Challenging the Limits of Cognitive Systems Engineering and Ecological Interface Design: Commander's Cyber Situational Awareness

Rob HUTTON[1], Hannah BLACKFORD[1], Kevin BENNETT[2], Nigel JONES[3], and Ade FISHER[4]

[1]Trimetis Ltd, UK; [2]Wright State University, USA; [3]RightObjective Ltd, UK; & [4]Montvieux Ltd, UK

Abstract. Military commanders are increasingly required to understand more than just the physical terrain. Understanding activities in cyberspace and their impact on operations presents a number of challenges for military personnel, tech-savvy or not. This paper presents a cognitive systems engineering approach to providing visualization solutions to support commander decision making. An Ecological Interface Design (EID) approach was used. Challenges for supporting cyber situational awareness are described.

Keywords. Cyber activity; Visualisation; Situational awareness; Cognitive Systems Engineering.

1. Introduction

This paper describes an Ecological Interface Design (EID) approach to the development of a visualization 'top view' to support a military Commander's understanding of activities in cyberspace and how they impact his mission objectives. The work described here was funded by the MOD Centre for Defence Enterprise and is reported in full in Hutton et al., (2016).

1.1 The Cyber Domain

An operational commander is responsible for planning, issuing orders and monitoring progress of activities towards operational objectives. In the world of tanks, planes and ships, the physical world is the primary domain of operations. More recently space and information/influence operations have also played a part in operations. The cyber domain represents an additional, complex and intangible operational space of networked systems, network control and access, unclear identities and allegiances, and rapidly changing circumstances. The success of future military operations will require the commander to understand activity in this space to the same extent that he can understand troop movements over physical terrain.

Visualisation in cyber operations presents a number of complex design challenges. The first relates to the multidimensionality of the problem, from the dimensions of cyber space (MOD DCDC, 2013) to the adversarial and contested nature of those dimensions. The second relates to the dynamism of the domain in terms of the speed that actions can have an impact, the speed at which capabilities e.g. exploits, vulnerabilities, and therefore risk, change. The third relates to the fact that much of what drives the causes and subsequent effects of activities in the cyber domain are based on people's behaviours and intentions, rather than laws of physics. Our understanding and subsequent models of the behaviours and intentions in this domain are relatively immature compared to say the laws of physics which dictate the control and related information requirements for an aircraft or nuclear power plant. Each of these challenges makes designing visualisations and displays to support cyber operations that much more challenging. EID has been demonstrated more in physical domains, but is less well documented and adapted to domains such as cyber. However, our experience has been that it does provide a structured and principled way to think about and design systems to support military thinking, threat assessment, risk management and decision making in a cyber context.

1.2 Cognitive Systems Engineering Approach: Ecological Interface Design

Cognitive systems engineering (CSE) is an integrated, universal, and interdisciplinary framework for understanding and improving complex work systems. This framework incorporates a set of conceptual distinctions, analytical modelling tools and procedures that are required for system analysis, design, and evaluation. EID uses mature computational resources e.g., interface technologies. to provide decision support tools that leverage the powerful perception-action capabilities of the human. Together, CSE and EID provide "... a systematic framework for collecting and then organizing data about work practices, so that the development of truly novel ways of working becomes more effective and efficient." (Vicente, 1999, p. 134). The defining characteristic of the CSE / EID approach is the emphasis that is placed on understanding the underlying work domain. A fundamental belief is that only by analysing and understanding the work domain will we be able to develop interfaces that support Commander understanding, and so provide effective decision making and problem solving support. CSE provides complementary analytical tools (the abstraction and aggregation hierarchies) that are used to model the constraints (or affordances) of the work domain. These constraints are characterised in terms of "means-ends" relations i.e. there are goals or ends that need to be achieved and there are means, the functional and physical resources that can be used to achieve them. The end product of work domain analyses is a model of the informational content that is required for effective system understanding and design.

A second requirement is to identify system constraints that are associated with the agent[1] who is 'controlling' the system. This includes both general capabilities / limitations of humans or machine decision makers, as well as specific knowledge like the expected levels of knowledge and training. CSE / EID characterises these capabilities / limitations as three different modes of behaviour: skill-based behaviours i.e. sensory-motor skills associated with perception and action; rule-based behaviours i.e. situation assessment and responses developed through prior experience; and knowledge-based behaviours i.e. problem solving and reasoning based on internal and external models. From the CSE / EID perspective the interface is the medium (a "virtual" ecology) which stands between the work domain of situations and the human one of awareness or 'understanding'. It will contribute a set of perception / action constraints that can help or hinder performance.

The success or failure of a graphical user interface will depend upon two very specific sets of mappings. One set of mappings occur between the interface and the domain. The "specificity" of the interface refers to the extent to which the geometrical constraints that it provides are a good match for those constraints that exist in the work domain i.e. does the visual evidence provided by the interface map directly onto significant possibilities or affordances of the problem space or work domain?. A second set of mappings occur between the interface and the agent. The 'attunement' of an agent refers to the extent to which 1) the representations allow the agent to pick-up information about the problem space e.g., the affordances; and 2) the agent has learned to appreciate what these patterns mean in terms of the appropriate actions to be taken.

[1] The term 'agent' is used to refer to both human operators e.g. Staff Officers or Commanders, and to machine system components e.g. automated or intelligent systems that might 'make decisions' such as prioritisation and processing of data. For our Cyber Visualisation concepts we expect the likely users to include staff officers, principals and Commanders at various levels of command. The system will support 'controllers' of the system as well as 'consumers' of the information.

A successful interface will be tailored to match both the specific work demands and the powerful perceptual skills of the agent. It will leverage the powerful skill-based behaviours of the human by allowing them to perceive and act directly upon the work domain i.e. keeping the perception-action loop intact. For example, the human will be able to perceive the affordances of the domain through consistent spatio-temporal patterns in the interface. The interface will also provide perceptual cues that trigger the powerful forms of expertise that are embedded in rule-based behaviours. With sufficient experience, operators will be able to recognise both situations and appropriate responses automatically e.g. "decisions" will be perceived directly without the need for extensive analytic reasoning. Finally, a successful interface will provide external models i.e. a simultaneous graphical explanation, of the "deep" structure of the work domain. This is necessary since even experts will eventually be confronted with situations they have never experienced or planned for. Under these circumstances the interface needs to support operators in reasoning about what is happening and what needs to be done.

In summary, the CSE / EID approach provides a principled and structured approach to system development, and in particular, to graphical user interface design. This framework allows designers be "in the ball park" of an effective interface design in less time than other approaches So it will cut down the number of design-evaluate iterations that are required to build effective decision support (Bennett & Flach, 2011).

1.3 Scope

Joint, Operational. We decided to investigate and develop solutions at a joint, operational level based on our understanding of: the nature of defence cyber operations; the variety of participants in the endeavour; and the owners of the assets that provide the cyber enabling capabilities. Without committing to a specific organisation or user, we envisioned a future environment where a Commander responsible for the cyber 'component' of operations would need to support a Joint Task Force Commander (JTFC) in understanding and tasking cyber capabilities. The Cyber Commander would need to: understand the JTFC's requirements with respect to a plan; generate a cyber plan to provide the required decisive conditions and supporting effects; and to monitor activities and events in the operating environment that impacted the cyber component of operations. The Cyber Commander would then need to be able to represent that understanding in JTFC planning and operations management activities such as planning groups and Situation Awareness Briefings.

Operational Impact. In order to achieve this, the interface requires inputs from across the headquarters on: intelligence in the form of threats, threat actors, threat capability and intent, and threat activity; J3 and J3 / J5 operational views in terms of cyber requirements to generate or support the achievement of a variety of effects and mission objectives; and the J6 / networks view of not only the 'near' networks and system assets, but also the mid-cyberspace coalition bearers and third party (commercial) bearers under contract, and the 'far' networks that might be relied upon for specific objectives e.g. ad hoc wireless networks, or other bearers whose networks may not be assured or controlled by trusted sources.

A Socio-Technical System. A key aspect of the effort was to support the translation of cyber activity and events into impact and implications on the mission objectives. Currently, the view of cyber is very focused on military computer network support, and very technical. However, in a broader cyber operations context, it is as much about the social side of cyber as the technical side. Our project attempted to provide the translation of technical cyber network defence operations into broader, non-cyber, HQ and mission implications - the 'so what' of cyber. However, our view of this changed during the project and we came to understand that the cyber picture is far broader than the military's own systems' view of networks and systems in cyber. It also needs to include 'mid' and 'far' networks i.e. computer networks that are relevant to the mission but not owned or assured by the military network providers. This is in addition to the non-technical side of cyber which is about the role of threat actors, and understanding their capabilities, reasons for 'being in the fight', and their 'urgency' with respect to involvement. Any support to the Commander's understanding of cyber space must also include the 'grey' space i.e. for those not obviously allies or adversaries, as well as the social / actor aspects of cyber. So a true socio-technical system view was required.

2. Work Domain Analysis

The focus of our initial effort was to conduct a preliminary Work Domain Analysis to inform the information content of the visualisation (Vicente, 1999). We used two primary sources of information: documentation and subject matter experts (SMEs) including a member of our team and nine military cyber SMEs. The document review included open source doctrinal publications and relevant research literature. The doctrinal resources included both UK and US for cyber operations, Cyber Electro Magnetic Activity (CEMA), strategic communications, information operations (and notions of information dominance, information superiority, and operations), Joint Force Communications and Information Systems (JFCIS) and Operational Planning doctrine. Open source research included work in cyber operations, cyber security, previous cyber visualisation work, and cyber operation case studies e.g. Russia-Georgia, Israel-Palestine, Ukraine, and Lithuania. Our interviews included nine SMEs with experience in cyber policy and doctrine, CIS operations, cyber defence operations, joint force cyber SMEs, and Army CEMA and cyber information exploitation.

We generated several iterations of an Abstraction Hierarchy (AH) that provided a functional representation of the cyber operations 'work domain' at a joint operational level (as opposed to a national strategic level or a service-specific tactical level).

The abstraction hierarchy serves as a functional, enduring foundation for the visualisation requirements to support commander (and his wider headquarters') understanding of the cyber activities in the wider operational context. A key challenge in developing the abstraction hierarchy is the multi-dimensional nature of cyber operations across several relevant dimensions described above but summarised as:

- Physical-Logical-Social / Cognitive: i.e. can be viewed through several 'lenses' in terms of the 'system of interest' from geographically represented, physically connected in some cases, but also logically in terms of a variety of electronic connections, some physical others virtual, and yet others social;
- Causal-Intentional: i.e. governed by laws of physics versus the intentions of people and their behaviours;
- Near-Mid-Far: i.e. the extent to which one has control and assurance over computer networks of relevance to an operational context, akin to a dimension of 'trust';
- HQ Functional aspects of Operations (J3), Planning (J5), Operations Support (J3 / J5), Intelligence (J2) and Network, Communications and Information System support (J6);
- Red-Grey-Blue: actors in a contested space with differing levels of alignment to the mission objectives. For simplicity's sake, we equate "blue" forces to those aligned with our interests e.g. friendly forces, allies, coalition forces, "red" to known adversaries, and "grey" to the rest. Threats to blue may come from a variety of sources not necessarily aligned between themselves, but mutually aligned against the blue / coalition objectives,

as well as non-aligned but necessary ‘middle-men’ i.e. those who either provide or are reliant on network, communications and information system capabilities that are contracted yet critical to mission success such as bearers for military communications and data transfer, or contractors reliant on others’ networks for their own operations e.g. fuel providers.

Each of these views presents relevant aspects of ‘the cyber operational picture’ for a Commander to understand with respect to his objectives.

Traditionally, CSE and CWA have been conducted in systems where the system is governed primarily by laws of physics e.g. nuclear power plants or chemical process control plants. There are some examples of CSE in military contexts e.g. (Bennett et al., 2008) where the system objectives are driven in part by human objectives. However many of the moving parts used to be physical systems such as vehicles moving over land, sea or air. The cyber context presents even more challenges to the representation of information in meaningful ways that support understanding, diagnosis, reasoning, and decision making.

3. Methodological Challenges

Given the sensitivities associated with the cyber context, access to SMEs presented a challenge. Feedback from the stakeholders indicated that we have generated a useful understanding of the cyber operations context, and one that has generated some new insights into understanding and interacting with cyberspace. Our discussions with SMEs have also uncovered some real challenges within the operational community on joint cyber operations thinking. These include: issues of what the appropriate organisational structure looks like; how to integrate planning across services and HQ function; how to regard ‘effects’ and how to represent them in a full spectrum, integrated fashion (not just a challenge for cyber, but one that is particularly difficult in that context); as well as challenges associated with the accompanying doctrine, policies and processes. The abstraction hierarchy / CWA approach is inherently generic in terms of people, tools, policies and processes that it can be applied to. But we have realised that we are still in the early stages of developing first-of-its-kind concepts and this presents analytical challenges on top of the visualisation design challenge. We would like to think that this effort has presented a useful view on the functional and visualisation requirements for supporting command decision making to enable integrated cyber operations in the military context.

One aspect of our efforts so far has been an emphasis on subject matter expertise on the technical side of cyber, and less so on the operational side. Additional efforts will be required to understand the operational commander’s view of and requirements for cyber information and visualisation, given that the ultimate exploiter of the information presented is the commander and his command team in a broader operational context.

4. Analysis

4.1 Commander Decision Requirements

At a very high level, we identified the following commander’s requirements with respect to his / her understanding of the cyber picture in the context of the larger operational picture:

- How are we doing against the plan?
- What is the risk that I am exposed to against plan requirements?
    - Risk management
    - Capabilities vs. Threats (characterising the ‘contested space’)

- How is activity in the cyber domain supporting or hindering the achievement of my goals?
- What threat actors do I need to be worried about?
- Do I need to do something different to address the risk and / or reduce the threat?
- Do I need to do something different to take advantage of an opportunity?

4.2 High Level Commander Understanding & Visualisation Requirements

To support the commander's understanding of the multi-dimensional complex, socio-technical battle space, including the cyber elements, the commander needs to be provided with the ability, via the visualisation and interaction approaches, to see information in a meaningful, functionally related way; to be able to interrogate that information in order to diagnose why things are happening; and to understand what impact events and activities have on the overall goals of the 'system'. For the information categories that are captured in the abstraction hierarchy, this occurs by looking at 'what' is represented at one level, by looking 'up' the AH diagram to answer the reasons 'Why?' that are important or relevant, and by looking 'down' the AH diagram to answer 'How?' that event or activity is being accomplished or enacted (Figure 1).

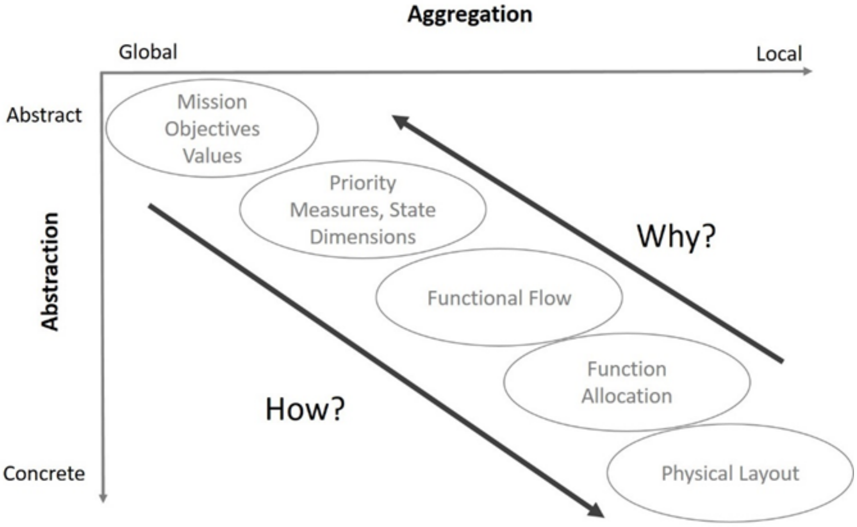

Figure 1. This representation captures the "how-what-why" functionality that is inherent to the Abstraction Hierarchy and essential for effective reasoning and sensemaking in a work domain.

A work domain analysis and its product, a populated abstraction hierarchy, provide the informational content that a Commander needs to understand by answering the 'how-what-why' questions. This is a fundamental aspect of EID. This information is then translated into integrated representations i.e. integrated in the sense that they span all information categories in the abstraction hierarchy that present the constraints and opportunities in a 'system' that allow or disallow / inhibit actions on the part of the commander. It is an action-oriented approach where the 'so what?' is defined by the commander's understanding or appreciation of the implications of a situation i.e. direct perception, and what he or she can do about it i.e. direct manipulation of the objects of interest.

The primary requirement that this presents for a visualisation tool is an integrated set of multiple views or windows onto the current situation. No one view is enough, and each view needs to be tied visually to functionally related aspects of the situation as presented by one view, and linked to other views. This supports the human factors requirement for visualising complex, multi-dimensional information using the principle of 'visual momentum' (Woods, 1984).

In addition, in order to support understanding, the visualisations need to provide direct indications of action opportunities, or in EID terminology, affordances. What does this situation or event 'afford' me in terms of my action options? This supports the EID principle of 'direct perception' (Bennett & Flach, 2011).

Finally, in order to support understanding, we might also point to visualisation requirements stemming from the situation awareness and decision making literature for supporting an understanding of the big picture, how situations got to where they are, and where they might go in the future (Endsley & Jones, 2016; Klein, 1999). This generates requirements in the detailed design of visualisations that support the presentation of historical information (how did this situation come about?) and of projections or anticipated trajectories of events or objects (how might this situation evolve). In the case of support to planning, ideally we would also provide the ability for a Commander to change a future parameter in the situation and see what might happen. This would support projection and evaluation of potential courses of action via actual simulation or support to the commander's mental simulation.

5. Commander Visualisation Support Concepts

A 'Cyber Visualisation Top View' concept was developed based on the analysis above, providing the Commander with an overview of the various perspectives on the cyber situation and meeting the following high level "understanding requirements":

- Multiple, coordinated views.
- Representations across multiple levels of functional abstraction as described in Vicente's Abstraction Hierarchy (Vicente 1999).
- Own-team information, Threat information, and the risk / opportunities emerging from the interaction across those two sets of information to support an understanding of the 'contested space'.
- Near-Mid-Far network representations to support an appreciation of the concepts of control and trust of networks.
- Physical, Logical and Social representations to support an appreciation of the multi-dimensional aspects of cyberspace.
- The red-grey-blue contested space concepts such as relative strength, 'superiority' concepts, and risk: red relative to blue / grey socio-technical systems.

An example of the 'Top View' is provided in Figure 2.

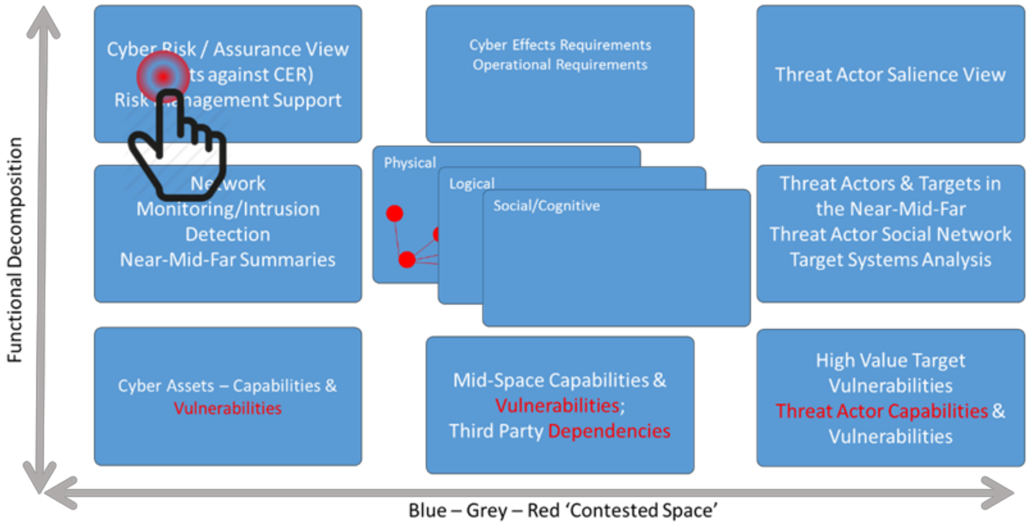

Figure 2. An illustration of the 'Cyber Visualisation Top View' supporting visual momentum across the multiple, coordinated views on the cyber situation. The Top View also has an implicit structure along dimensions of functional decomposition

(from high level purposes to low level, concrete assets) and across the contested space between Blue and Red, with third party bearers (Grey) in the equation.

Two other more detailed concepts supporting the Top View concept were also generated as part of the project. Stakeholder feedback relating to the three visualization concepts was good, including the identification of a number of other issues relating to the larger socio-technical context and challenges that impact on a Commander's ability to understand and interact with cyberspace.

6. Acknowledgements

This work was funded under contract to the UK Ministry of Defence through the Centre for Defence Enterprise funding, in support of Defence Science & Technology Laboratories (Dstl).

7. References

Bennett, K. B., Posey, S. M., & Shattuck, L. G. (2008). Ecological interface design for military command and control. *Journal of Cognitive Engineering and Decision Making, 2(4),* 349-385.

Bennett, K. B., & Flach, J. M. (2011). *Display and interface design: Subtle science, exact art.* CRC Press.

Endsley, M. R. & Jones, D. G. (2016). *Designing for situation awareness: An approach to user-centered design* (2nd Ed). CRC press.

Hutton, R. J. B., Blackford, H. E., Fisher, A., Jones, N., & Bennett, K. (2016). *Supporting commander understanding of cyber activities through Ecological Interface Design: Phase 1 Summary and Phase 2 Technical Proposal*. Trimetis Technical Report TTR012016. Bristol, UK: Trimetis Ltd.

Klein, G. (1999). *Sources of power: How people make decisions*. MIT press.

MOD DCDC (2013). *Cyber Primer.* Development, Concepts & Doctrine Centre. Crown Press.

Woods, D. D. (1984). Visual momentum: a concept to improve the cognitive coupling of person and computer. *International Journal of Man-Machine Studies, 21(3),* 229-244

Vicente, K. J. (1999). *Cognitive work analysis: Toward safe, productive, and healthy computer-based work.* CRC Press.