought, a memory, sensor output, algorithm output, text, an image, a document, a song, etc. Content would also include the medium that contains the content, such as paper, binary file, sound waves, etc., as it can be challenging to separate the content from the medium. Activities in this battlespace might include obtaining the adversary's content, obtaining content about the adversary, protecting our own content, controlling the publicly released content so as to control the narrative, etc.

A **content generator** produces the content described above. It could be a person's brain, something felt, tasted, heard, seen, or smelt by a person (i.e., the human acting as a sensor), a sensor, an algorithm, etc. Both humans and technology can be content generators. Activities in this battlespace might include acting against an adversary's content generator, protecting our own content generator, purposely having a generator produce false content, etc.

The **conduit** is the mechanism for getting content from one entity to another. Conduit is used as an all-encompassing term to represent the manner in which content is moved. This could be speaking, sign language, a computer network or

broadcast, an application used to move/distribute content (e.g., a text messaging application, Facebook, Twitter), the handing of a hard or soft copy of a document to someone, etc. Even though Figure 1 shows only one conduit, there could be many unique conduits placed in series or parallel carrying the same content. For example, the process of converting a thought into spoken words that travel through the air as soundwaves can be thought of as several conduits in series; e.g., from neurons firing, to manipulating mouth muscles, to pressure variation in the air. Also, content going into a conduit may end at a content generator; or content leaving a repository may end in another repository. Activities in this battlespace might be to disrupt, infiltrate, or protect a conduit, set up a conduit to spread false content, etc.

The **repository** is a place for content storage. It could be a person's brain, a server, a filing cabinet, etc. Activities in this battlespace might be to infiltrate, destroy, or protect a repository, etc.

3. SA ELEMENTS OF IW

Under these four smaller battlespaces, it is proposed that there are three types of elements to be catalogued so as to achieve SA: physical elements, digital elements, and human elements (includes psychological elements). The following gives examples of elements under the smaller battlespaces for illustrative purposes.

Physical elements used to help build SA would include an awareness of the physical world that has a direct bearing on what is happening in the information battlespace. For example, in the content generator battlespace, an SA-building element could be the knowledge of the existence and the status of the adversary's sensors. In the content battlespace, an SA-building element could be the physical status of a collection of hard-copy-only paper documents, for example, ones that are in transit. In the conduit battlespace, an SA-building element could be the status of the physical security of critical telecommunication fibres. In the repository battlespace, an SA-building element could be the status of physical infrastructures that house important libraries or servers. It would also be the physical components of the server; such as drives, the casing, etc.

Digital elements used to help build SA would include awareness of the digital world that has a bearing on what is happening in the information battlespace. For example, in the content generator battlespace, an SA-building element could be monitoring critical algorithms for evidence of tampering. In the content battlespace, an SA-building element could be monitoring internal electronic documents for tampering or corruption. In the conduit battlespace, an SA-building element could be status reports on attempted intrusions into a protected computer network. In the repository battlespace, an SA-building element could be monitoring the structure (i.e., not the data) of critical databases, looking for corruption.

Human elements used to help build SA would include facts that are human related, that have a bearing on what is happening in the information battlespace. For example, in the content generator battlespace, an SA-building element might be tracking the location of human assets who provide eye-witness information. In the content battlespace, an SA-building element might be monitoring how the public or adversary perceives a situation. In the conduit battlespace, an SA-building element might be monitoring a network of people that is in place to relay critical information. In the repository battlespace, an SA-building element could be monitoring the cognitive abilities of a workforce [6] and how their cognitive function is impacting short term and long term memory.

Dividing up the information battlespace and SA elements as described above is not critical for achieving SA in IW, but given how large the information battlespace is, it is proposed to be useful. Such a division could aid in identifying gaps and needs, as well as helping to combat the enormity of the SA problem. It is also an explicit reminder that there are physical, digital, and human elements to SA in IW for those who might be biased to one type of element.

It is promising that the battlespace division and the SA elements encompass cyber-physical-social systems (CPSS). A cyber-physical system has both physical and software components interwoven and interacting with each other, such that the interactions alter the system; e.g., autonomous vehicles. A CPSS has humans also woven into the system. For example, Zhong et al. [5] proposes that a command and control organization could be treated as a CPSS. A CPSS has content generators, content, and conduits as part of the system. Even the terminology, cyber-physical-social, generally aligns with the terminology used here: digital, physical, and human elements. Given that monitoring a CPSS might be a task in maintaining SA, it is encouraging that the model can account for all the aspects of a CPSS.

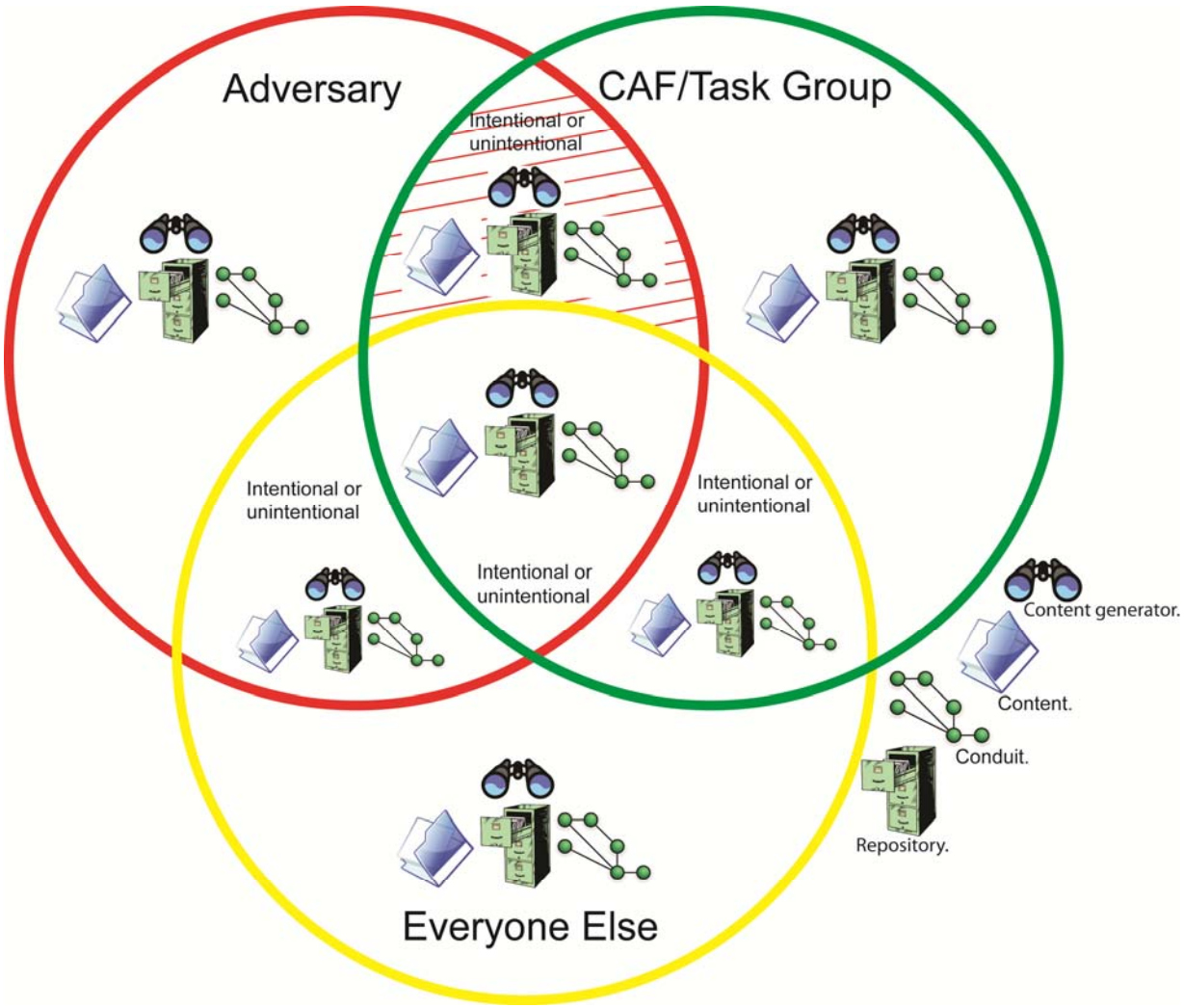

Figure 2. A Venn diagram of access to content generators, content, conduits, and repositories. The green circle indicates what we actually access. The red circle indicates what the adversary has access to. The yellow circle indicates what everyone else (possibly including other government departments) has access to. When the circles overlap, it means both parties have access to certain content generators, content, conduits, and repositories. The segment with the red lines indicates the overlap that the example focusses on.

4. DEFINITION OF SA IN IW

So, what does the term "situation awareness" mean in the Information Warfare domain? To modify Endsley's definition, it is postulated that it means:

> *The perception of the physical, digital, and human elements within the content generator, content, conduit, and/or repository battlespaces of the IW environment, during a volume of time; followed by the comprehension of the meaning of the elements, and the projection of their status in the near future.*

In MIW, all the SA elements would be those specifically supporting maritime activities and operations.

The changes to the Endsley definition may impact the design of future decision support systems by bringing awareness to the needs of MIW. For example, those who generate a Recognized Maritime Picture (RMP) may decide to include information aspects in the picture that have not been included previously or might want to generate a separate Recognized Maritime Information Picture. This would impact the design of future systems supporting RMP generation. However, the level of importance MIW SA has and whether the design of a decision support system needs to be altered, depend on the needs of the mission and mandate that the decision support systems are supporting.

5. AN EXAMPLE

Imagine someone is tasked with providing situation awareness specifically regarding access within the four MIW battlespaces for a specific maritime mission. The general Venn diagram regarding access might look something like Figure 2. We consider here the part of the Venn diagram where the Canadian Armed Forces (CAF) and the adversary both have access, or are suspected to both have access, to the same things. Table 1 gives fictitious examples of information that, in the context of the example, is being used to build MIW SA. The information is organized based on the battlespaces and SA elements discussed in this paper. For clarity, only the Digital-Content Generator box has more than one SA-building report, but in reality this might not be the case.

Table 1. The information battlespace versus the types of situation awareness elements found in IW. A blank box implies there is nothing to report.

	Content generator	Content	Conduit	Repository
Physical SA elements	Adversary known to gain physical access to coastal AIS receiver network. Monitoring via commissionaire in progress. No suspicious activity in last 24 hours.		Adversary known to gain access to farm under which digital fibre is laid. Monitoring via satellite in progress. No suspicious activity in last 24 hours.	Suspicious access to room containing database servers at 03:07. Records indicate they left the room at 03:20. Investigation in progress.
Digital SA elements	Pattern of life algorithm used to guide surveillance tasks was confirmed to be altered by a hostile outside entity. Monitoring of algorithm code in progress. No suspicious activity in the last 24 hours. Data provider known to also sell to adversary has stopped providing data since 15:08.	Modified documents placed on a lightly protected CAF network have not yet been downloaded.	Unclassified network was infiltrated by unknown entity at 04:22 and then kicked off the network at 04:23. Investigation in progress, but initial findings suggests an adversary sympathizer actor.	
Human SA elements	Data analyst reports being approached by suspicious individual at a bar Tuesday PM. Background check of the individual in progress but initial findings indicates they might belong to an adversary cell.	See Content generator note.		

While the example is simply for illustrative purposes, it should be stated that if the investigation mentioned in the Physical-Repository box results in discovering it was a trusted CAF member who entered the room, that report might be moved to the CAF/Task Group access list to maintain awareness. Other investigative findings might also move information to another place in the Venn diagram in Figure 2.

However, the task and the Venn diagram are merely being used to show how information can be categorized. All the captured information in Table 1 helps form the MIW SA regarding access and can contribute to a Recognized Maritime Information Picture.

6. CONCLUDING REMARKS

Further research is required to validate that the model outlined in this paper is correct and useful. One test of its accuracy will be to identify an actual maritime mission/operation and identify all the elements of the information environment that must be catalogued to achieve the required SA for activities within that mission/operation. The mandate to maintain a recognized maritime picture and common operating picture appear to be adequate initial test subjects. In this situation, monitoring the content generators, content, conduits, and repositories, to ensure continuous and accurate information would be a large part of maintaining MIW SA for that mandate. The SA elements would likely be dominated by physical and digital elements, with minimal human elements.

REFERENCES

[1] Blakeley, D., "Information as War," Royal Canadian Navy, Crowsnest, 6-7 (2017).

[2] Endsley, M. R., "Situation awareness global assessment technique (SAGAT)," Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, 3, 789-795 (1988).

[3] Porche, I., Paul, C., York, M., Serena, C. C. and Sollinger, J. M., [Redefining information warfare boundaries for an army in a wireless world], Rand Corporation, (2013).

[4] Hazen, M. G., Isenor, A., Desharnais, F. and Randall, T., "Characteristics of Information Warfare: The Battle for the Narrative," 22nd International Command and Control Research and Technology Symposium, 1-14 (2017).

[5] Liu, Z., Yang, D.-s., Wen, D., Zhang, W.-m. and Mao, W., “Cyber-physical-social systems for command and control,” IEEE Intelligent Systems, 26(4), 92-96 (2011).

[6] Yan, C., Fu, K. and Xu, W., “On Cuba, diplomats, ultrasound, and intermodulation distortion,” Computers in biology and medicine, 104, 250-266 (2019).