# Towards a Semiotic Information Position Framework for Network Centric Warfare

**Topics**

Information and Knowledge Exploration

Information and Knowledge Exploitation

Concepts, Theory, and Policy

**Saša Baškarada**

sasa.baskarada@dsto.defence.gov.au

Joint Systems Research

Joint Operations Division

Defence Science & Technology Organisation

506 Lorimer Street

Fishermans Bend Victoria 3207

Australia

+61 3 9626 7916

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JUN 2011** | | **00-00-2011 to 00-00-2011** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Towards a Semiotic Information Position Framework for Network Centric Warfare** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence Science & Technology Organisation,Joint Operations Division,506 Lorimer Street,Fishermans Bend Victoria 3207 Australia,** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.**

14. ABSTRACT
**Semiotics is a field of study that deals with the relationships between representations, intended meanings, and interpretations of signs and symbols. As such, it is of particular relevance to a range of network centric warfare primitives, including data, information, knowledge, awareness, and understanding. In this paper, we apply semiotics to such primitives in the physical, information, cognitive and social network centric warfare domains from the syntactic, semantic, and pragmatic perspectives. As a result, we present the Semiotic Information Position (SIP) framework and evaluate it through a thought experiment involving a simple command and control scenario.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **35** | |

# Abstract

Semiotics is a field of study that deals with the relationships between representations, intended meanings, and interpretations of signs and symbols. As such, it is of particular relevance to a range of network centric warfare primitives, including data, information, knowledge, awareness, and understanding. In this paper, we apply semiotics to such primitives in the physical, information, cognitive and social network centric warfare domains from the syntactic, semantic, and pragmatic perspectives. As a result, we present the Semiotic Information Position (SIP) framework and evaluate it through a thought experiment involving a simple command and control scenario.


# Introduction

On 3 July 1988, the US Navy Cruiser USS Vincennes shot down an Iran Air Airbus A300 civilian airliner over the Strait of Hormuz, killing all 290 passengers on board. A number of investigations have offered a range of possible explanations [17, 24, 36]. For instance, it has been suggested that the Aegis System recycled target tracking numbers, displayed targets using inappropriate symbols, and displayed inconsistent information [20]. One of the key contributing factors was the fact that the USS Vincennes crew incorrectly thought that the Airbus was descending even though the Aegis System correctly indicated that the airplane was ascending [24]. This misinterpretation has been attributed to the fact that the altitude was displayed as a four digit number (e.g. 13,000 feet would appear as 1,300) on a small display off to the side of the primary screen. Furthermore, altitude was embedded in a list of other numbers, including range, speed, bearing, etc. and did not show a trend [46]. Psychological evaluations of the crew members found that *"misjudgements due to stress, and unconscious distortion of data played a major role in the crew's misinterpretation of the Aegis System data"* [20, p. 114]. Recent research has also identified a range of supervisory control deficiencies, which have been attributed to the fact that the ship's crew was in-the-loop (as the lethal agent) as well as on-the-loop (providing supervisory control) [22].

The goal of Network Centric Warfare (NCW) or Network Enabled Capability (NEC) has been described by the UK Secretary of State for Defence as follows: *"to provide the right information, to the right place, at the right time, to enable the right decision, to deliver the right outcome for Defence"* [43, p. 7]. As such, NCW concepts are being embraced by many armed forces around the world. For instance, all of the US Service and Joint Transformation Roadmaps are based on the NCW theory [45], and NEC is at the core of

the transformation of the UK armed forces [42, 43]. Similarly, the Australian 2009 Defence White Paper identifies *"networked capability"* as a key attribute of the future Australian Defence Force (ADF) [7, p. 67], and the Australian NCW Roadmap details milestones for progressive delivery of networked maritime, land, air, and intelligence, surveillance and reconnaissance (ISR) domains [8]. NATO has also identified NEC as a high priority alliance goal [6, p. 1].

The goal of NCW, to reduce ambiguity in situational awareness, has long been a key aspect of military theory. For instance, Clausewitz talked about the *"fog of war"* [12, p. 104] and Sun Tzu wrote *"know thy enemy and know thyself"* [41]. As such, understanding information uncertainty is critical in the context of NCW [13]. While the concept of information superiority has been clearly defined in terms of relative information needs and positions (i.e. information situations and a relative information advantage) [2], relevant dimensions have been revised several times [2, 3, 5]. Yet, ambiguity remains in definitions and potential overlap exists between categories. For instance, correctness and consistency may be defined in terms of required accuracy, and currency and timeliness may be defined in terms of availability or completeness. Similarly, information reach may be defined in terms of accessibility, and quality of interaction may be defined in terms of information richness.

While the existing information position framework may have practical utility, it is not comprehensive, and it does not have a solid theoretical foundation. Furthermore, it ignores much of the meaning-making detail inherent in network centric C2 systems, and it cannot be used to draw inferences between the C2 system components and the resulting situational awareness. Given that humans make meaning and construct their reality through creation and interpretation of signs [10], we use semiotics to comprehensively analyse how relevant NCW primitives are interpreted across the physical, information, cognitive and social domains, and to build a theoretical foundation from the syntactic, semantic, and pragmatic perspectives. The resulting framework, which is aimed at simplifying the formulation of a measure of information superiority, is evaluated through a thought experiment involving a hypothetical Command and Control (C2) scenario.

## Semiotics

Semiotics is a field of study that deals with the relationships between representations, intended meanings, and interpretations of signs and symbols. According to Deely, *"at the heart of semiotics is the realisation that the whole of human experience, without exception, is an interpretive structure mediated*

*and sustained by signs"* [15, p. 5]. As such, modern semiotics studies the construction of meanings with respect to communication as well as to the construction and maintenance of reality [10]. According to Eco, semiotics is concerned with anything that can be taken as a sign [18]. Thus, semiotics involves the study of anything which stands for something else [10]. Swiss linguist Ferdinand de Saussure and American logician and philosopher Charles Sanders Peirce are considered as the founders of semiotics [10]. As a linguist, Saussure was interested in the relationships between words (or signs) and he argued that linguistics should be enclosed by an umbrella science of signs within society [26]. He defined a sign as an object with a meaning, comprising a signifier (signifiant) and a signified (signifié) [10] (see Figure 1). Many semioticians, including Eco, nowadays refer to the signifier and signified as sign-vehicle and meaning, respectively [18]. The signifier carries the meaning and refers to the form that the sign takes. The signified refers to the concept the signifier represents; a mental activity of receiving a signifier represents the actual meaning that is carried. Thus, both the signifier and the signified were considered as psychological (abstract) concepts, which did not necessarily have to be physical. However, according to Eco, Saussure *"did not define the signified any too clearly, leaving it half way between a mental image, a concept and a psychological reality"* [18, p. 14]. Similarly, the signifier is nowadays commonly interpreted as the *"material (or physical) form of the sign"*, which can be *"seen, heard, touched, smelt or tasted"* [10, p. 15]. Saussure also argued that signs only make sense in relation to other signs, and that there is no inherent relationship between the signifier and the signified [38]. Accordingly, he identified two pertinent relationships (see Figure 1). As discussed above, signification (i.e. what is signified) refers to the relationship between the signifier and the signified. Value refers to the relationship between signs. As such, a sign has no absolute value; the value only emerges in relation to other signs.

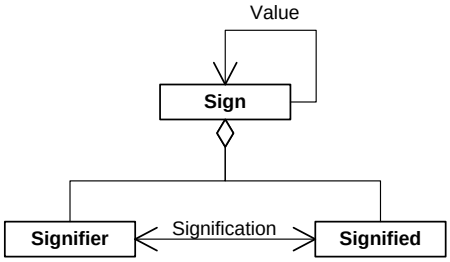



**Figure 1: Saussure's Sign (developed from [38])**

Peirce famously stated that *"nothing is a sign unless it is interpreted as a sign"* [34, p. 308]. He approached semiotics from a process perspective, defining semiosis as *"an action, an influence, which is, or involves, a cooperation of three subjects, such as a sign, its object and its interpretant, this tri-relative influence not being in anyway resolvable into actions between pairs"* [34, p. 411]. Thus, Peirce defined

semiosis as comprising three basic elements (see Figure 2). A sign (representamen) stands to somebody for something in some respect or capacity. An object (referent) is that referred to by the sign. The interpretant is an individual's comprehension of, and reaction to, the sign-object association. Comparable to Saussure's model, Peirce's semiosis elements do not refer to human subjects or physical objects, but to abstract entities [18]. According to Silverman, the representamen is similar in meaning to Saussure's signifier whilst the interpretant is similar in meaning to the signified [39]. Peirce's object (referent) does not have an equivalent concept in Saussure's model.

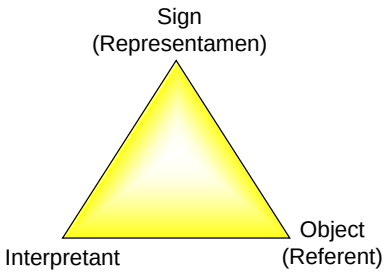



**Figure 2: Semiosis (developed from [34])**

The American philosopher Charles W. Morris defined semiosis as *"a process in which something is a sign to some organism"* [30, p. 366]. He extended Peirce's semiotics by focusing on the relationships between signs and other signs, signs and objects, and signs and interpretants [29]. As a result he proposed three complementary areas of study. Syntactics (or syntax) is the study of the formal or structural relations between signs (representaments). Semantics is the study of the relations of signs to objects which they stand for (representament to referent). As such, semantics deals with rules that state the conditions under which signs apply to objects. According to Fiordo, *"signs denote whatever conforms to the stipulated condition of the semantic rule, and the rule determines the class or kind of things denoted"* [19, p. 58]. Pragmatics is the study of the relation of signs to interpreters (representament to interpretant). For instance, pragmatics deals with rules which state the conditions in the interpreters under which the sign vehicle is interpreted as a sign [19]. However, according to Zemanek, syntactics, semantics, and pragmatics are difficult, if not impossible, to consider in isolation from each other [47]. For instance, pragmatics is always applicable since *"there is always an observer and because no language [or sign system] makes sense without interpretation"* (p. 141). Similarly, semantics is always applicable as well; *"unless we play a meaningless game with characters [or signs]"*. If semantics were to be formalised independently of syntactics one would require a metalanguage, which in itself would carry semantics and syntactics. Similarly, due to the difficulty of separating form and meaning, considering syntactics without a reference to semantics is also difficult.

It is important to note that a number of Defence conferences and workshops were influenced by semiotics in the mid 1990's [1]. Furthermore, some attempts have already been made to apply Morris' work to domains of NCW and information quality. For instance, Mittal et al. [27] proposed syntactic, semantic, and pragmatic linguistic levels of interoperability for network-centric modelling and simulation (see Table 1). Similarly, Price and Shanks used Morris' categorisations to develop a semiotic information quality framework [35]. Accordingly, they proposed three semiotic information quality categories. The syntactic category describes the degree to which data conform to metadata. The semantic category describes the degree to which data correspond to represented external phenomena. The pragmatic category describes the degree to which data are suitable for a given use. Several seminal NCW publications make only passing remarks about semantic and do not address pragmatics at all [2, 4, 6, 44].

**Table 1: Linguistic Levels of Interoperability (developed from [27, p. 11])**

| **Level** | **Objective** | **Example** |
|---|---|---|
| Pragmatic:<br>how information in messages is used | The receiver reacts to the message in a manner that the sender intends | An order from a commander is obeyed by the troops in the field as the commander intended. |
| Semantic:<br>shared understanding of meaning of messages | The receiver assigns the same meaning as the sender did to the message. | An order from a commander to multi-national participants in a coalition operation is understood in a common manner despite translation into different languages. |
| Syntactic:<br>Rules governing composition of messages | The receiver is able to receive and parse the sender's message | A common network protocol (e.g. IPv4) is employed ensuring that all nodes on the network can send and receive data bit arrays adhering to a prescribed format. |

# Network Centric Warfare

Alberts et al. defined Network Centric Warfare (NCW) as: *"an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronisation"* [3, p. 2]. As such, the objective of NCW is increased tempo of operations, responsiveness, and combat effectiveness as well as lower costs and risks [44].

As defined, NCW assumes the following four propositions [3, pp. 193-197] (see Figure 3):

1. A robustly networked force improves information sharing.
2. Information sharing and collaboration enhance the quality of information and shared situational awareness.
3. Shared situational awareness enables self-synchronisation.
4. These, in turn, dramatically increase mission effectiveness.

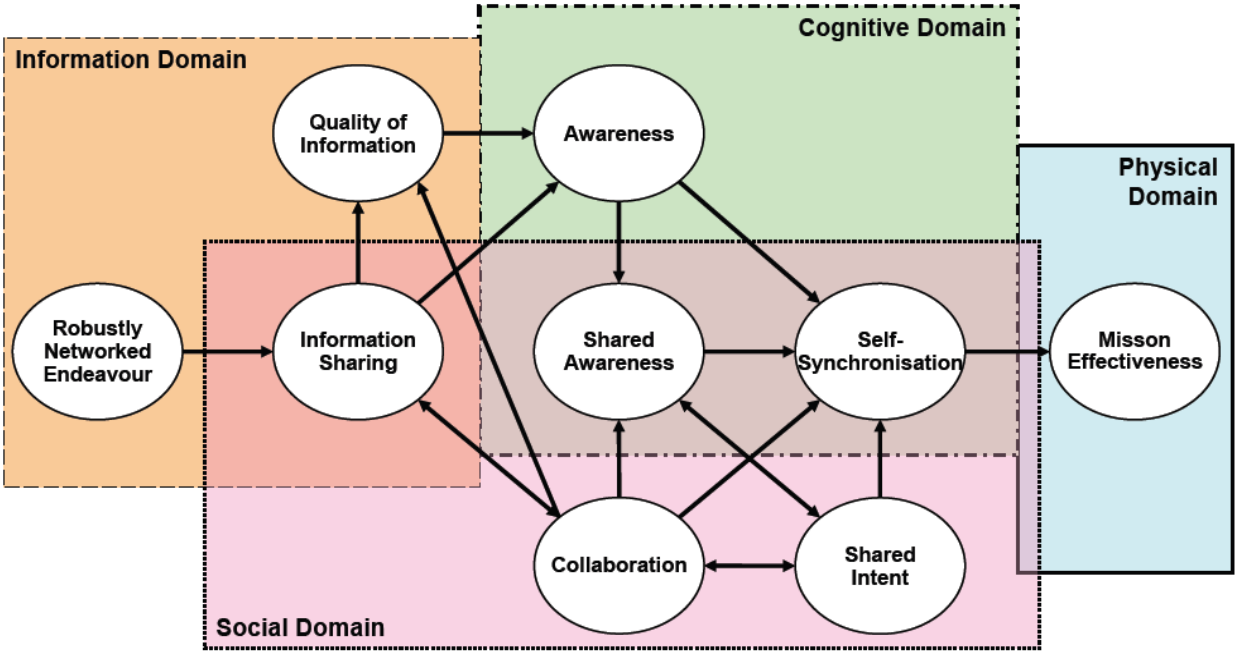



**Figure 3: Network Centric Value Chain (adopted from [6, p. 27])**

A study that investigated the applicability of NCW tenets in Operation Iraqi Freedom (OIF) showed that *"new sensors, extended connectivity, and new information systems enhanced the combat effectiveness of the force"* [9, p. 1]. Recent experimental research has also provided evidence in support of the above hypotheses [25].

NCW was initially defined in terms of three distinct domains [2]. The physical domain is the real-world where physical platforms and communications networks reside. Events take place in the physical domain across the ground, sea, air, and space. The physical battlespace includes sensing, deciding, and acting entities [3]. The information domain is an abstraction of the physical domain, comprising models (i.e. simplified representations) of the physical domain (or the real-world) as well as knowledge from the cognitive domain. It is important to note that such knowledge may or may not correspond to real-world entities. The cognitive domain is *"where perceptions, awareness, understanding, beliefs, and values reside and where, as a result of sensemaking, decisions are made"* [2, p. 13]. In the context of NCW, the cognitive domain represents subjective interpretations of the physical domain that are based on the information domain. Alberts and Hayes subsequently also proposed a social domain, which integrates individual cognitive activities into shared/collective consciousness/awareness [4]. In addition to the four domains, NCW theory also defined a set of key primitives (Table 2), which map to one or more domains each [2].

It has been argued that shared awareness and self-synchronisation lead to emergent behaviour and, thus, that NCW should be considered in terms of Complex Adaptive Systems (CAS) [28, 32]. As such, tagging of agents/entities is of critical importance for identification and organisation. Defined with reference to CAS and directly applicable to NCW, tags *"almost always define the network by delimiting the critical interactions, the major connections"* [23, p. 23]. Metaphors, often applied in the information domain are akin to tagging [14].

As previously stated, research results have indicated that force connectivity positively correlates with force effectiveness [16]. As such, interoperability is not only critical in the physical domain, but also in the information, cognitive and social domains [31, 40] (see Figure 4). However, research has also identified a range of potential obstacles to effective collaboration, including: hierarchical mindsets (traditional flow of orders), resistance to change, system limitations, and the like [11].

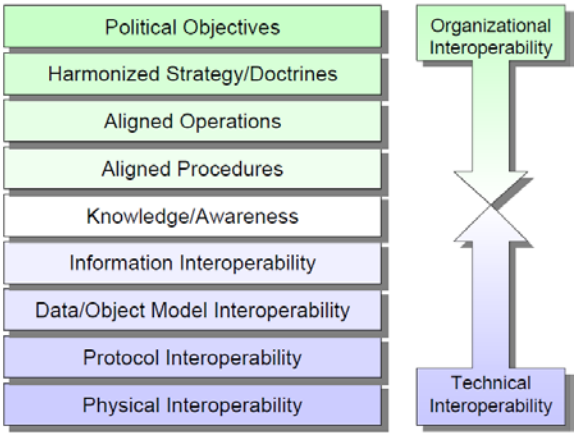



**Figure 4: Layers of Interoperability (adopted from [40, p. 18])**

**Table 2: NCW Primitives (developed from [2, pp. 14-29])**

| Primitive | Description |
|---|---|
| Sensing | Direct sensing takes place when humans experience an object or event in the physical domain with one of their senses. Indirect sensing takes place when a sensor is employed by a human to facilitate sensing some aspect of the physical domain. |
| Data | Data is a representation of individual facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. |
| Information | Information is the result of putting individual observations (sensor returns or data items) into some meaningful context. |
| Knowledge | Knowledge involves conclusions drawn from patterns suggested by available information. |
| Awareness | Awareness relates to a situation and, as such, is the result of a complex interaction between prior knowledge (and beliefs) and current perceptions of reality. |
| Understanding | Understanding involves having a sufficient level of knowledge to be able to draw inferences about the possible consequences of the situation, as well as sufficient awareness of the situation to predict future patterns. |
| Sharing | Sharing (information/knowledge/awareness) is an interaction that can take place between two or more entities. |
| Collaboration | Collaboration is a process that takes place between two or more entities and implies working together toward a common purpose. |
| Decisions | Decisions are choices about what is to be done. |
| Actions | Actions take place in the physical domain and are triggered by decisions in the cognitive domain that either are directly translated into action or have been transported through the information domain to others. |
| Synchronisation | Synchronisation is the meaningful arrangement of things or effects in time and space. |

Information Superiority, a concept central to NCW, has been defined as *"a state that is achieved when a competitive advantage is derived from the ability to exploit a superior information position"* [3, p. 34]. Alberts et al. went on to argue that *"in military operations this superior information position is, in part, gained from information operations that protect our ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same"* [3, p. 54]. As such, information superiority is a relative concept, dependent on competing information needs and positions (i.e. relative information situations) (see Figure 5).

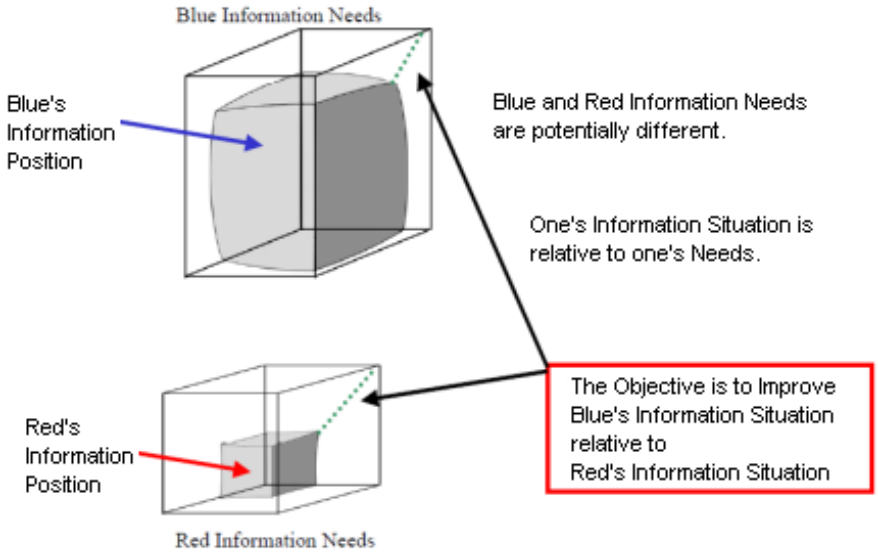



**Figure 5: Relative Information Advantage (developed from [2, p. 108])**

Information position was initially defined in terms of three dimensions: relevancy, timeliness, and accuracy [3]. However, those three dimensions were later revised by Alberts et al. to information richness (information quality), information reach (distribution), and quality of interaction [2] (Figure 6).

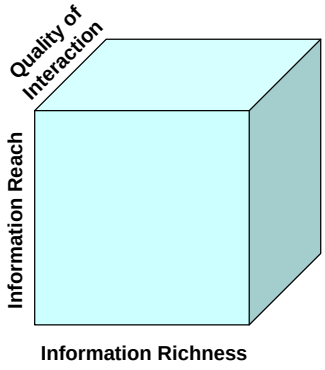



**Figure 6: Dimensions of Information Position (developed from [2, p. 104])**

Information richness comprises eight attributes, including: completeness, correctness, currency, accuracy, consistency, relevance, timeliness, and assurance. Information reach deals with the number and variety of people, work stations, or organisations that can share information. Quality of interaction refers to the nature of the interaction among actors. It deals with data/text/voice exchanges, static/dynamic images, assurance, delay, and so on. However, there is much ambiguity in definitions and potential overlap between categories. A fourth dimension, information security, was later also added to the framework [5] (see Figure 7).

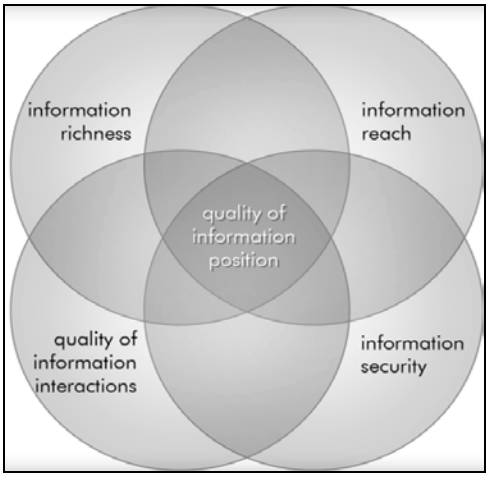



**Figure 7: Quality of Information Position (adopted from [5, p. 142])**

## Towards the Semiotic Information Position Framework

While the concept of relative information advantage (see Figure 5) has been well understood for a long time and proven throughout history [2], the dimensions of the relevant information position have been proposed in an ad hoc manner and, as a result, they have been revised several times [2, 3, 5]. Furthermore, the relative information advantage has been constrained only to the information domain [2, p. 53], whereas it is clearly dependant on data from the physical domain and on interpretations in the cognitive and social domains. Furthermore, since semiosis may be mediated by thought (through a living organism) [33], or by artificial intelligence (computational semiotics) [37], the semiotic triangle (see Figure 2) needs to be applied to each of the NCW domains.

As such, sensing entities in the physical domain (indirect sensing) interpret signs (physical phenomena) from their environment and generate relevant data elements, which are then passed to the information domain. The information domain then interprets and integrates such data elements, potentially

received from a heterogeneous set of sensing entities from the physical domain, and generates new models (i.e. information and knowledge) suitable for human comprehension. Next, people interpret any such models in order to derive knowledge and situational awareness as well as to inform their decision making in the cognitive domain. Finally, people interact with other people (potentially from different services, organisations, or nations) to generate shared awareness and understanding.

Syntactic, semantic, and pragmatic rules apply to each of the domains, and each application of the semiotic triangle introduces potential opportunities for misinterpretation. As a result, it is critical to analyse one's information position in terms of relevant NCW primitives across all four domains from the syntactic, semantic, and pragmatic semiotic perspectives. Accordingly, we propose the Semiotic Information Position (SIP) framework shown in Figure 8. Table 3 shows a preliminary instantiation of this framework, which aims to provide an initial explanation of some relevant relationships.

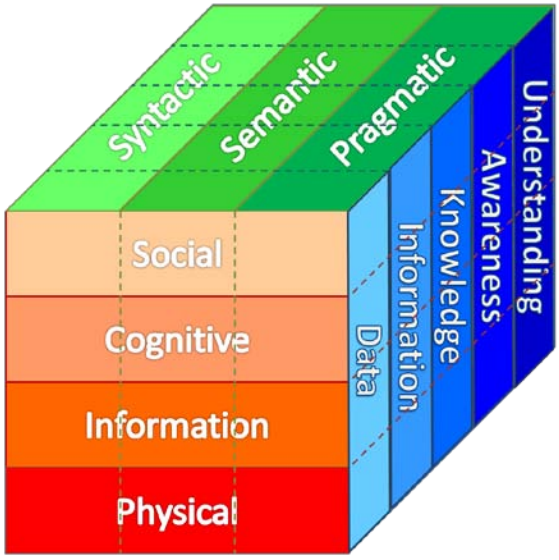



**Figure 8: Semiotic Information Position (SIP) Framework**

**Table 3: Preliminary Instantiation of the Semiotic Information Position (SIP) Framework**

| | | Semiotic Perspective | | |
|---|---|---|---|---|
| | | **Syntactic** | **Semantic** | **Pragmatic** |
| **NCW Domain** | **Social** | Deciding and acting entities have the ability to:<br>• perceive relevant **knowledge** elements;<br>• recognise the types of such elements;<br>• recognise relevant configurations of such elements; and<br>• encode explicit **knowledge** into **knowledge** elements. | Deciding and acting entities have the ability to:<br>• interpret relevant **knowledge** elements to inform **shared situational awareness**;<br>• interpret relevant **knowledge** elements and situational **awareness** to inform **shared understanding**;<br>Based on different configurations of such **knowledge** elements, deciding and acting entities have the ability to generate different interpretations of each **knowledge** element. | Based on their **shared situational awareness** and **shared understanding**, deciding and sensing entities have the ability to generate different interpretations of same **knowledge** elements. |
| | **Cognitive** | Deciding and acting entities have the ability to:<br>• perceive relevant **knowledge** elements;<br>• recognise the types of such elements;<br>• recognise relevant configurations of such elements; and<br>• encode explicit **knowledge** into **knowledge** elements. | Deciding and acting entities have the ability to:<br>• interpret relevant **knowledge** elements to inform situational **awareness**;<br>• interpret relevant **knowledge** elements and situational **awareness** to inform **understanding**;<br>Based on different configurations of such **knowledge** elements, deciding and acting entities have the ability to generate different interpretations of each **knowledge** element. | Based on their situational **awareness** and **understanding**, deciding and sensing entities have the ability to generate different interpretations of same knowledge elements. |
| | **Information** | The information system has the ability to:<br>• receive **data** elements from heterogeneous sensing entities;<br>• recognise the types of such **data** elements;<br>• recognise relevant configurations of such **data** elements;<br>• encode standardised **data** elements;<br>• retrieve standardised **data** elements;<br>• encode relevant **information** elements;<br>• retrieve relevant **information** elements;<br>• recognise the types of such **information** elements;<br>• recognise relevant configurations (patterns) of such **information** elements;<br>• encode relevant **knowledge** elements;<br>• retrieve relevant **knowledge** elements;<br>• recognise the types of such **knowledge** elements;<br>• recognise relevant configurations of such **knowledge** elements; and<br>• encode such **knowledge** elements into **knowledge** elements suitable for human comprehension. | • The information system has the ability to interpret heterogeneous **data** elements into standardised **data** elements.<br>• Based on different configurations of **data** elements, the information system has the ability to generate different interpretations of each **data** element.<br>• Based on different configurations (patterns) of relevant **information** elements, the information system has the ability to generate meaningful **knowledge** elements. | Based on its situational **awareness**, the information system has the ability to:<br>• generate different interpretations (i.e. meaningful **information** elements) from same **data** elements.<br>• generate different interpretations (i.e. meaningful **knowledge** elements) from same patterns of **information** elements. |
| | **Physical** | Sensing entities have the ability to:<br>• perceive relevant physical phenomena;<br>• recognise the types of such phenomena;<br>• recognise relevant configurations of such phenomena; and<br>• encode relevant **data** elements. | • Sensing entities have the ability to interpret relevant physical phenomena into **data** elements.<br>• Based on different configurations of such phenomena, sensing entities have the ability to generate different interpretations of each phenomenon. | Based on their situational **awareness**, sensing entities have the ability to generate different interpretations of same physical phenomena. |

# Thought Experiment

To illustrate the framework described above, let us consider a simple Command and Control (C2) thought experiment. The Observe, Orient, Decide, and Act (OODA) loop, initially proposed in the context of air-to-air combat, represents a traditional view of C2 and has been used for decades as the basis of both analysis and training [2, 21] (see Figure 9). While it greatly simplifies the joint hierarchical model underlying military operations, it is a useful tool for supporting high-level analyses of network centric C2 scenarios. As Figure 9 shows, observations originate in the physical domain, where they are encoded into the information domain. People then decode those observations from the information domain to inform their shared situational awareness and understanding, which aid their decision making. Such decisions are then encoded in the information domain before being actioned in the physical domain.

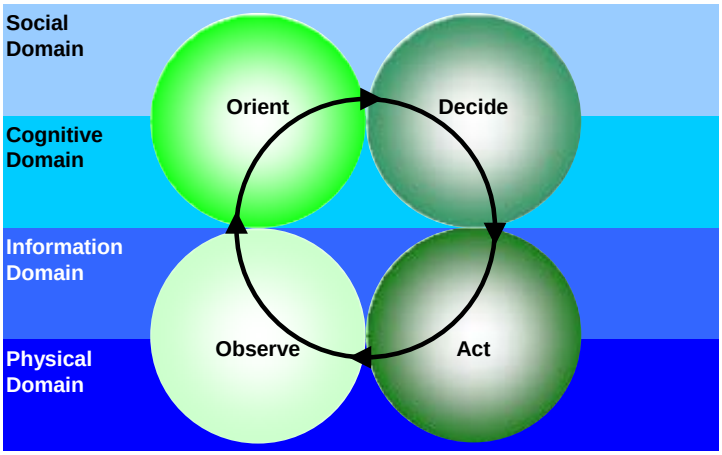



**Figure 9: Traditional View of C2, OODA Loop (developed from [2, p. 132])**

Let us now evaluate our SIP framework through a simple hypothetical C2 scenario (Figure 10). Let us imagine that two heterogeneous radars (sensing entities), a passenger plane, and an anti-aircraft missile are situated in the physical domain. Furthermore, three military personnel – one Commanding Officer (CO) and two operators – are situated in the cognitive domain (for the sake of simplicity, let us ignore the fact that their bodies are in the physical domain; let us for now just focus on their minds). Similarly, the server shown in the information domain should be considered as representative of the information it stores. Any commercial airliners are allowed to fly through; however, any incoming enemy fighter aircraft should be destroyed with the missile.

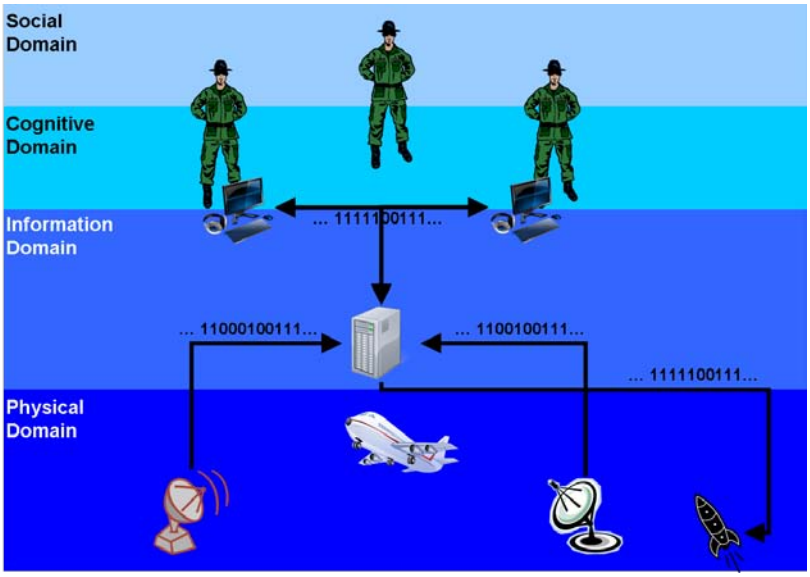



**Figure 10: A Hypothetical C2 Scenario**

The existing information position framework (see Figure 6 and Figure 7) ignores much of the meaning-making detail involved in this hypothetical C2 scenario. As such, it cannot be used to draw inferences between the C2 system components and the resulting situational awareness. For instance, the existing framework may not have been very useful in an investigation trying to explain the USS Vincennes incident mentioned in the introduction. On the other hand, our SIP framework explains cross-domain interpretations and it can be used to critically analyse and/or inform situational awareness in terms of the C2 system components and their capabilities and interactions. Let us now analyse this scenario in the context of the SIP framework in order to illustrate the complexities involved in each domain. Errors in any of the following aspects may lead to misinterpretations of the real-world, thus, increasing the ambiguity in situational awareness.

From the syntactic perspective, radars need to be able to sense incoming signals and recognise their types (e.g. signal noise, echo, clutter, etc.). Furthermore, radars need to be able to recognise relevant configurations of such signals (e.g. echoes usually arrive in a specific pattern), and they need to be able to encode relevant signals for transmission to the server (e.g. through XML, TCP, IP, etc.). From the semantic perspective, radars need to be able to interpret the signals they have received (e.g. clutter means that the signal is contaminated and can be ignored). They also need to be able to generate different interpretations of each signal based on different configurations of such signals (e.g. if the signal has moved it can be considered as a target, whereas if the signal remains stationary it may be considered as clutter). From the pragmatic perspective, the radars may be able to ignore certain false

positives by cross-referencing them to a ground map. Furthermore, given the complexities involved in radar signal processing, it needs to be noted that there are many more potential syntactic, semantic, and pragmatic implications; the above is a very simplified explanation only aimed at illustrating the relevance of the SIP framework.

From the syntactic perspective, the server needs to be able to receive communication from heterogeneous radars (i.e. there needs to be a common communication protocol as well as a common ontology). From the semantic perspective, the server needs to be able to integrate such heterogeneous data into a standardised model as well as to interpret it into information (e.g. range, altitude, direction, or speed) and knowledge (e.g. variation in altitude may indicate ascent or descent). From a pragmatic perspective (e.g. based on a commercial flight schedule), the server may be able to ignore certain objects (or at least identify them as low threats). Finally, the server needs to be able to encode all of this information and knowledge into models suitable for human understanding (e.g. combinations of visual and audio signals/signs).

From the syntactic perspective, the two operators need to be able to recognise and differentiate different audio and visual signals received from the information domain (e.g. flashing lights, coloured dots on the computer screen, or a sound alarm). From the semantic perspective, they need to be able to interpret the meanings of such models to inform situational awareness (e.g. “are we under attack?”), and understanding (e.g. “what may happen if we fire the missile?”). For instance, a flashing light may indicate a warning, whereas a flashing light combined with a sound alarm may indicate immediate danger. From the pragmatic perspective, situational awareness and understanding may lead to different interpretations of same audio/visual signals. For instance, prior intelligence may have a significant influence on peoples’ interpretations of such signals (e.g. an anticipation of an enemy aircraft may influence false-positive identifications). Furthermore, experience of personnel, uniqueness of audio/visual signals, lack of confidence in equipment or leadership, and length of time available to evaluate such signals have also been identified as factors with potential negative impacts on subjective interpretations [36]. As a result, establishing shared awareness is essential to any effective decision making.

Considering our hypothetical scenario, the two operators need to be able to establish a level of shared awareness in order to effectively inform the CO. As such, the two operators need to be able to encode their individual situational awareness states using a shared ontology, language, and communication

protocol. For instance, operators from the same service and nation, sitting in the same room, may be able to verify their individual interpretations through verbal communication (e.g. “are you seeing what I am seeing?”); however, operators from different services and/or different nations, sitting in two different building, may need to be able to communicate their individual situational awareness states through the information domain (e.g. using pictorial representations). From the pragmatic perspective, any inconsistencies in individual situational awareness states may lead to re-evaluation of previous interpretations, thus, potentially increasing consensus and enhancing shared situational awareness.

## Discussion

Direct sensing (e.g. when a person directly observes an object by looking at it) is usually preferred to indirect sensing (e.g. using a sensor, such as radar). However, for obvious reasons, direct sensing is not always practical or even possible and, thus, indirect sensing is more commonly used in the context of NCW. While direct sensing only requires a person to correctly interpret what they are sensing, indirect sensing involves multiple interpretations/translation by several entities across all of the NCW domains. As such, indirect sensing introduces additional complexities that need to be considered from the syntactic, semantic, and pragmatic perspectives. Errors in interpretations in any of the domains from any of the perspectives may lead to misinterpretations of reality, leading to ambiguity in situational awareness. The framework presented in this paper provides a sound theoretical foundation for defining and analysing one’s information position in the context of NCW. However, given the lack of empirical validation it is difficult to estimate realistic practical implications.

## Conclusion and Future Research

NCW theory is having a significant impact on a number of military transformations around the globe. The concept of information superiority is at the core of NCW and has been defined in terms of a superior information position. However, relevant dimensions were proposed in an ad hoc manner and, as a result, have been revised several times. Furthermore, the existing information position framework ignores much of the meaning-making detail inherent in network centric C2 systems. As such, it cannot be used to draw inferences between the C2 system components and the resulting situational awareness. Given that people construct their reality through creation and interpretation of signs, this paper has

proposed the SIP framework, which addresses key NCW primitives from the syntactic, semantic, and pragmatic perspectives across all NCW domains. As a result, our SIP framework explains cross-domain interpretations and it can be used to critically analyse and/or inform situational awareness in terms of the C2 system components and their capabilities and interactions.

While the resulting framework provides a sound theoretical foundation, this paper has only provided a preliminary analysis of relevant implications. As a result, there is a need to undertake further work in order to explore key syntactic, semantic, and pragmatic rules for specific NCW scenarios as well as to empirically test them in either a simulated or a real-world environment. Furthermore, situating the SIP framework into the broader literature on situational awareness and decision-making would provide a means to evaluate it in the context of cognitive theory.

## Acknowledgements

The author would like to gratefully acknowledge the thoughtful review and important insights provided by Dr Simon Ng, Ms Vivian Nguyen, and Dr Paul Whitbread. The views expressed in this paper are the views of the author and do not necessarily represent the views of the Australian Department of Defence.

# References

1. AI'95. *Proceeding of the Artificial Intelligence in Defence Workshop*. in *Eighth Australian Joint Conference on Artificial Intelligence*. 1995. Australian Defence Force Academy, Canberra.
2. Alberts, D.S., J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare*. 2001: CCRP.
3. Alberts, D.S., J.J. Garstka, and F.P. Stein, *Network Centric Warfare*. 2 ed. 1999: CCRP.
4. Alberts, D.S. and R.E. Hayes, *Power to the Edge*. 2003: CCRP.
5. Alberts, D.S. and R.E. Hayes, *Understanding Command and Control*. 2006: CCRP.
6. Alberts, D.S., R.K. Huber, and J. Moffat, *NATO NEC C2 Maturity Model*. 2010: CCRP.
7. AU-DOD, *Defending Australia in the Asia Picific Century: Force 2030*. Defence White Paper. 2009, Canberra, ACT: Australian Government, Department of Defence.
8. AU-DOD, *NCW Roadmap 2009*. 2009, Canberra, ACT: Australian Government, Department of Defence.
9. Cammons, D., J.B.T. III, D.E. Williams, A.Seise, and D. Lindsay, *Network Centric Warfare Case Study*. 2005, Carlisle Barracks, PA US Army War College.
10. Chandler, D., *Semiotics: The Basics*. 2 ed. 2007: Routledge.
11. Cheah, M. and P. Thunholm. *Overcoming Obstacles to Collaboration*. in *15th International Command and Control Research and Technology Symposium*. 2010. Santa Monica, California.
12. Clausewitz, C., *On War*. 2008, Readford, VA: Wilder Publications.
13. Cramer, M.A., J.E. Beach, T.A. Mazzuchi, and S. Sarkani, *Understanding Information Uncertainty within the Context of a Net-Centric Data Model: A Mine Warfare Example.* The International C2 Journal, 2009. **3**(1).
14. Czerwinski, T.J., *Coping with the Bounds: A Neo-Clausewitzean Primer*. 1998: CCRP.
15. Deely, J., *Basics of Semiotics*. 1990, Bloomington, IN: Indiana University Press.
16. Deller, S., S.R. Bowling, G.A. Rabadi, A. Tolk, and M.I. Bell, *Applying the Information Age Combat Model: Quantitative Analysis of Network Centric Operations.* The International C2 Journal, 2009. **3**(1).
17. Dotterway, K.A., *Systematic Analysis of Complex Dynamic Systems: The Case of USS Vincennes*. 1992, Monterey, CA: Naval Postgraduate School.
18. Eco, U., *A Theory of Semiotics*. 1979: Indiana University Press.
19. Fiordo, R.A., *Charles Morris and the Criticism of Discourse*. 1977: John Benjamins Publishing Company.
20. Fisher, C.W. and B.R. Kingma, *Criticality of Data Quality as Exemplified in Two Disasters.* Information & Management, 2001. **39**: p. 109-116.
21. Grant, T. and B. Kooter, *Comparing OODA & other models as Operational View C2 Architecture Topic: C4ISR/C2 Architecture*, in *10th International Command and Control Research and Technology Symposia (ICCRTS)*. 2005.
22. Hew, P., E. Lewis, P. Radunz, and S. Rendell. *Situation Awareness for Supervisory Control: Two Fratricide Cases Revisited*. in *15th International Command and Control Research and Technology Symposium*. 2010. Santa Monica, California.
23. Holland, J.H., *Hidden Order: How Adaptation Builds Complexity*. 1995, Reading, MA: Addison-Wesley.
24. Klein, G.A., *Sources of Power: How People Make Decisions*. 1999: The MIT Press.
25. Manso, M. and B. Manso. *N2C2M2 Experimentation and Validation: Understanding Its C2 Approaches and Implications*. in *15th International Command and Control Research and Technology Symposium*. 2010. Santa Monica, California.
26. Mick, D.G., *Consumer Research and Semiotics: Exploring the Morphology of Signs, Symbols, and Significance.* The Journal of Consumer Research, 1989. **13**(2): p. 196-213.
27. Mittal, S., B.P. Zeigler, and J.L. Risco-Martin, *Implementation of a Formal Standard for Interoperability in M&S/Systems of Systems Integration with DEVS/SOA.* The International C2 Journal, 2009. **3**(1).
28. Moffat, J., *Complexity Theory and Network Centric Warfare*. 2003: CCRP.
29. Morris, C.W., *Foundations of the Theory of Signs*. 1938, Chicago: Chicago University Press.
30. Morris, C.W., *Signs, Language and Behavior*. 1946, New York: Prentice-Hall.
31. Ng, S., D. Hall, R. Gani, and T. Clark. *Integration: Why Do It? What Does It Mean?* in *10th International Command and Control Research and Technology Symposia*. 2005. Washington, DC.

32. Ng, S. and D. Lowe. *The Implications of Complex Adaptive Systems Thinking for Future Command and Control*. in *11th International Command and Control Research and Technology Symposia*. 2006. Cambridge, UK.
33. Odgen, C.K. and I.A. Richards, *The Meaning of Meaning*. 8 ed. 1923, New York, Harcourt: Brace & World, Inc.
34. Peirce, C.S., *The Essential Peirce, Volume 2: Selected Philosophical Writings, 1893-1913*. 1998: Indiana University Press.
35. Price, R. and G. Shanks, *A semiotic information quality framework:development and comparative analysis.* Journal of Information Technology, 2005. **20**: p. 88–102.
36. Roberts, N.C., *Reconstructing Combat Decisions: Reflections on the Shootdown of Flight 655*. 1992, Monterey, CA: Naval Postgraduate School.
37. Roy, D., *Semiotic Schemas: A Framework for Grounding Language in Action and Perception.* Artificial Intelligence, 2005. **167**: p. 170-205.
38. Saussure, F.D., *Course in General Linguistics*. 1983, London: Duckworth.
39. Silverman, K., *The Subject of Semiotics*. 1983, New York: Oxford University Press.
40. Tolk, A. *Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability*. in *8th International Command and Control Research and Technology Symposium*. 2003. Washington, D.C.
41. Tzu, S., *The Art of War*. ca. 6th century BC.
42. UK-MOD, *Joint Service Publication 777 - Network Enabled Capability*. 2005: United Kingdom Ministry of Defence.
43. UK-MOD, *NEC: Understanding Network Enabled Capability*. 2009, London, UK: Newsdesk Communications Ltd.
44. USA-DOD, *Network Centric Warfare Department of Defense Report to Congress*. 2001, Washington: CCRP.
45. USA-DOD, *The Implementation of Network-Centric Warfare*. 2005, Washington, DC: USA Department of Defense.
46. Venturi, G. and J. Troost. *An agile, user-centric approach to combat system concept design*. in *10th International Command and Control Research and Technology Symposium*. 2005.
47. Zemanek, H., *Semiotics and Programming Languages.* Communications of the ACM, 1966. **9**(3): p. 139-143.

Australian Government
Department of Defence
Defence Science and
Technology Organisation

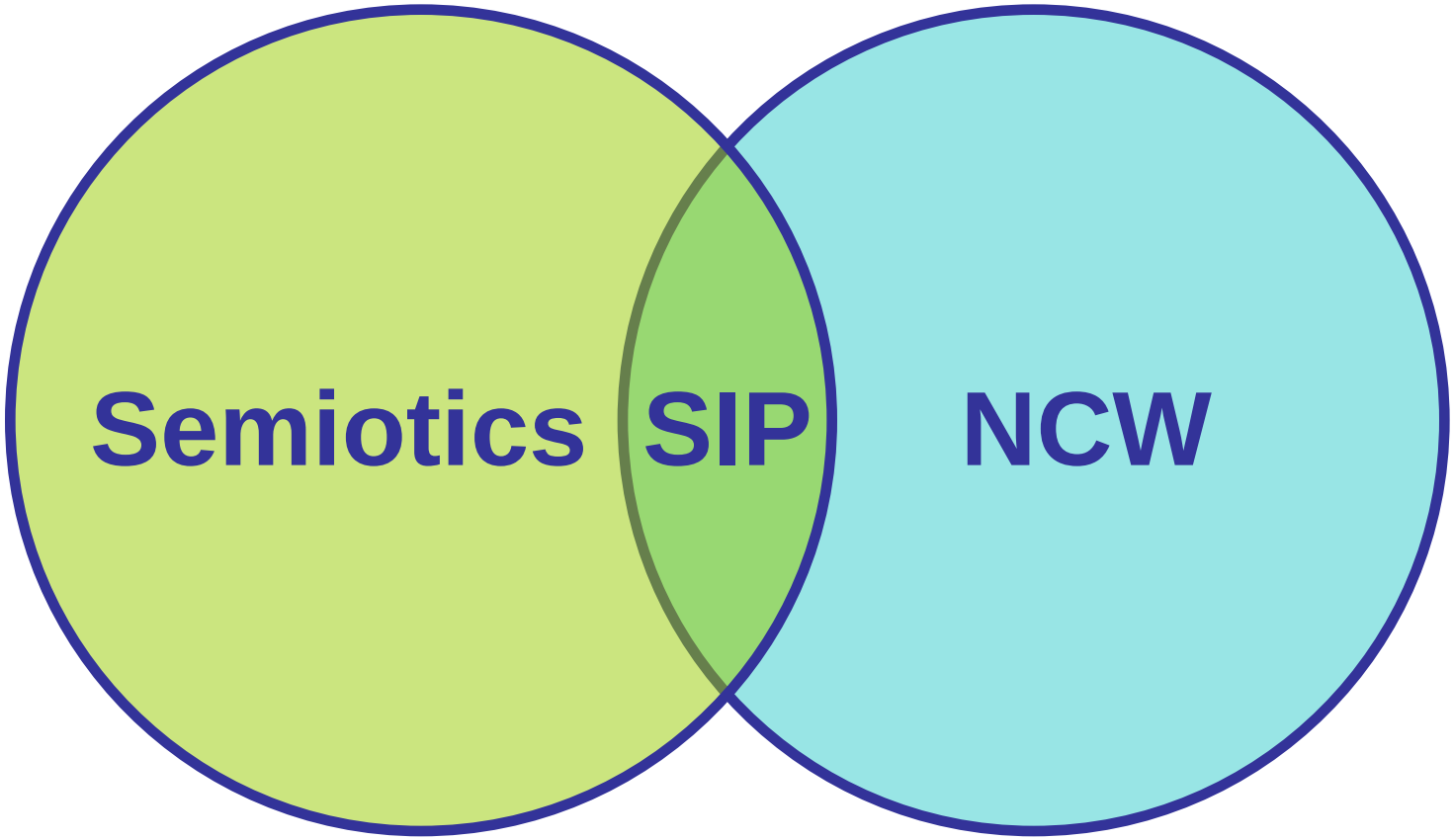
# Towards a Semiotic Information Position Framework for Network Centric Warfare

**Dr Saša Baškarada**
Joint Systems Research
Joint Operations Division
Defence Science & Technology Organisation

16th International Command and Control Research and Technology Symposium (ICCRTS)
Québec City, Canada,
21–23 June 2011

DSTO

# Contents



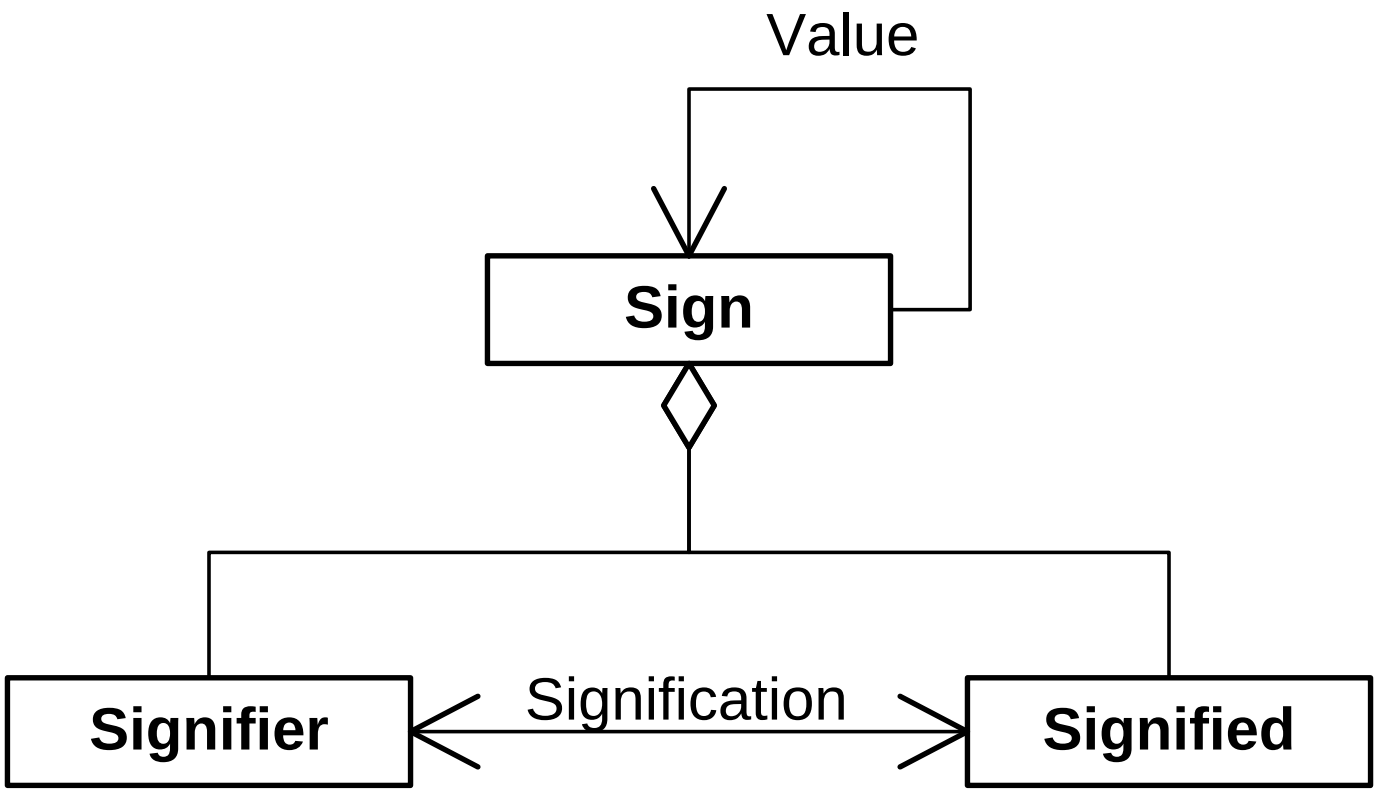

DSTO

# Semiotics

- A field of study that deals with the relationships between representations, intended meanings, and interpretations of signs and symbols.
- Is concerned with anything that can be taken as a sign [1].

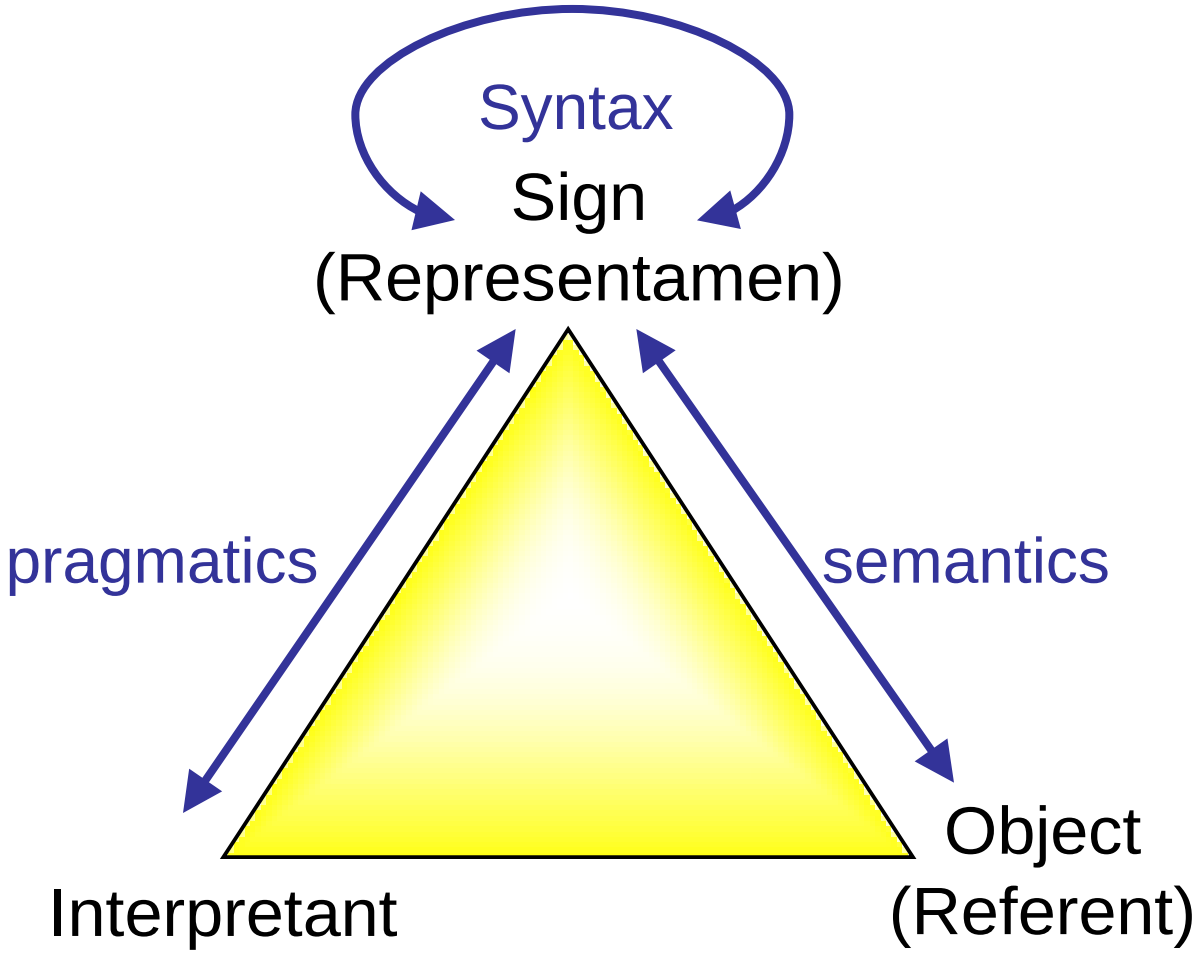
DSTO

# Saussure's Sign



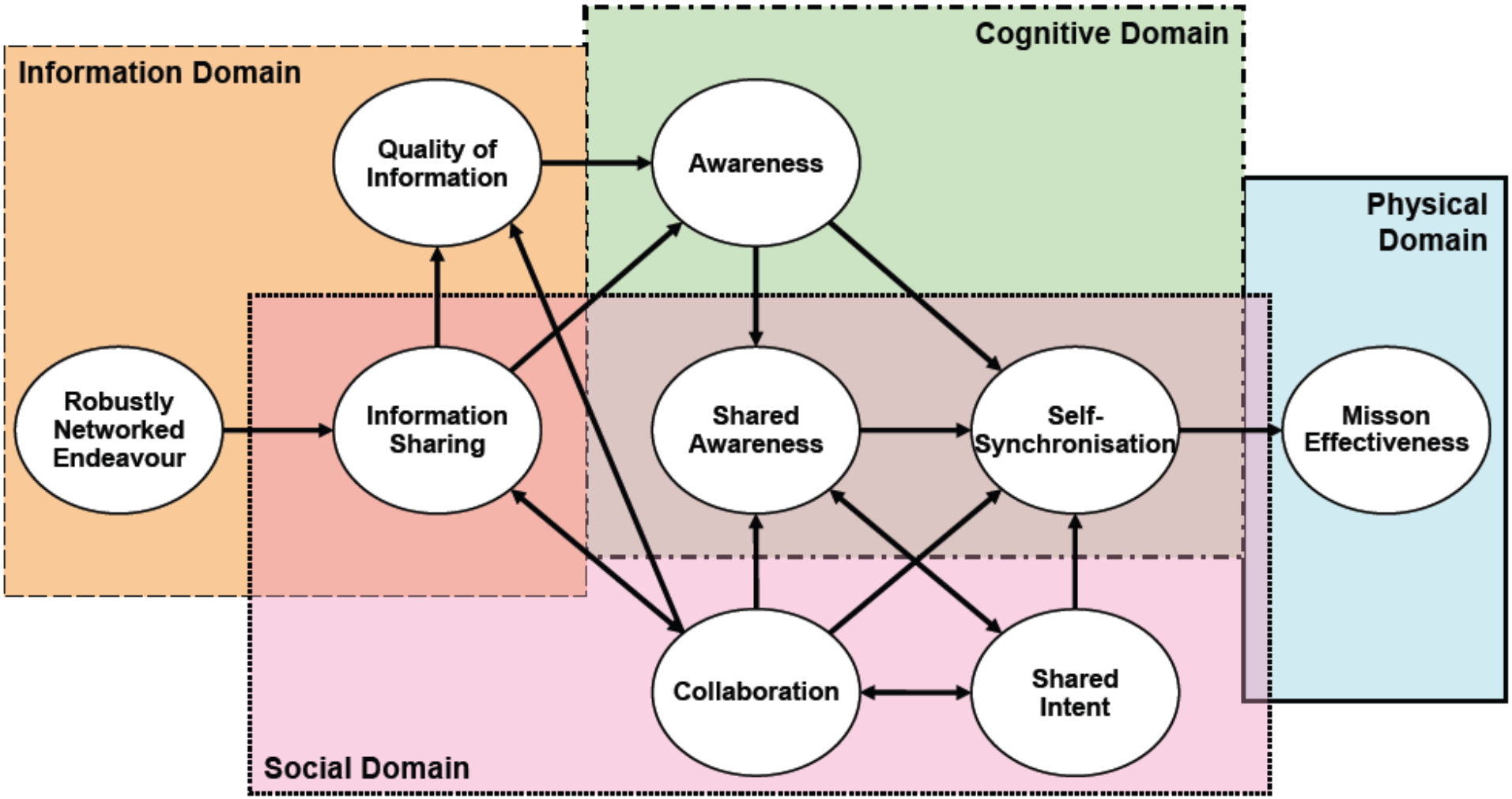

developed from [2]

# Peirce's Semiosis




developed from [3, 4]

# Network Centric Warfare




adopted from [5, p. 27]

# NCW Primitives

Sensing

Data

Information

Knowledge

Awareness

Understanding

Sharing

Collaboration

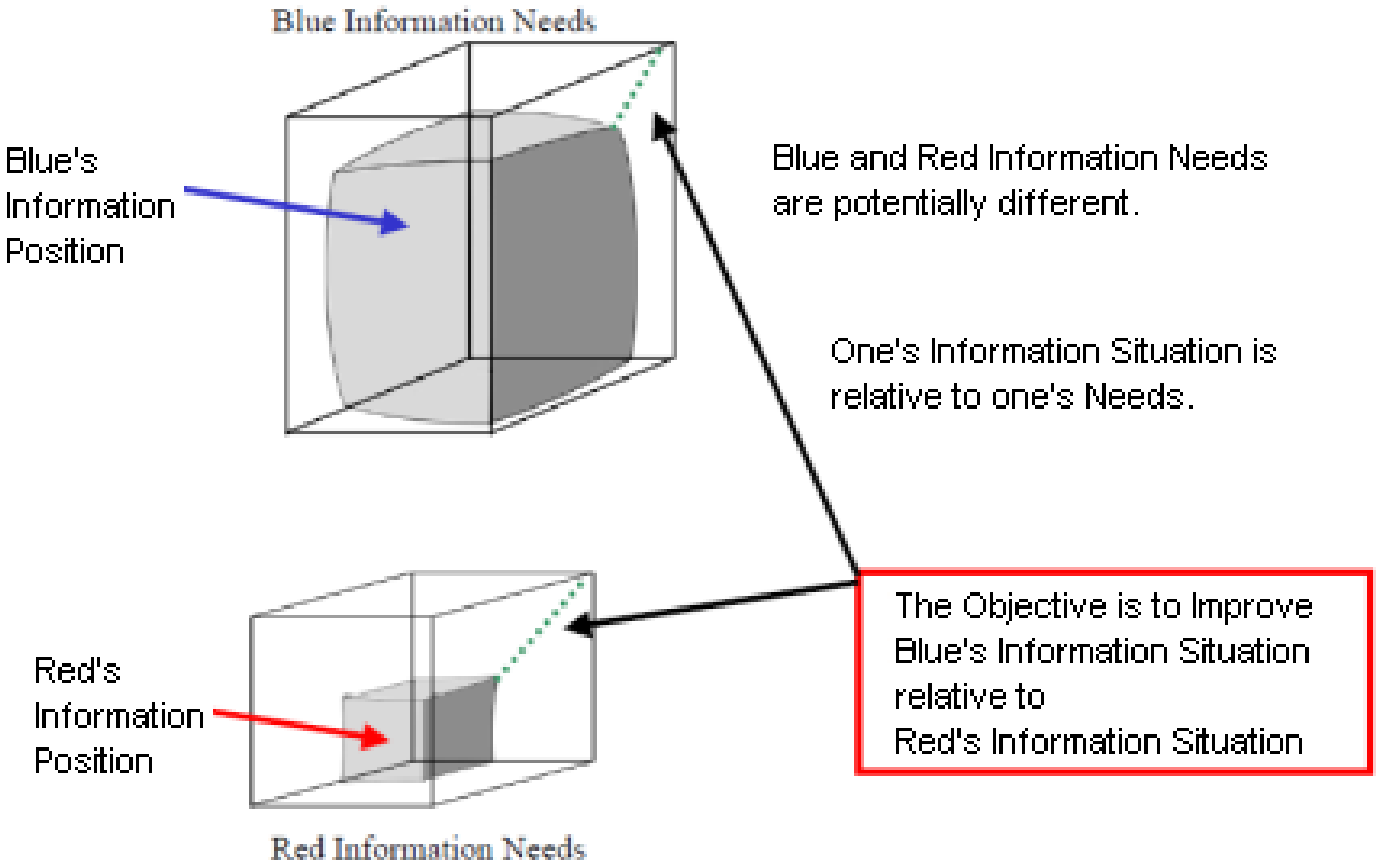
Decisions

Actions

Synchronisation

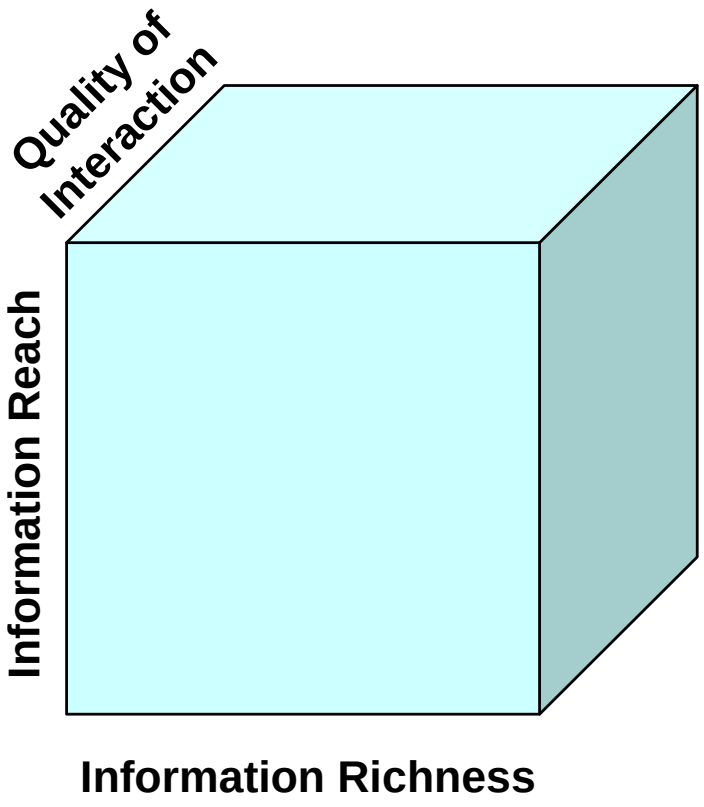
DSTO

# Relative Information Advantage




adopted from [6, p. 108]

# Dimensions of Information Position




developed from [6, p. 104]

## Information Richness

- completeness
- correctness
- currency
- accuracy
- consistency
- relevance
- timeliness
- assurance

## Information Reach

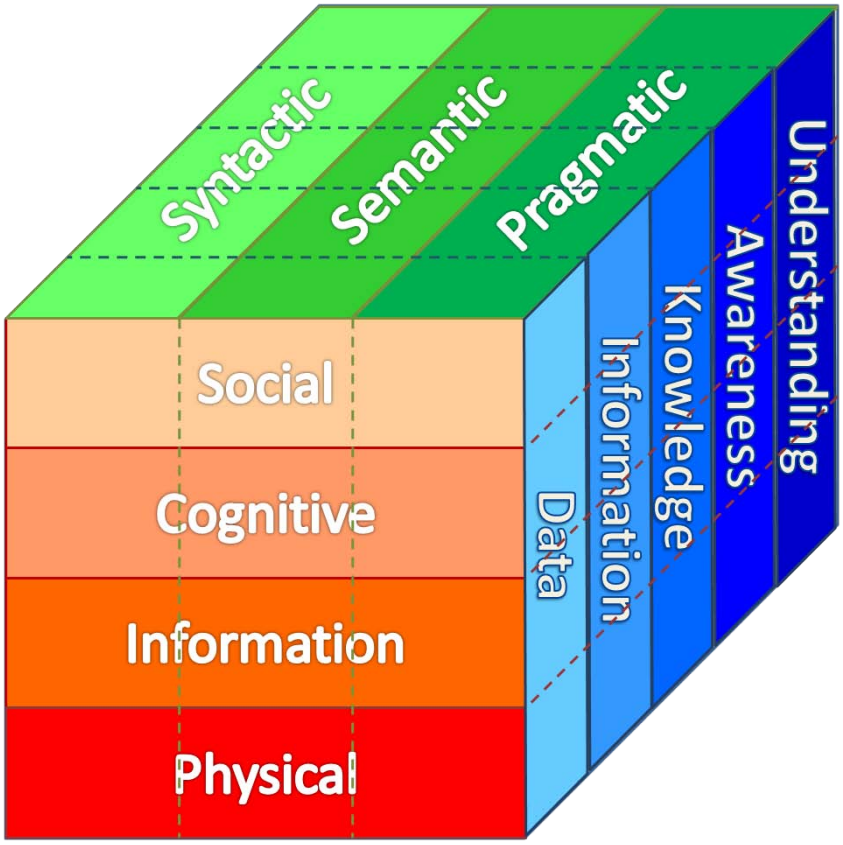
- number and variety of people, work stations, or organisations that can share information

## Quality of Interaction

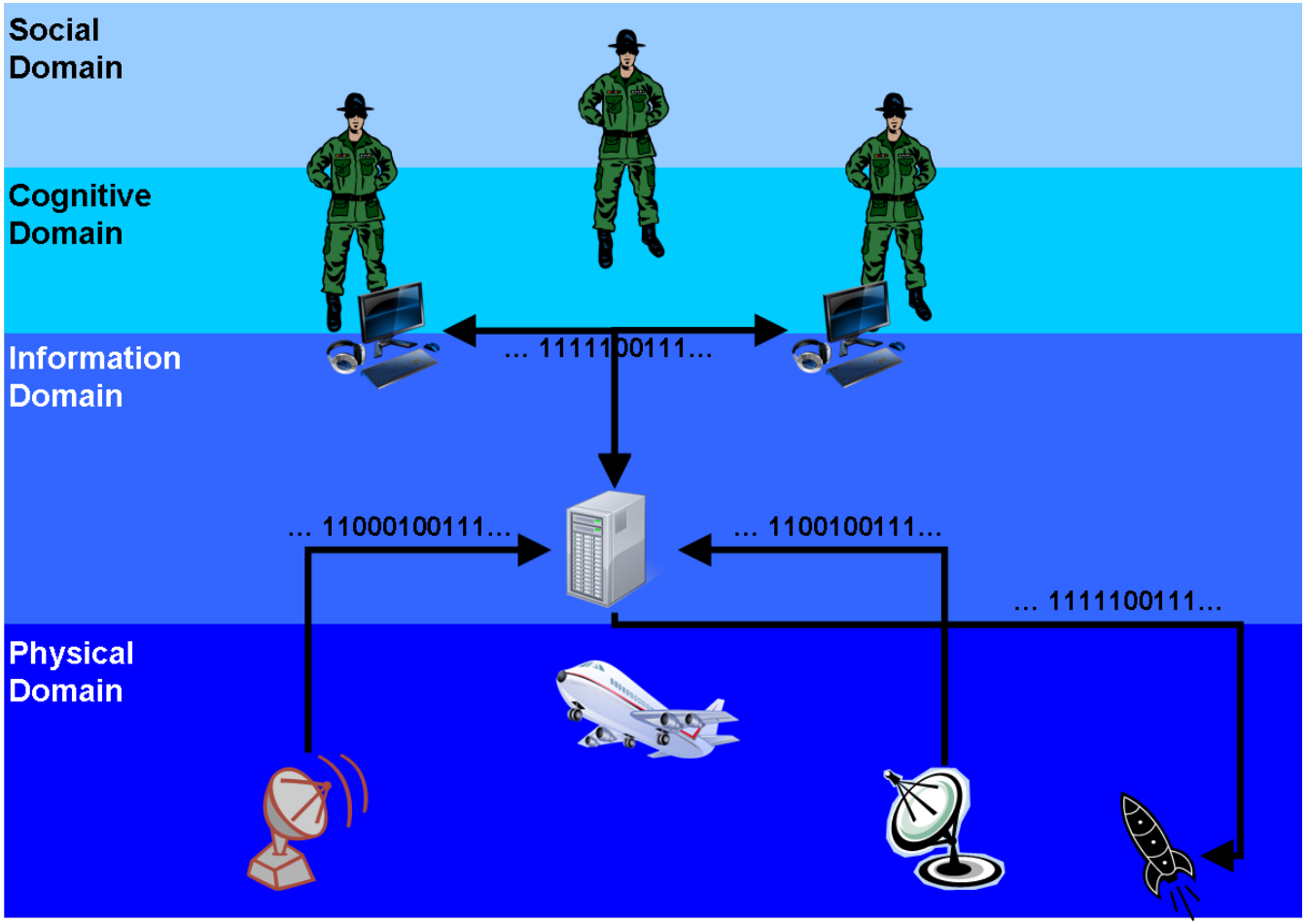
- data/text/voice exchanges
- static/dynamic images

DSTO

# Semiotic Information Position Framework



# Thought Experiment



# Conclusion

- Indirect sensing involves multiple interpretations/ translation by several entities across all of the NCW domains.
- Errors in interpretations in any of the domains from any of the perspectives may lead to misinterpretations of reality, leading to ambiguity in situational awareness.
- The SIP framework explains cross-domain interpretations and it can be used to critically analyse and/or inform situational awareness in terms of the C2 system components and their capabilities and interactions.

DSTO

# Future Research

- Identify key syntactic, semantic, and pragmatic rules for specific NCW scenarios.
- Investigate impact on mission effectiveness.
- Relate to the broader cognitive science literature.

DSTO

# Thank You

DSTO

# References


1. Eco, U., *A Theory of Semiotics*. 1979: Indiana University Press.
2. Saussure, F.D., *Course in General Linguistics*. 1983, London: Duckworth.
3. Peirce, C.S., *The Essential Peirce, Volume 2: Selected Philosophical Writings, 1893-1913*. 1998: Indiana University Press.
4. Morris, C.W., *Foundations of the Theory of Signs*. 1938, Chicago: Chicago University Press.
5. Alberts, D.S., R.K. Huber, and J. Moffat, *NATO NEC C2 Maturity Model*. 2010: CCRP.
6. Alberts, D.S., J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare*. 2001: CCRP.