Slow Education and Cognitive Agility: Improving Military Cyber Cadet Cognitive Performance for Better Governance of Cyberpower

Benjamin James Knox, Norwegian Defence University College, Cyber Academy, Lillehammer, Norway & Department of Information Security and Communication Technology, NTNU, Gjøvik, Norway
Ricardo G Lugo, Dept. of Psychology, Inland University of Applied Science, Lillehammer, Norway
Kirsi Helkala, Norwegian Defence University College, Cyber Academy, Lillehammer, Norway
Stefan Süetterlin, Faculty of Health and Welfare Sciences, Ostfold University College, Halden, Norway

https://orcid.org/0000-0003-3698-4585

ABSTRACT

Governance of cyberpower from a military perspective are focused on the efforts to control and influence events occurring in cyberspace. For the Norwegian Defence, this means educating cyber engineers, responsible for governing cyberpower effects, beyond technical skills and competencies. To match the complexity of modern warfighting necessitates adaptive high-order thinking skills. Building on earlier cognitive engineering and human factors research in cyber defence this article suggests how Slow Education has the potential to improve cognitive performance among cyber cadets. Slow techniques were applied to 37 cyber cadets during a three-year bachelor programme at the Norwegian Defence Cyber Academy. The quantitative data for this study was gathered during a two-week Cyber Defence Exercise. Combining and applying a novel pedagogic method with psychological techniques suggests reflective pondering, self-regulation and metacognition as being associated with cognitive agility. This study helps develop and make metrics available that are suitable to evaluate human performance in cyber defence.

KEYWORDS

Cognitive Agility, Cyber Operations, Cyber Security Education, Cyberpower Governance, Hybrid Space, Metacognition, Slow Education

1. INTRODUCTION

Cyberpower is an emerging phenomenon in the Defence realm. It is shaping attitudes, behaviours and decision-making as a result of its ability to: “…create advantages and influence events in all the operational environments…” (Kuehl, 2009, p. 38). Gray (2013) sees cyberpower as “the ability to do something strategically useful in cyberspace” (p. 9). This can be understood as giving agency to any actor, to support or undermine systems of governance, coordination, cooperation and competition (Nye, 2013). Digital technologies provide new capabilities, such as being able to move in three-dimensional space, as well as new threats, such as the use of drones and cyberwarfare. This research provides insights into the development of cyberpower capabilities at the Norwegian Defence Cyber Academy.
2010). As a productive power, cyberpower manifests through relationships and network convergence (Stevens, 2016). One can argue that governing cyberpower is essential to absolutely everything a modern military hopes to accomplish due to its utility to “influence tangible and intangible assets through digital means” (Knox, 2018, p. 11). For this reason, Defence forces need to advance their understanding of the cyberspace military context, in order to mitigate negative consequences when human agency, empowered by cyberpower, is influencing and driving change at rates traditional good governance systems, and codes of practice cannot control (Stevens, 2015).

In the following the changing face of military operations is presented; detailing the effects of cyberpower and the need for adaptations in educational methods to meet the cognitive challenges these effects present. Previous research is introduced to frame the current contribution in the context of operating with cognitive agility in hybrid environments. The concept of Slow Education is then presented, and the importance of metacognition is made clear. The methods section begins with detailing the Slow Education interventions that were applied at the Norwegian Defence Cyber Academy (NDCA) to embed, inform and maintain metacognitive activity. Next, the methods section details how quantitative data was gathered to operationalize and assess cognitive performance in a cyber defence training environment. First, participants completed three trait questionnaires (Response, Self-regulation, Metacognition) before a Cyber Defence Exercise (CDX). Then during the same CDX participants plotted their cognitive focus in the Hybrid Space application (Jøsok et al., 2018) allowing for the researchers to observe for individual use of flexible cognitive processes (Knox et al., 2017). The results section shows the associations between specific cognitive strategies and cognitive agility, represented as cognitive focus movements in the Hybrid Space. Further, we discuss the results in the context of improving performance in military cyberspace operations before the paper concludes and presents future work.

The complexity of cyberspace requires a higher level of understanding regarding own and adversary actions and interactions as information is pushed and pulled from multiple-centers of gravity (Alberts & Hayes, 2003). Educating military personnel to plan, operate and govern complex digital-battlespaces demands focus on the complex mental challenges presented at multiple layers of abstraction. Technological developments may lead to augmented cognition with novel techniques such as artificial intelligence, virtual reality, machine learning and nanotechnology. These emerging technologies are already changing the way of warfare and are demanding adaptations and constant revisions of how to maintain and improve daily operative performance. The digitized context of the future operating environment will subject tactical level decision making to increased levels of scrutiny as incorrect choices and actions can lead to geo-political consequences and unexpected collateral damage (UK MOD, 2014). For young military personnel to accurately govern themselves, technology, cyberpower effects and others in military cyberspace operations, will require the application of flexible cognitions through hierarchies, as well as improved understanding across domains. For example, it is important that military cyber personnel are capable of analysing, evaluating, synthesizing, interpreting and lastly articulating cyberpower effects in relation to wider geopolitical conditions, as well as relating to its application in multidomain military contexts (Knox et al., 2018). When attribution and deterrence in cyberspace are framed by uncertainty, shifting interpretations and applications of cyberpower, deciding what is a tactical attack or an advanced persistent threat becomes far more than a simple exercise in classification.

The authors define governance of cyberpower as legitimate efforts to make events by, with and through cyberspace happen in a productive direction. This definition allows for governance to be understood as a practice capable of occurring at lower levels in military hierarchies, as it meshes both the process and performance concepts of governance (Hyden, 2004). At this level, good governance is more representative of the techniques required to: “...impose a general framework of order on the disorder, to prescribe the general flow of action rather than to try to control each event” (FMFM1, 1989). Conceiving governance this way is similar to what has been described as situational leadership (Northhouse, 2009). Situational leadership is defined as leaders able to diagnose the demands of
Related Content

Tools and Technologies for Professional Offensive Cyber Operations
[www.igi-global.com/article/tools-and-technologies-for-professional-offensive-cyber-operations/104523?camid=4v1a](www.igi-global.com/article/tools-and-technologies-for-professional-offensive-cyber-operations/104523?camid=4v1a)

Analysis of Success of Mobilization to Terror using Tools of Neuro-Linguistic Programming (NLP)
[www.igi-global.com/chapter/analysis-of-success-of-mobilization-to-terror-using-tools-of-neuro-linguistic-programming-nlp/140518?camid=4v1a](www.igi-global.com/chapter/analysis-of-success-of-mobilization-to-terror-using-tools-of-neuro-linguistic-programming-nlp/140518?camid=4v1a)

Online Social Networking: A Source of Intelligence for Advanced Persistent Threats
[www.igi-global.com/article/online-social-networking/75761?camid=4v1a](www.igi-global.com/article/online-social-networking/75761?camid=4v1a)