Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 52-19 (2019) 163–168

Cognisance as a Human Factor in Military Cyber Defence Education

Benjamin J. Knox * **Ricardo G. Lugo** ** **Stefan Sütterlin** ***

* *Norwegian Defence University College, Oslo, Norway (e-mail: bknox@cyfor.mil.no).*
** *Inland Norway University of Applied Sciences, Elverum, Norway (e-mail: ricardo.lugo@inn.no)*
*** *Östfold University College, Halden, Norway (e-mail: stefan.sutterlin@hiof.no)*

Abstract: Cyber Defence Exercises (CDX) are common training and learning tools. A recently discussed challenge in cyber defence teaching and training is the gap between the fast technological advancement accompanied by rapidly changing demands on future cyber defence operators, and the lack of science-based teaching and training methods.
A growing body of evidence suggests a crucial role of human factors as a central predictor for human performance in sociotechnical systems. While this has been acknowledged in a wide range of safety-critical applied fields, there is still a lack of knowledge about the impact of human factors on cyber defence performance. The lack of conventional metrics of performance and learning progress contribute to this deficit.
To address this gap, the Norwegian Defence Cyber Academy (NDCA) follows a science-based educational approach that identified in a series of empirical studies cognitive-psychological predictors for learning success of future cyber defence operators. These predictors and elements of a human factors research program are deeply embedded into educational practice and include processes such as metacognition, self-regulation, coping, communication and shared mental modelling. Slow education methods and mentoring are fundamental to enabling the advancement of human factors cognisance among military cyber cadets.
As a tool for efficient training, the NDCA developed and implemented a mentoring concept that involves a cyber defence retrospective timeline analysis involving expert and practitioner level mentors. The timeline differentiates between performance relevant hard- and soft-skills and leads progressively towards an alignment of Security Operation Centre (SOC)- and expert judgments of performance. The NDCA argues that this educational concept facilitates educational benefits based on insight, accurate self-perception, motivation and decreased team workloads following more efficient collaboration.

Keywords: Cyber Security; Human Factor; Education; Mentoring; Performance; Cognisance.

1. INTRODUCTION

The performance of human agents in socio-technical systems such as cyber defence settings is co-determined by human factors (Gutzwiller et al. 2015). The positive or detrimental effects human factors can have on performance outcomes in these socio-technical systems depends to a large degree on the level of expertise, both on individual and team level. It is therefore of utmost importance to raise awareness amongst future experts and include human factor teaching already at the early stages of cyber defence education. This article proposes the educational model applied at the Norwegian Defence Cyber Academy (NDCA) in which expert mentoring is embedded into a slow education concept. We argue for the inclusion of human factor research in training of cyber officer cadets and the implementation of a mentoring concept focussing on hard and soft skill development directly linked to Cyber Defence Exercises.

1.1 Education in Human Factors

The rapid emergence of cyber security and cyber defence as a field of study and practice has lead to a mismatch between evidence-based teaching and training methods of future cyber operators on one side, and the rapidly progressing skill requirements for effective and adaptive performance on the other (Hoffman 2014, Upton & Creese 2014). A clear educational and scientific focus is required to ensure cyber operators develop the necessary technical competencies, as well as the mental skills that have the capacity to avoid the natural inclination towards cognitive rigidity and instead promote cognitive flexibility (Feltovich, Spierer & Coulson 1997, Klein & Baxter 2006). Achieving success in the face of adversaries who have developed tactics, techniques and procedures over decades in live and simulated environments (Antal 2018) requires defence forces adapt tactics, leadership models, and cyber-team training techniques to address power imbalances. When an adversary is capable of operating below the

2405-8963
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2019.12.168

threshold of war, able to employ tactics that we may yet not be aware of or able to see, may wish to appear clumsy, counterproductive, obvious and easily debunked (Giles 2016), then cyber defence teams should be trained and adaptable enough to not be influenced by knowledge obfuscation or reflexive control (Thomas 2011). To do this may require Complexity Preservation in training. This requires learners to practice in varied contexts at boundaries of current knowledge and skills, accessing knowledge when it is useful or needed, anticipatory thinking, and consider the implications of the current situation for the future, and the alternative ways in which situations may evolve, updating and re-configuring understanding on-the-fly and constantly, and juggling priorities and goal-conflict resolution (Ward et al. 2018). Building utility and resilience in cyber defence teams to ensure mission assurance, means establishing a holistic framework for performance measurement in cyber range environments. Education methods that rely on concepts of learning to store, share and retrieve knowledge are no longer sufficient. Neither is reliance on attending a finite number of scheduled exercises per year sufficient to be classified an expert, or a high performing cyber-team.

The attempt to identify human factor variables predictive for performance and accelerated learning that can be developed early in the cyber defence education process are vital components to ensure mitigating defenders fixed-action patterns; such as negative affect in the form of rumination focussed on internal emotional processes (Nolen-Hoeksema 1991). Failure to address this will only weaken the strongest link in cyber defence, allowing an adversary to exercise cyber power and exploit fixed-action patterns by triggering such behavioural features, leading defenders to be exploited to the point where they misinterpret and/or worse over-react to a cyber-attack. Defenders may also make decisions based upon logic misconceptions, cognitive biases or emotional influences, or rely unconsciously too heavily on intuitive decision-making strategies (Lugo et al. 2016). Institutions need cyber defenders with adaptive and resilient cognitive regulatory strategies. For example, defenders need to be able to measure and monitor their own performance relative to their actual performance or learning rate. This practice is needed to extend current knowledge, whilst facilitating the acquisition of new knowledge and reasoning competencies, at the edge of their current cognisance (Ward et al. 2018).

1.2 The role of mentoring for metacognition and motivation

The term human factors encompasses a variety of human characteristics, abilities, and behavioural traits. A factor with known importance for learning progress is the individuals insight into its own cognitive processes, a prerequisite for goal-directed improvements or compensations. A substantial body of research supports the predictive power of metacognition for academic performance (Young & Fry 2008) as well as in cyber defence scenarios (Knox et al. 2018). Metacognition is defined as awareness of ones own knowledge - what one does and does not know - and ones ability to understand, control, and manipulate ones cognitive processes (Meichenbaum 1985). In practice, metacognition means awareness of and exerting control over ones thinking in planning, monitoring, and evaluating ones cognitions, emotions and behaviors, and actively adapting to the situational demands. In addition to the persons knowledge and awareness of own skills (e.g. self-efficacy), beliefs (confidence), and expected outcomes (situational knowledge), metacognitive knowledge such as technical and experiential knowledge are vital to improve performance. Metacognition develops when the learner, alongside the expert mentor, monitors, debugs, and evaluates what is learned (Nietfeld & Schraw 2002). Reflecting upon how cognitions affect behavior is also essential for metacognitive development. One key process to facilitate metacognitive skills is the reception of precise feedback from mentors and/or peers. Besides facilitating metacognitive accuracy, mentoring and expert-mentors feedback has also the potential to increase motivation and thus the effort an individual invests into a challenging (difficult and/or tiring) task when maneuvering in a complex socio-technical system. The motivation to invest effort has been found to be a significant predictor for cyber defence team performances (Helkala et al. 2016), provided there is a substantial level of domain knowledge in place. Evidence from pedagogical research indicates a clear association between expert mentoring and academic performance (Rhodes 2008), self-regulatory skills (Wentzel 2019), satisfaction levels, and lower stress and anxiety levels (Crips & Cruz 2009).

1.3 Retrospective verbal reports as an educational tool in CDX

An efficient tool to realize mentoring in a CDX context and to tap into the resources experts can offer for the cyber defence education, are retrospective verbal reports (RVR). In more general contexts, RVR have been shown to differentiate between experts and novices and are used to extract covert cognitive processes. RVRs provide explicit descriptions of chosen problem-solving strategies and can be facilitated through cuing. RVR access both short-term memory systems, through episodic descriptions, and long-term memory systems, such as goals, procedures and strategies (Taylor & Dionne 2000). RVRs are used to capture expert performance strategies, operationalize and integrate these approaches into testable paradigms, and accelerate learning by training novices on identified factors from expert reports. This approach has been proven to facilitate performance in nursing (Ericsson & Ward 2007), sports (Meichenbaum 1985) and in military domains (Hoffman et al. 2014). The NDCA educational concept uses RVR techniques in a structured mentoring scheme applied on cyber cadets.

2. EDUCATIONAL APPROACH IN THE NORWEGIAN DEFENCE CYBER ACADEMY

At the NDCA the Bachelor in Technology is grounded in a philosophy of mentorship from selection to graduation. The NDCA feeds officers and non-commissioned officers to all defence services. With the right mental competencies, cyber cadets can adapt rapidly after graduation to their chosen operating environment and perform. Mentoring can scaffold cyber hard skills and human soft skills. At the NDCA these two features are constantly combined and tested in order to ensure holistic performance enhancement at individual and cyber-team level. The approach

the NDCA takes to educating military cyber cadets is built upon traditional military methods, combined with methods that are founded in cognitive engineering and techniques known to accelerate learning (Hoffman 2014) where interventions are made in an attempt to develop adaptive skills. In their final six months cadets specialize in the areas of network establishment and maintenance or defensive cyberspace operations. The NDCA aims to shape individuals capable of governing cyber power effects in military cyberspace operations following a personal development approach. This centres on certain cognitive skills known to support professional performance, such as metacognition, coping strategies (Helkala et al. 2016) self-regulatory processes (Bandura 1986; Bohlmann & Downer 2016), and communication (Knox et al. 2018).

2.1 Slow Education

The approach the NDCA takes to presenting human factor skills to cyber cadets is through slow education methods (Knox et al. 2019). Slow education is an adaptive non-standard based approach to education, and mentoring is a central concept in the slow education strategy. Mentors can support how learners consolidate experiences and new knowledge to long-term memory through for example reflection (Halpern 1998).

The present article argues for the beneficial effects of mentoring on individual and cyber-team performance. The mentoring scheme is implemented during the annual capstone CDX held at the NDCA. The CDX has a research based methodology designed to improve both personal and professional development aspects. The mentor function model (Figure 1) allows for cadets to engage in deliberate practice (Ericsson et al. 1993) and deliberate performance (Fadde & Klein 2010) in a safe-to-fail environment. Like most military exercises, key to achieving the CDX goals is an After Action Review (AAR) process. AARs are defined as a guided analysis of an organizations performance to be conducted during and at the conclusion of an event for future improvement (US Army 2014). The daily AAR at the NDCA CDX allows the cadet run Security Operation Centres (SOC) the opportunity to: question, interpret and understand Red Team threat modelling and attack methods, and cross-learn between SOCs in an open and safe setting. The Scenario Team, Green Team, Red Team and Mentor Teams all have an active role in helping the learners calibrate their own understanding. The crux of this AAR session is to develop the cadets understand function (Ministry of Defence 2015) and overall domain cognisance.

The purpose of the retrospective-timeline construction (Figure 1) is to generate observable events, the main actions that were taken, and key mental events that were important to them. The timeline intends to capture their cognition in context and aims to include key moments they noticed, that caught their attention, that they understood, or when their understanding changed, decisions or judgements they made, or gut feelings experienced, moments of being unsure as to what was going on, actions taken or not taken (but considered), key moments where they had to just trust, or not trust, times when they had to seek or give input to others, and moments of significant communication (including things that were not said, that in hindsight, needed saying) intended to build self-efficacy, domain understanding, cyber-team performance and where possible; accelerate learning.

A key daily task for the expert mentor and the cadets is to construct three timelines (see Figure 1). Timelines and Retrospective-Timelines were constructed in sequence:

- *Mentor Timeline:* This is a continuous process that involved the expert mentor populating his own timeline with observations. This timeline can be thought of as a kind of truth line. The expert mentor has oversight on the exercise events matrix, giving full insight to Red Team activities, as well as other scheduled scenario injects. The expert mentor observes for hard and soft skills, noting events, or non-events throughout each day.
- *Cadet Retrospective-Timeline 1 (RT1):* At the end of each day, prior to entering the AAR each SOC uses 30 minutes to reflect on the days events and plot them on a timeline. Cadets were instructed to take a retrospective account of moments where hard skills and soft skills were required/arose that either aided, abetted or hindered individual or team performance. The purpose is to encourage reflection and attention to performance factors. As well as an attempt to trigger attention and focus to avoid the inevitable mental switch-off/slow down as the daily scenario ends.
- *Retrospective-Timeline 2 (RT2):* Once the AAR is complete, cadets return to their SOC and together with their mentor constructed a second retrospective-timeline. The purpose of RT2 is to as far as possible according to their now deeper understanding of the days events connect cognition to context based on learning manifest. This active reflection process is led by the expert mentor who is able to use his truth-line as reference. On completion of RT2 the cadets should have greater clarity and cognisance relating to actions, interactions and decision-making.

In addition to an expert mentor, each SOC had a practitioner level mentor. Ideally, this person is closer in age and experience to the cadets than to the expert. The practitioner mentors role and function is more peer support, providing a cognitive and context bridge between expert and novice. The practitioner mentor supports populating the expert mentor timeline.

The allocation of mentors to each SOC during the CDX is as follows:

- *SOC 1:* Two experienced cyber defence practitioner level mentors (one on the cusp of meeting expert criteria). Both were Non Commissioned Officers (NCO) and neither had previous experience or training in retrospective-timeline activity.
- *SOC 2:* One military officer expert mentor and one practitioner level NCO. Neither had experience or training in retrospective-timeline activity.
- *SOC 3:* One civilian expert mentor plus an NCO practitioner. Neither had experience or training in retrospectivetimeline activity.

- *SOC 4:* One military officer expert mentor with training and experience in retrospective-timeline activity, plus a civilian practitioner with no experience or training in retrospective-timeline activity.

At the NDCA an expert is objectively defined as an individual with over fifteen years experience in the field of cyber security, information technology, information security. This individual will also have as a minimum a Masters with multiple additional field related qualifications. Ideally the expert will have a PhD and practical experience of conducting cyber-military operations. A practitioner level mentor may have 5+ years experience, and with a number of additional cyber related courses added to her CV.

3. EFFECTS AND EXPERIENCES

When conducting training on cyber ranges it is critical to establish the baseline domain cognisance of participants to ensure task and case balancing (Kick 2014). Establishing in advance areas that may affect performance is crucial with regards to training efficiency. Scoring high in capture the flag training scenarios reveals limited information as a holistic measure of performance as they tend not to give indicators of a robust and cognitively resilient cyber-team. If a cyber range scenario is out of the cognisance space of a member(s) of the training audience then there is the inevitable risk that team member(s) will struggle to cope and become a burden on the team. This situation is detrimental for the individual and group efficacy. As well as novices and all other levels of cyber operators, non-technical personnel in key positions in organisations - who are not immune for cyber-fire - should themselves take an active part in cyber defence training. These leaders are often the high value targets for adversaries as they lack necessary cyber cognisance. Consequently, training on a cyber range with team members who have more domain knowledge, will require that the range and the team members have the capacity to accommodate those with less. Importantly also, umpires, mentors and expert facilitators need to understand human factors, as well as having expertise in hard tech skills, if they are measuring and supporting individual and team performance.

Further research is needed to develop the necessary criteria to ensure expert mentor(s) have the required skill set to support holistic skill development. Technical knowledge consistent with the domain of operations is a prerequisite. Although many systems and their architectures are alike, the context in which cyber defence occurs and how incidents are handled will vary according to individual sector (business) objectives. Combined with this knowledge, the expert mentor should be proficient in the domain of human factors. For many experts in cyber defence, cognisance relating to human factors for adaptive performance is an unfamiliar field and represents a domain of uncertainty.

An outstanding challenge for future work is to put experts through a similar process as conducted in the CDX for cyber cadets. In addition to retrospective-timeline analysis, a Cognitive Task Analysis could also be extremely useful tool to reveal expert mental processes (Crandall 2006) that can be fed back into novice and practitioner level training packages.

Future collaborative research should also include how to integrate cyber doctrine, military strategy and cyber tactics into the education at NDCA. Cyber cadets need to know how to identify, synthesize and respond to hostile cyberpower effects. This means an organisational shift from reactive, linear, information assurance approaches to methods that provide mission assurance and are founded on operational objectives and the reality that cyberspace and the cyber domain is a battlefield that needs defending. To do this requires comprehensive domain cognisance, beyond tech savvy. The large proportion of cyber cadets are highly intelligent. At the NDCA, forty cadets are selected each year from over 300 applicants, all of whom have highly competitive STEM backgrounds. With this academic baseline, the opportunity for complexity preservation by scaffolding new knowledge is possible. The NDCA makes cadets study strategy and doctrine as early as their first semester. When it pertains to the cyber domain, the argument often presented in military circles of too much too soon is challenged as our adversaries will be targeting our weak points, and its the cadets who are the governors of tactical, operational and strategic level digital ecosystems. The NDCA therefore starts building an education platform around new thinking that pertains to advanced understanding, planning, and cooperation that leads to a place where the cyber operators can govern military operations in the one domain where characteristics and features are constantly evolving.

4. FUTURE WORK

A next step for the NDCA is to build on earlier slow education approaches [34]. The intent is to further encourage deeper mental processes in the form of improved cadet situational metacognitive judgements (SMJ). This can be achieved by asking them to rate the three areas judgement of own performance, confidence, and effort. The recommended methodology for this would be cadets answer short questionnaires at key times during the day. For this purpose the Task Workload Scale should be omitted due to the scales focus on personal (individual) demands, but the Teamwork and Task-Team component should be included.

4.1 Pre-mission questions

- How well do you think you will do?
- How sure are you about this judgment?
- How confident are you right now?
- How much effort will this need to do well? (Continuous assessment of increasing/decreasing amounts.)
- How well will your team do?
- How sure are you about this?

4.2 Post-mission and post-RT1 questions:

- How well did you think you did?
- How sure are you about this judgment?
- How confident were you during the exercise?
- How much effort did you put in through the exercise? (Continuous assessment of incr./decr. amounts.)
- How well did your team do?
- How sure are you about this?

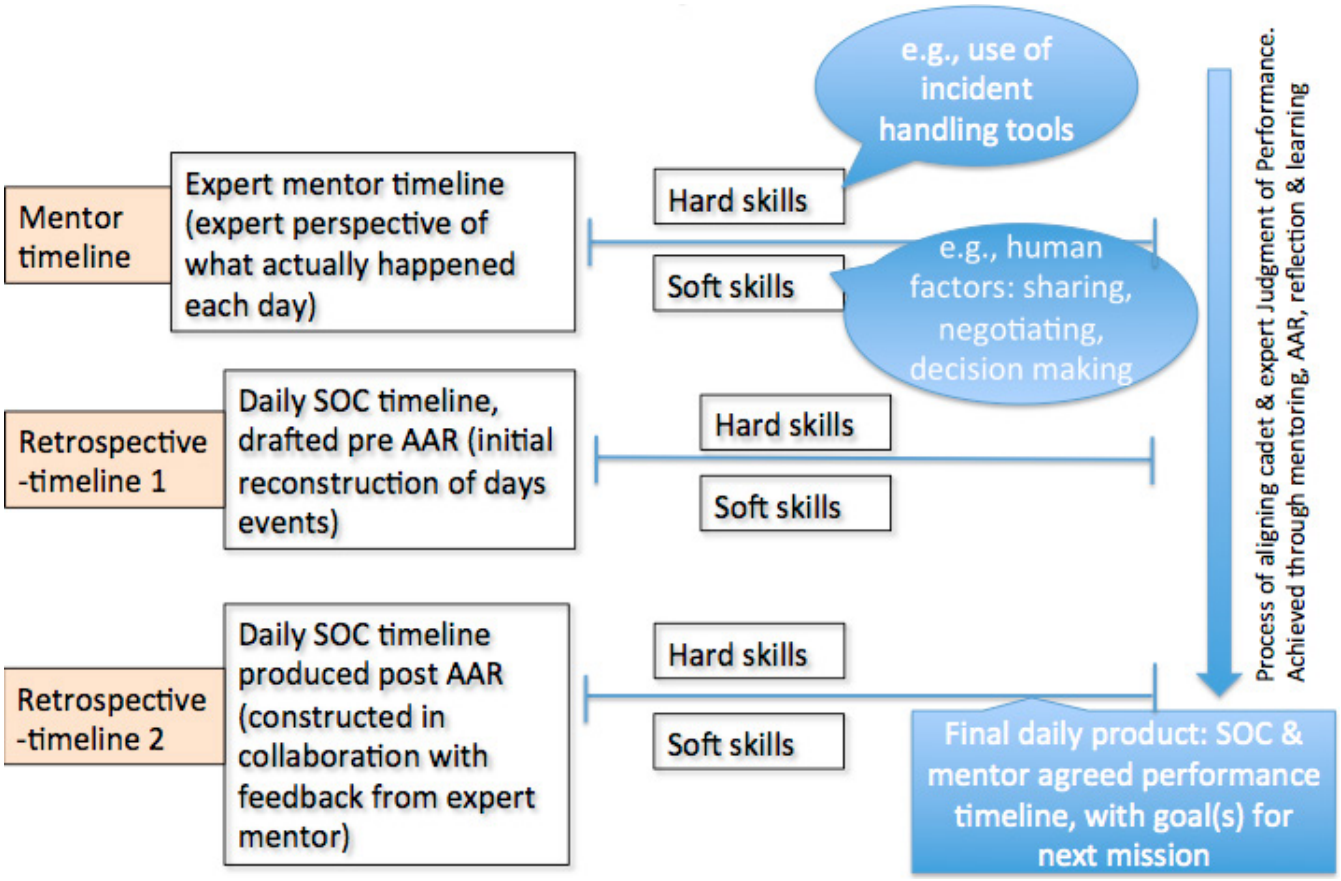

Fig. 1. Mentor concept as implemented in the annual capstone CDX. Three timelines are produced each day in each SOC in accordance with the days cyber related events. This process should enable the cadets to identify realistic and achievable goals for improved performance for the next day.

4.3 Post-RT2 questions:

- Having completed RT2, how well did you actually do today?
- How sure are you about this judgment?
- Having completed RT2, how confident are you now about tomorrow?
- Having completed RT2, how much effort would you have actually needed to use to get closer to the expert level? (Less, same, more, alot more)
- Having completed RT2, how well did your team actually do today?

The outcome for cadets completing this intervention is improved critical self reflection for more accurate measurement and monitoring of own and cyber-team performance relative to actual performance or learning rate (Ward et al. 2018). This, in combination with the retrospective-timeline analysis means the XDCA encourages adaptive performance by facilitating metacognitive skills and reflective practice immediately prior to, midst and on completion of work (Fadde & Klein 2010).

5. CONCLUSION

This critical appraisal contributes to highlighting the obvious need to include findings of human factors research into cyber defence education and training. Currently these key components of developing competent cyber operators do not meet a sufficient knowledge base, and warrant systematic educational approaches starting from an early phase in the educational process.

Through the inclusion of scientifically validated concepts that benefit insight, accurate self-perception, motivation and decreased team workload, the NDCA is able to preserve complexity during protracted periods of training for novice level cyber operators. Applying a rigorous expert mentoring model, that is built into the design and architecture of a capstone cyber defence exercise, allows the NDCA to develop cadets understand function as well as their wider domain cognisance.

It remains to be established if the NDCA mentor concept aligns with earlier research that indicates associations between expert mentoring and academic performance. In 2019 the researchers will aim to validate the mentor model by investigating motivation, satisfaction, stress and anxiety levels during the CDX.

6. REFERENCES

Antal, J 2018, No Train, No Gain. How the US Army's National Training Center is Preparing for High-Intensity War, *Military Technology*, vol. 12, no. 12, pp. 4.

Bandura, A 1986, *Social foundations of thought and action: A social cognitive theory*, Prentice Hall, Inc., Englewood Cliffs, NJ.

Bohlmann, N & Downer, J 2016, Self-regulation and task engagement as predictors of emergent language and literacy skills, *Early Education and Development*, vol. 27, no. 1, pp. 18-37.

Crandall, B, Klein, G, Klein, G, & Hoffman, R 2006, *Working minds: A practitioner's guide to cognitive task analysis*, MIT Press, Cambridge.

Crisp, G & Cruz, I 2009, Mentoring college students: A critical review of the literature between 1990 and 2007, *Research in Higher Education*, vol. 50, no. 6, pp. 525-545.

Ericsson, K & Ward, P 2007, Capturing the naturally occurring superior performance of experts in the laboratory: Toward a science of expert and exceptional performance, *Current Directions in Psychological Science*, vol. 16, no. 6, pp. 346-350.

Ericsson, K, Krampe, R, & Tesch-Roemer, C 1993, The role of deliberate practice in the acquisition of expert performance, *Psychological Review*, vol. 100, pp. 363-406.

Fadde, P & Klein, G 2010, Deliberate performance: Accelerating expertise in natural settings, *Performance Improvement*, vol. 49, no. 9, pp. 5-14.

Feltovich, P, Spiro, R, & Coulson, R 1997, *Expertise in context: Human and machine*, MIT Press, Cambridge, MA.

Giles, K 2016 *Russias new tools for confronting the west: continuity and innovation in Moscows exercise of power*, Royal Institute of International Affairs, Chatham House.

Gutzwiller, RS, Fugate, S, Sawyer, BD & Hancock, PA 2015, The human factors of cyber network defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 59, no. 1, Sage CA: Los Angeles, CA, pp. 322-326.

Halpern, D 1998, Teaching critical thinking for transfer across domains: Disposition, skills, structure training, and metacognitive monitoring, *American Psychologist*, vol. 53, no. 4, pp. 449-455.

Helkala, K, Knox, BJ, Jsok , Knox S, & Lund, M 2016, Factors to Affect Improvement in Cyber Officer Performance, *Information and Computer Security*, vol. 24, no. 2.

Hoffman, RR, Ward, P, Feltovich, PJ, DiBello, L, Fiore, SM, & Andrews, D 2014, *Accelerated expertise: Training for high proficiency in a complex world.* Psychology Press, New York.

Kick, J 2014, *Cyber Exercise Playbook* (No. MP140714), MITRE Corporation, Bedford.

Klein G, & Baxter, H 2006, *Cognitive transformation theory: Contrasting cognitive and behavioral learning*, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC 2006): Training the 21st Century 4-7 December 2006, Orlando, Florida, USA.

Knox, BJ, Josok, O, Helkala, K, Khooshabeh, P, Odegaard, T, Lugo, RG, & Sütterlin, S 2018, Socio-technical communication: The hybrid space and the OLB model for science-based cyber education, *Military Psychology*, vol. 30, no. 4, pp. 350-359.

Knox, BJ, Lugo, RG, Helkala, K, & Sütterlin, S 2019, Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower, *International Journal of Cyber Warfare and Terrorism*, vol. 9, no. 1, pp. 48-66.

Lugo, RG, Sütterlin, S, Knox, BJ, Jsok, , Helkala, K, & Lande, N 2016, The moderating influence of self-efficacy on interoceptive ability and counterintuitive decision making in officer cadets, *Journal of Military Studies*, vol. 7, no. 1, pp. 44-52.

Meichenbaum, D 1985, Metacognitive methods of instruction: Current status and future prospects, *Special Services in the Schools*, vol. 3, no. 1-2, pp. 23-32.

Nietfeld, J & Schraw, G 2002, The effect of knowledge and strategy training on monitoring accuracy, *The Journal of Educational Research*, vol. 95, no. 3, pp. 131-142.

Nolen-Hoeksema, S 1991, Responses to depression and their effects on the duration of depressive episodes, *Journal of Abnormal Psychology*, vol. 100, no. 4, pp. 569-582.

Rhodes, J 2008, Improving youth mentoring interventions through research-based practice, *American Journal of Community Psychology*, vol. 41, no. 1-2, pp. 35-42.

Sellers, J, Helton, W, Nswall, K, Funke,G & Knott, B 2014 Development of the team workload questionnaire (TWLQ), *Proceedings of the human factors and ergonomics society annual meeting*, vol. 58, no. 1, pp. 989-993, SAGE Publications, pp.989-993.

Taylor, K & Dionne, J 2000, Accessing problem-solving strategy knowledge: The complementary use of concurrent verbal protocols and retrospective debriefing, *Journal of Educational Psychology*, vol. 92, no. 3, pp. 413-425.

Thomas, T 2011, Recasting the red star: Russia forges tradition and technology through toughness, *Foreign Military Studies Office*, Fort Leavenworth, Kan.

Upton, S & Creese, S 2014, The danger from within, *Harvard Business Review*, vol. 92, no. 9, pp. 94-101.

US Army FM 6-0 2014, *Commander and Staff Organisation and Operations*, 2014. [Online]. Available: http://www.milsci.ucsb.edu. [Accessed: 28- Feb- 2019].

Ward, P & Williams, A 2003, Perceptual and cognitive skill development in soccer: The multidimensional nature of expert performance, *Journal of Sport and Exercise Psychology,* vol. 25, no. 1, pp. 93-111.

Ward, P, Gore, J, Hutton, R, Conway, G & Hoffman, R 2018, Adaptive skill as the conditio sine qua non of expertise, *Journal of Applied Research in Memory and Cognition,* vol. 7, no. 1, pp. 35-50.

Wentzel, K 2019, Students relationships with teachers, in J Meece & J Eccles (eds), *Handbook of research on schools, schooling and human development*, London: Routledge, pp. 93-109.

Young, A, Fry, S 2008, Metacognitive awareness and academic achievement in college students, *Journal of the Scholarship of Teaching and Learning*, vol. 8, no. 2, pp. 1-10.