EAI Endorsed Transactions
on Security and Safety

Editorial

Preface to special issue on the cognitive science of cyber defence analysis

Nancy. J. Cooke[1,*] and Michael. D. McNeese[2]

[1]Arizona State University, Santa Catalina Hall 7271 E. Sonoran Arroyo Mall Mesa, AZ 85212
[2]The Pennsylvania State University, 332Q Information Sciences and Technology Building
University Park , PA 16802

Abstract

An introduction to the key topics in the cognitive science of cyber defence analysis including an overview of the challenges that exist and need to be faced in the field.

Keywords: cognitive science, cyber defence, research challenges.

Received on 24 March 2013; published on 03 May 2013

doi: 10.4108/trans.sesa.01-06.2013.e1

1. Introduction

Cyber defence is an increasing area of importance for a nation's strategic defence planning and preparedness because it enables the protection of human life, valuable resources, assets, and services. Because various types of computer-based systems are ubiquitous and envelop a large sphere of interdependencies across the planet, cyber security and defence is becoming a critical and valuable component of strategic management, information assurance, and tactical operations. The scope of coverage within the area of cyber defence now extends into the following realms:

- Virtual Interactions / Virtual Work
- Cyber Security
- Cyber Infrastructure
- Cyber Warfare / Cyber Offense
- Cyber Telemedicine
- Cyber Space
- Cyber Protests / Cyber Riots

Recent cyber security attacks are reaching an alarming level with ensuing psychological and physical losses. This is not only within typical military domains, but is increasingly present over a wide array of environments with exploitation of cell phones, social media, and mobile applications being increasingly vulnerable. Cyber defence is extremely complex and simultaneously involves the integration of many systems, networks, analysts, and users as tremendous amounts of data come on the scene and are transformed into new vulnerabilities.

In this special issue we define cognitive science broadly to include those disciplines concerned with the science of the mind where the mind can be that of a human, an artificial agent, or a collection of humans and agents. Given the challenges of the cyber domain, cognitive science offers the advantage of more effectively integrating human thought within an emerging context in order to improve intuitive understanding, inferential analytics, alternative explanation, rational integration, and collective induction in addressing cyber defence problems. These capabilities may be amplified through the use of informatics therein expanding joint human-computer analysis in cyber defence. We have indicated before that (McNeese, Cooke, & Champion, 2011) cyber security and defence is defined and acted upon by humans for humans, envelops through human interaction where computer architecture-networks-mobile devices-tools are the media for both success and destruction, and is targeted towards thwarting humans acting to carry out adversarial

*Corresponding author. Email:Nancy.Cooke@asu.edu

missions. Indeed, this is clearly a domain that is predicated on human cognition and team interaction.

Historically this domain has been in the hands of technology developers with a focus primarily only on computational approaches. In turn, the focus, planning, and operational priorities are reticent and deficient in considering human interaction /cognitive science perspectives within cyber defence. Although technology innovation is certainly important, consideration of cognitive science within complex cyber systems presents the possibility of developing cohesive, interdisciplinary approaches that afford transformative solutions for ill-defined and persistent cyber security problems. Continuing on the path of a technology-centered approach will result in narrow, limited solutions typified by the presence of errors, missed opportunities, and eventually catastrophic failures.

This special issue has the goal of communicating specific issues at the intersection of cognitive science and cyber defence to begin understanding problems and opportunities at a deeper level, and to offer potential solutions that are viable, scalable, sustainable, and resilient.

What does cognitive science bring to the cyber defence table? The traditional disciplines of cognitive science that take varying perspectives on the science of the mind include linguistics, cognitive psychology, neuroscience, philosophy, computer science, and anthropology. A myriad of approaches can be directed at understanding cognitive science as applied to cyber defence. Cognitive task analysis, cognitive work analysis, human systems integration, human factors, cognitive modelling, human-centered design, human-computer interaction, and artificial intelligence each provide methods, tools, and perspectives that can be applied to understanding the mind's role in cyber defence. We also consider the science of the mind in the context of large complex systems of which cyber systems are perfect examples. The cyber defence system can include multiple layers of human and artificial intelligent agents interacting with each other and various forms of automation consisting of multiple types of networked computational technology. Therein the goal of this special section is to look at the intersection of cognition, computation, and context as it relates to informing the design of technologies that support and assist humans working within the cyber domain.

There are many ways in which cognitive science can contribute to cyber issues. The theoretical foundations of the field provide the basis for understanding cognitive capabilities and limitations of humans in the context of their interactions with technology. Issues such as trust in automation, situation awareness, and cognitive resilience are prime candidates for this domain. Further, the field has a rich array of methods to offer that range from laboratory experimentation to the analysis of knowledge, expertise, and tasks in the field, to computational cognitive modelling and simulation. These methods, coupled with cognitive science theory, can lay a strong foundation for the design of technology to assist humans and enhance their cognitive performance.

Along with the possible contributions are also numerous challenges associated with the cognitive science of cyber defence. Cyber defence presents a set of unique challenges to cognitive scientists who have aptly applied their science to domains such as command, control, communication, and intelligence; intelligence analyst work; emergency crisis response; and information fusion. One of the main unique challenges is that cyber is not a domain subject to physical space. Cyber space is a place that does not have normal limits of physics in both time and space. It is a space that can quickly be changed by the adversary, where deception can be exacted and information is often hidden in unique ways. In addition to this primary constraint there are a number of additional challenges that need to be overcome to address the cognitive science of cyber defence. These include:

- Access to analysts by researchers is becoming increasingly more difficult so alternative methodologies for acquiring knowledge and designing systems are needed,
- Volume of information is at big-data proportions and at extreme scale, is subject to much uncertainty, and has a limited half-life,
- Because cyber defence is a dynamically changing area with big-data components, it is difficult to track and understand the intentions of the adversary, difficult to obviate the lightning quick adversarial response, and therein hard to produce resilient forms of counter / counter-counter measures that are effective,
- Computer-based tools are often not designed for emergent, adaptive situations and therein can appear rather brittle unless a big picture approach is incorporated into their design,
- Traditional focus is on isolated individual work, whereas teamwork is less emphasized and understood,
- Stove-piping of policy, data, analysts, and tools tends to inhibit information sharing, coordination, and collaboration, therein leading to increased probability of being blind-sighted in cyber domains,
- It is difficult to establish situation / activity awareness in this kind of mutable, ephemeral context.

In order to respond to and address the above issues and others, this special issue draws upon a variety of theoretical foundations, alternative methodological approaches, and highlights appropriate solutions that offer viable outcomes to address the large amount of problems and difficulties within cyber defence. Nixon and McGuiness overview the space of human factors that pertain to cyber security and cover diverse areas of social and organizational factors, manpower, personnel, human factors engineering, system safety, training, and health hazard assessment. Three of the articles in this issue

focus on one of these areas. Haas, et al. take a human factors engineering perspective and look at the role of cyber disruptions on emotions and neurological activity associated with cyber awareness and decision making. Andrews, et al. focus on training and examine strategies for training supervisors as a means of mitigating cyber insider threat. Finally, Cooke, Champion, Rajivan, and Jariwala take the position that teamwork is a critical weakness in the current cyber defence domain, thereby emphasizing social and organizational factors. To round out the special section, Tyworth, Giacobe, Mancuso, McNeese, and Hall describe how the living lab methodology can be used to better understand the role of human cognition in cyber defence.

2. Research gaps identified

The multiple perspectives that are presented in this special section inform how cognitive science can be of greater use within cyber defence to increase the rate of success in protecting human life, valuable assets, and strategic commodities. As we have pulled together material for this special section we have identified gaps and challenges in current research on the cognitive science of cyber security.

- Understanding analyst expertise for training and cognitive aiding
- Function allocation of cognitive tasks to human and artificial agents
- Improving resilience and adaptability of cyber system
- Understanding effective collaboration in cyber defence
- Developing test beds and scenarios for assessments of new technologies or training
- Driving technological assistance from an understanding of cognition in the cyber context
- Measures of the effectiveness of a cyber analyst or a cyber system
- Predictive models of cyber systems

We hope that this special section can lay the ground work for research that addresses these pressing issues.

3. References

[1] McNeese, M. D., Cooke, N. J., & Champion, M. (2011). Situating Cyber Situation Awareness. *Cognitive Technology, 16,* 5-9.