Understanding Cyberspace Through Cyber Situational Awareness

Mr. B.R. Parish and Prof. B.K. Madahar
Defence Science and Technology Laboratory
Cyber and Information Systems Division
Salisbury, Wiltshire SP4 0JQ
UNITED KINGDOM

brparish, bkmadahar@dstl.gov.uk

ABSTRACT

This paper provides discussion around commonly used, but often misunderstood, concepts of Cyber Situational Awareness (Cyber SA), relating relevant UK military doctrine to the widely recognised Endsley [1] model of situation awareness (SA). The key finding is that, in the context of UK military, Cyber SA is important but not sufficient. Furthermore that the concept of SA has evolved and been developed for more traditional military operational environments as opposed to the ethereal and more complex Socio-Technical System of Systems(STSOS) environments that define cyberspace, often referred to as the 5th battlespace [2]. This has led to divergent technical views between those who use the Endsley model (e.g. Academia and Industry) and those governed by military doctrine, and supporting models, such as the armed forces.

To close this gap, arguments are provided in the paper to highlight the critical importance of Situational Understanding. That cyberspace 'understanding' is required to support decision making, and 'understanding' is underpinned by SA. There is a need for the community to shift its language and approach to move from a desire to achieve Cyber SA to a desire to achieve (and apply) true cyberspace Understanding within the context of complex STSOS.

Rationale for this approach and current technical thinking is articulated in this paper. It details the challenges facing UK Ministry of Defence (MOD) in understanding cyberspace and developing understanding to operate in (or through) cyberspace.

1.0 BACKGROUND

This paper is not intended to provide a lengthy debate on what may be meant by 'cyberspace' – this is available elsewhere [3]. In many cases the term cyberspace has become a conventional means to describe anything associated with the internet and internet culture; with the advent of wide range of internet enabled consumer technologies cyberspace is, unknowingly to consumers in some cases, growing not only in breadth and diversity, but also in socio-technical complexity.

The following definitions are used by UK MOD [5]:

Cyber	*To operate and project power in and from cyberspace to influence the behaviour of people or the course of events.*
Cyberspace	*An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains.*

Importantly, the MOD definition for cyberspace intentionally includes more than just the internet and associated Information and Communications Technology (ICT) and networking, and as such mirrors diversity in consumer/industrial technology to include control and management systems, such as building management systems (e.g. heating, ventilation, and air conditioning (HVAC) control systems). Additionally, this definition includes the data hosted on such systems. Cyberspace is, therefore, a complex Socio-Technical System of Systems (STSOS) with the connective threads and information fabric enabling and shaping the modern world, its societies, cultures, economies, technologies and industries. It comprises physical, logical and cognitive elements, the digital assets that connect functions and direct data/information/decision flows (see Figure 1) [2]. Unconstrained by borders or geography, cyberspace is omnipresent, it permeates most, if not all, civil and military sectors and is difficult, if not impossible, to regulate and impose national authority on. It is ethereal and complex offering a diversity of opportunities to do good as well as bad. The most serious of which is cyberattack compromising nation's security and defences by exploiting vulnerabilities of people, processes and technologies enabling its digital enterprise (i.e. the STSOS) [2].

Hence in 2015, UK reaffirmed cyber threat as one of the highest level risks (Tier 1) [4] to the security of the UK, and UK MOD treats cyberspace as the fifth operating environment in addition to the land, maritime, air and space environments [5]. As such, MOD aims to preserve its freedom of action and manoeuvre in, or through, cyberspace; prioritising effort and accepting risk where necessary. In order to achieve this it must be able to understand cyberspace and make effective decisions relating to its own, or an adversary's, use of cyberspace. This understanding of the STSOS and its many attributes, see Figure 1, underpins and is critical to decisions and actions.

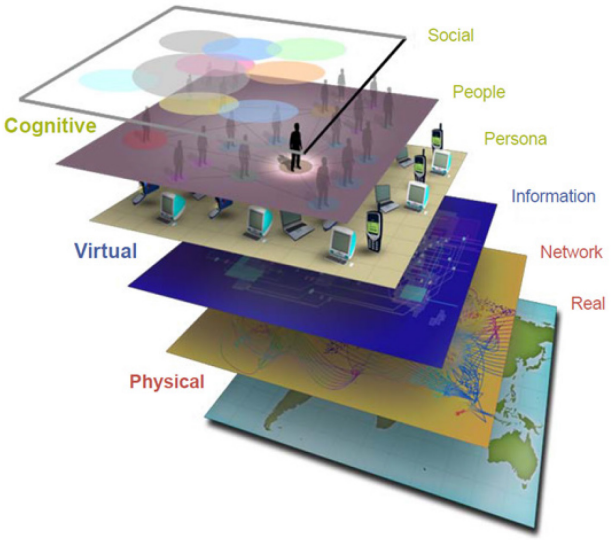

Figure 1: Layered view of cyberspace.

2.0 SITUATIONAL UNDERSTANDING AND SITUATIONAL AWARENESS

Situational Awareness (SA) is the perception of a particular area of interest, problem or situation bounded by time and space in the context of a mission or task. It provides the ability to identify what has happened and what is happening, but not necessarily why it has happened [6]. Typically SA usually supports military decision makers in relation to knowing about the state of an operating environment and relevant entities within it. For example SA may be described as having three main components, with the additional attributes, as shown in the columns of Table 1.

Table 1: Components of SA.

Operating Environment Awareness	Adversary Awareness	Mission / Business Awareness
• Own Position • Environmental Factors, Landscape & Geography • Location of Other Entities	• Adversary Position • Adversary Capability • Adversary Posture • Indicators & Warnings	• Status of Desired Outcome or Mission Objective • Progress Against Desired Outcome or Mission Objective

Cyber SA, as a concept, typically tries to apply these traditional SA concepts in the context of cyberspace and operating in cyberspace. There are several complex challenges surrounding SA relating to cyberspace. Not all of these challenges are unique to SA in cyberspace but, if the challenge is not unique, the nature of cyberspace often confounds the issue because of the complexity of STSOS. SA challenges in cyberspace include:

- Complex cyberspace STSOS architecture:- the socio-technical architecture includes intangible artefacts that are relevant in understanding the cyberspace operating environment. How easy is it, for example, to observe and make sense of what is fundamentally a stream of formatted units of data, bits or symbols within digital transmission;
- Persistence and pervasiveness:- with many technologies directly or indirectly connected, on a continual or intermittent basis, to the networked world the result is unknown/poorly understood relationships between physical, cognitive and virtual entities (a characteristic that adversaries with malicious intent will consistently aim to exploit). In addition, cyberspace is not just the wired and wireless connection environment but also includes digital interaction through the Electromagnetic Environment (EME). It will become increasingly important to understand both cyberspace and the EME as they have intrinsic and pervasive touch points and system relationships;
- 'Big data':- the volume, velocity, variety[1] of data generated in cyberspace often overwhelms the ability to analyse it in depth and therefore truly understand;
- Geospatial and temporal aspects:- relating cyberspace activities to physical geography at commensurate spatial and temporal scales is required. The physical area of operation is just one of the important layers in cyberspace, and a small subset of it (see Figure 1). The persistent, pervasive and borderless nature of cyber activities allows both simultaneous global and local operations and effects;
- Speed of effect:- whilst the propagation speed of transmission in cyberspace is dependent on the physical medium used, suffice it to say that effects in cyber systems can be rapid and real-time, at the 'speed of light', and propagate through the system almost instantaneously. This requires operators and decision makers across the enterprise to be able to direct, coordinate, authorise and execute action in a timely manner to exploit opportunity and manage threat. This drives a pace of decision making at all levels that could challenge current operational tempo and associated command assumptions;
- Attribution:- cyber activity is notoriously difficult to trace and, despite technological developments, many cyber incidents are likely to be deniable and some untraceable. Whilst in some cases an adversary may specifically want their effect to be overt and 'flagged' as originating from a certain geographical region or threat actor, in other cases effects will be combined with efforts to obfuscate and/or deceive in order to manipulate the cognitive domain decision making; and

[1] Number of V's is often debated, with Doug Laney often given credit for originally describing Big Data challenges relating to Volume, Velocity & Variety. Other V's, such as Veracity and Variability are sometimes included. https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

- Operational effect:- recognising the reach, speed, and impact of propagation, cyber capabilities may be seen to be flattening traditional hierarchy of strategic, operational and tactical actions, with local and tactical actions given global reach and potentially strategic impact. Cyber SA therefore requires broad integration of awareness at all STSOS layers, systems scales, spatial and temporal scales, and operational levels.

3.0 SA IN DECISION MAKING

The above challenges need to be considered with respect to current UK Military doctrine as defined in MOD's Joint Doctrine Publication 04, JDP 04, [6]. In UK military, decision-making at all levels comprises several basic steps: **direction; consultation; consideration; decision; and execution**. Extracted from JDP 04 [6], these steps and the utility of knowledge and information in this process can be graphically represented [Figure 2].

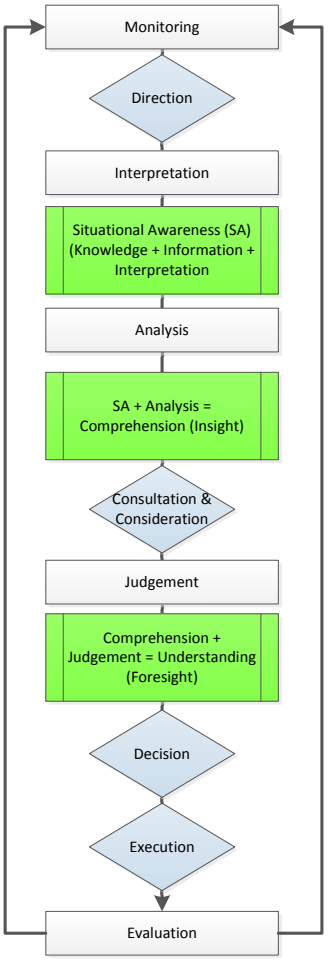

Figure 2: Model interpreted from JDP 04.

From Figure 2 it can be seen that SA is a fundamental building block of decision making but that comprehension and judgement (i.e. understanding) is needed to make decisions and achieve foresight. Understanding is about making better decisions based on the most accurate depiction possible. The purpose of understanding is to equip decision-makers at all levels with the insight and foresight required to make effective decisions as well as manage the associated risks and second and subsequent order effects [6].

Comparison of the JDP 04 decision making model with the foremost academic model for SA reveals a close relationship but also key differences.

Figure 3 is interpreted from a seminal paper by Endsley [1] which has been widely debated, and at times extended, and is used in many other SA studies. In summary this gives three levels of SA:

- L1 Perception:- to perceive the status, attributes and dynamics of relevant elements in the environment;
- L2 Comprehension:- synthesis of disjointed L1 elements. Goes beyond simply being aware of the elements that are present to include understanding of the significance of those elements in light of pertinent operator goals;
- L3 Projection:- ability to project the future actions of the elements in the environment – at least in the very near term.

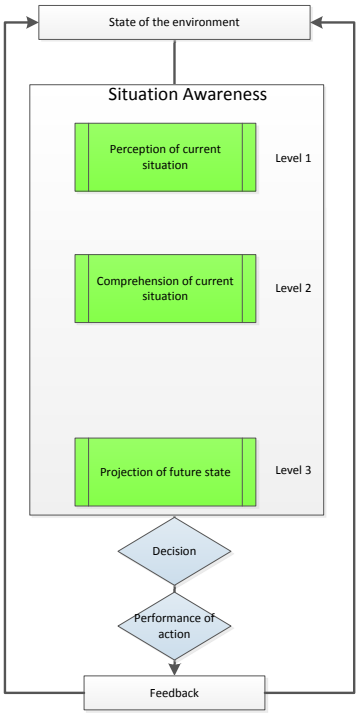

Figure 3: Model from Endsley (1995).

As stated by Endsley (1995), the words “perception”, “comprehension”, and “projection” can be taken to denote progressively increasing awareness levels ranging from (i) basic perception of important data, (ii) interpretation and combination of data into knowledge, and (iii) ability to predict future events and their implications.

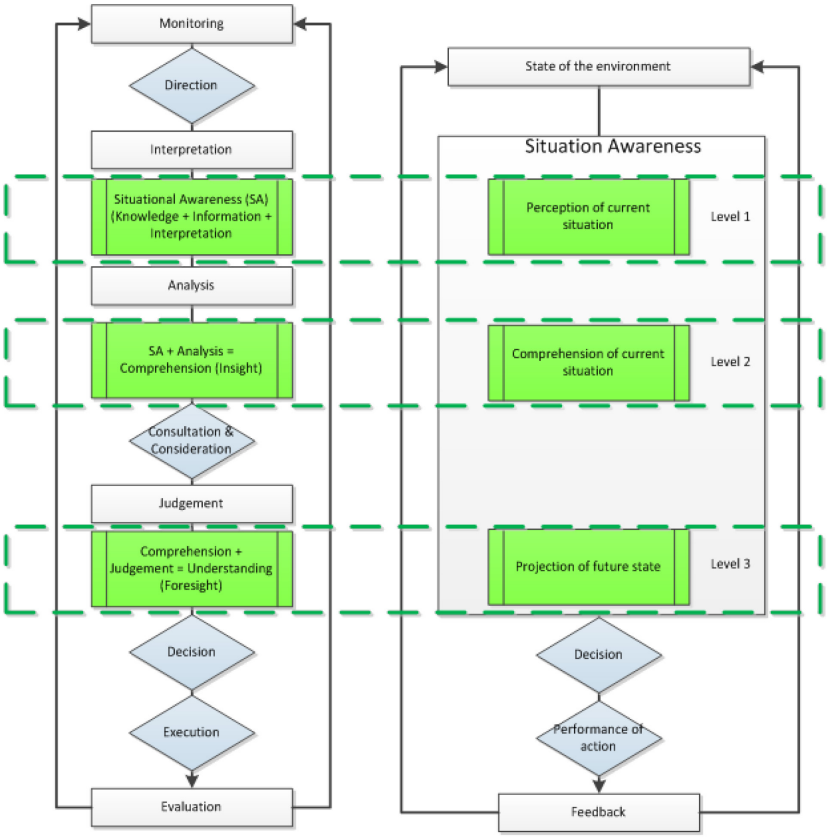

Figure 4: UK MOD JDP 04 model (left) and Endsley model (right) and relationship (dashed boxes).

A comparison between the two models defines a relationship which is represented by the dashed boxes in Figure 4. Both models reflect a decision making process which is preceded by observation of pertinent aspects of the operating environment, and iterates through evaluation and feedback loops that initiate observations of changes in the operating environment.

The key difference, however, is that fundamentally the Endsley model of SA, having three levels or states, reflects the concept of "understanding" and the ability to project into the future (foresight). SA in the Endsley model is "based on far more than simply perceiving information about the environment, it includes comprehending the meaning of that information in an integrated form, comparing it with operator goals and providing projected future states of the environment that are valuable for decision making" [1]. Whereas in the military context (JDP 04), SA is usually about knowing about the environment, knowing something is happening but not knowing why. True understanding is achieved when you have the ability to predict forward which enables candidate courses of action (CoA)[2] to be considered. For this reason it is determined that cyber SA is a legitimate and desirable concept, but only because it enables cyberspace 'understanding'. Commanders require SA to conduct detailed analysis to identify the atmospherics and boundaries of a problem. This analysis leads to understanding and the development of insight and foresight [6]. Therefore, in the context of UK military, cyber SA is important but not sufficient to solely enable effective decision making.

[2] CoA - an option that will accomplish or contribute to the accomplishment of a mission or task, and from which a detailed plan is developed.

4.0 AREAS OF RESEARCH INTEREST

In UK MOD, these models (and the relationship between them) depicting the role of foresight in decision making have been used to articulate focus for research effort. Aim is that capabilities can be developed for specific steps within the models through understanding of the relevant inputs and outputs for a specific user and use case.

In light of the challenges outlined earlier, the following comprehensive list, not necessarily complete or exhaustive, describes some of the areas of research interest for UK MOD to enable capabilities in cyber SA, but moreover to achieve cyber understanding:

- Identification of Cyber Environment 'Vital Terrain'
  - What cyberspace 'terrain' is critical to operations and why? What virtual space or physical ICT infrastructure is either critical to a mission/decision, or offers additional benefits to gaining understanding of area of operation?
- Cyberspace Indicators & Warnings
  - What do we need to observe (or can we observe) in terms of Indicators & Warnings in cyberspace operational environment? These items of information reflect the intention or capability of a potential adversary to adopt or reject a CoA that may be present in both physical, cognitive and virtual domains.
  - With continual threat development and diversity, and limited historical scenarios to investigate, how do we know what these indicators are? Can post-event analysis of digital enterprise data track and trace own and adversary action to inform future indicators?
  - Which heuristic approaches to indicators are available that are agnostic of threat vector and not dependent on matching signatures of activity against database of known activity or entities of interest?
  - How do we fuse the broadest set of diverse indicators to generate enhanced SA and underpin robust understanding?
- Mission Impact
  - Given the complexity of cyberspace systems, how can we inform CoA determination by understanding the propagation of effect through a system?
  - Can this enable damage and impact to be accurately estimated, informing mitigation activity or response and recovery plans?
  - Approaches will need to be able to trace impact through virtual, physical and cognitive domain and the domino effect of second, third, and nth-order events. What are they and their utility?
- Predictive CoA Analysis
  - In order to enable true understanding (or Endsley Level 3 SA (Projection)) predictive approaches are required. How do we understand threat actor TTPs (Tactics, Techniques, and Procedures) to predict adversary CoA and enable counter tactics?
  - Novel approaches to integrate intelligence are needed. How can we best combine commercially available cyber threat intelligence from security vendors, and classified intelligence from military and allied partners (across government and international) sources?
  - Are probabilistic analysis tools that can estimate, on the basis of past (historical) data, the probability of an event occurring again available? For example, application of Game Theory, or other mathematical/statistical models of conflict, that optimise across a range of potential CoA.

- Enable comprehension and judgement
  - Recognising that understanding is fundamentally a human, cognitive concept, how do we better enable the application of judgement (such as deliberation or intuition based on experience) to analysed data and information relating to cyberspace activity?
  - How do we present this information and complexity intuitively to decision maker – typically human-computer interfaces are primarily mouse, keyboard, monitor but do virtual reality, augmented reality, mixed reality approaches (for example) offer new ways to view, analyse and use data?
- Shared Situational Awareness
  - Battlespace management is intrinsically collaborative, both up and down the chain of command, and between levels of command [7]. In other traditional operating environments battlespace management is achieved through shared situational awareness to enable informed decision making. How do we transition this to cyberspace, the fifth operating environment?
  - Approaches are required to generate a fused cyber operational picture – that can be integrated with other operational pictures. Tactical operational pictures are required to be timely, high fidelity, validated in order to enable a commander to understand his environment and, drawing upon his intellect and experience, to make valid decisions based on the information available [7]. How do we address this challenge which is less about how to visualise cyberspace but more about how to fuse this operational picture, intuitively with other operational pictures?

5.0 FROM SITUATIONAL AWARENESS TO UNDERSTANDING

Cyber SA has, in one form or another, been a topic of academic research for some time [7]. Furthermore, an internet search, using phrase “cyber situational awareness”, returns a number of white papers and a list of commercial products.

On closer examination, however, it is clear that some Cyber SA solutions, offered by commercial internet/cyber security vendors, only address part of the required jigsaw of capability. This is because many of the challenges faced in Defence are not directly relevant or applicable in the commercial world. Whilst large commercial organisations are involved in defending their own digital enterprise, they will rarely be involved in the broader digital enterprise and dynamic cyberspace - “cat-and-mouse” operations that the UK MOD has to deal with and is preparing for. Furthermore, many commercial products aimed at generating SA, are often aimed at providing indicators and warnings, and less so about providing decision support tools to aid true (predictive) understanding.

Considering the challenges set out within this paper, it is the belief of the authors that there is a need in the research community to:

- Recognise differences in terminology and language between models of decision making in order to shift from a desire to achieve SA to achieving (and applying) true cyberspace understanding;
- Apply automation wherever possible in order to relieve the cognitive burden on the analysts / decision makers and allow decision makers to focus on applying judgement where it is most valuable in the decision making process. Opportunities for this are most probable starting at the top of the decision making process [Figure 2], for example automating approaches for monitoring, detection and analysis to achieve SA;
- Apply innovation in machine learning and, for example, human-agent-collaborations to assist cognitive processes and decision making at an operational tempo relevant to cyber operations;

- Understand how to integrate a range of diverse tools, that may have strengths and weaknesses in different areas, to underpin a holistic systems engineering approach to understanding cyberspace; and
- Extend breadth of approaches to achieve understanding from traditional computer networking to the rest of the digital enterprise, in order to be inclusive of all potential adversary vectors to exploit vulnerabilities or routes of propagation through the STSOS (e.g. including embedded control systems, building/vehicle management systems).

6.0 CONCLUSION

Identifying the differences between the interpretation of situational awareness and the SA models used by academia/industry and government has been critically important. They have provided a useful distinction to inform the UK MOD Cyber Science & Technology Programme when conducting research on behalf of the UK military. For example, JDP 04 [Figure 2] is familiar with the military community and often used when discussing requirements and capability needs. The Endlsey model [Figure 3] is more familiar within the academic and industrial supply base. Misunderstanding over terminology can lead to poorly focused research. There is a need for the community to shift its language and approach to transition from a desire to achieve cyber SA to achieving (and applying) true cyberspace understanding. Taking this shift in emphasis, additional fundamental challenges are exposed which require focus of S&T research to address and achieve Cyberspace Understanding.

In particular in encapsulating the critical role of foresight which needs to be aided by, and better represented in, the models. This coupled with the same for insight can provide the knowledge, comprehension and judgement needed to achieve better understanding. Research in support, including automation, has to help develop capabilities across specific steps within the models, ensuring that the relevant inputs and outputs can be addressed for a specific user and use case. Within this context, the themes for research of note are:

- Identification of Cyber Environment 'Vital Terrain'
- Cyberspace Indicators & Warnings
- Mission Impact
- Predictive Course of Action Analysis
- Enabling comprehension and judgement
- Shared Situational Awareness

7.0 REFERENCES

[1] Endsley. M. R., "Toward a theory of situation awareness in dynamic systems". Human Factors 37(1), 32–64, 1995.

[2] Madahar. B.K., "Cyber Defence", Defence and Surveillance Section Pan European Networks: Science & Technology, 1, 2013.

[3] NATO Cooperative Cyber Defence Centre of Excellence Cyber Definitions [https://ccdcoe.org/cyber-definitions.html] Accessed 15 September 216.

[4] "National Security Strategy and Strategic Defence and Security Review 2015, A Secure and Prosperous, United Kingdom", November 2015 [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf].

[5] Development, Concepts and Doctrine Centre. "The Cyber Primer (2nd Edition)", July 2016, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf].

[6] Development, Concepts and Doctrine Centre. "UNDERSTANDING', Joint Doctrine Publication 04, December 2010, [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33701/JDP04Webfinal.pdf].

[7] Development, Concepts and Doctrine Centre. 'BATTLESPACE MANAGEMENT', Joint Doctrine Publication 3-70 (JDP 3-70), December 2012 [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/142588/20130313-jdp3_70_Batspc_Man.pdf].

[8] Franke. U. & Brynielsson, J., "Cyber situational awareness – A systematic review of the literature", Computers & Security Vol46, 18-31, 2014. [http://www.sciencedirect.com/science/article/pii/S0167404814001011].