Submission of abstract to
International Society of Military Sciences, Helsinki 13-29 October 2020
Working group: Military Education

Title: **"Human resilience against negative effects of digitalization"**

Authors:

Kirsi **Helkala** – Norwegian Defence University College/Norwegian Defence Cyber Academy (NDCA) and
Carsten **Rønnfeldt** - Norwegian Defence University College/Norwegian Military Academy (NMA).

Influencing people's minds, values and attitudes has always been an integral part of war (Taylor, 2003). The emergence of cyberspace adds new dimensions to such efforts (UK Ministry of Defence, 2020). Many of these concern the information domain in which digital information is processed and disseminated, yet in this paper we focus on potential negative effects of digitalization in the cognitive domain, i.e. the realm where situational awareness, decisions along with perceptions and values are shaped. It is widely recognized that wars are lost or won in the latter domain (Forsvarsstaben 2007, p. 70). This poses a host of questions of both offensive and defensive nature for professional military education, but here we are particularly interested in the defensive aspects and how we as educators can help cadets learn to operate efficiently while under influence and stress. More specifically we ask the question: **How can professional military educate prepare future officers to be resilient against negative effects of digitalization?**

We address the question by discussing findings from studies of cadet performance during cyber defence exercises at the Norwegian Defence Cyber Academy (NDCA) and by highlighting some key concepts relevant to gain a better understanding of the issues involved. Before addressing the main research-question we clarify some basic conditions upon which influence at an individual level is based and particularly focus on the human sensory system. We then map out different ways this sensory system can be influenced, both deliberate efforts – including information operations as conceptualised within the alliance (see NATO 2009) – and those that are not necessarily deliberate. The latter includes internet addiction understood as individuals' excessive or poorly controlled preoccupations, urges or behaviours regarding computer use and internet access that lead to impairment or distress (Shaw and Black 2008); as well as technostress which Sellberg and Susi (2014) defines as:

> "a condition of constant high cognitive demand and physiological arousal. The condition is observable in people who, over time, have experienced reduced possibility of understanding, and gaining overview and control over information and workplace processes. The condition ensues from interaction with technology that lacks in usability, and (or) inapt organisational demands and conditions for its use."

A key feature in fostering resilience at an individual level against such negative effects of digitalization is awareness of their existence and to understand that we are always under the influence of others. In order to resist this influence, we need to learn how to calm ourselves and to gain a better picture of the whole situation we are in before we take decisions on how to act (Bakir 2018).

Gaining situational awareness and understanding of "the bigger picture" are normal military activities and always part of military operations, cyber operations included. To gain such competence in the cyber domain NDCA-cadets undertake one or two exercises a year and their performance is studied. Among others we identified key coping strategies to reduce stress and to increase cadets' ability to operate efficiently. During one of the semesters, students were self-reporting their usage of coping strategies in different military and class room contexts (Helkala, Knox and Jøsok 2015). The results indicated that "having control" was the main factor in order to perform well and this applied both to a military and to a classroom context. The same coping strategies were also usable when operating in the cyber domain (Helkala, Knox and Jøsok 2016) and "having control" was found to be the main factor in good performance in this domain as well.

Dragano and Lunau (2020) points to education, technical support and planned implementation of technologies as important to reduce technostress. The stress factor is also discussed in (Nindl et al. 2018) presenting roundtable discussions on resilience for military readiness and preparedness from five domains in a point-counterpoint format: physiological versus psychological resiliency, differences of sex, contributions of aerobic and strength training, thermal tolerance, and the role of nature versus nurture. The authors conclude that interconnectedness of those five domains calls for interdisciplinary approach to build resilience and argue that this can be enhanced by training in realitybased scenarios.

Several studies on cyber operator performance followed NDCA cadets during a cyber defence exercise (Knox et al. (2019), Jøsok et al. 2019, and Knox et al. 2020). This exercise is run in a cyber range, a closed virtual system, where different information systems can be built, operated, used, attacked and defended. The exercise is based on real life scenarios and from the human point of view we have used for example malicious mass targeting and malicious individual targeting as a way to enter the system. We have influenced the students by media coverage and human intelligence about demonstrations and political disturbance and put students to handle the communication with the public. An important issue is that the students are responsible for how their group behaves and works. Each group has a mentor giving guidance related to the actual cyber defence, but how the students solve both internal issues and other exercise scenario related issues is their own responsibility.

Cyber power is increasingly used in information operations to target individuals as assets in digital information system. To enhance individuals' resistance against such offensive operations, Paul and Elder's (2005) notion of the critical consumer of information seems useful. The notion refers to persons capable of exercising critical thinking in a larger, informative and cultural context. By asking questions beginning with "what", "how" and "why" a critical consumer extends attention beyond the actual incident, focuses on the big picture, understand the dynamics that influence him/her and gains a broader situational awareness.

Summing up, we find that educational approaches that encourage self-regulation and critical thinking can help develop more officers that are more resilient to the negative effects of digital influence.

References

Bakir, V. and McStay, A.: Fake news and the economy of emotions. Digital Journalism 6(2), 154–175 (2018). https://doi.org/10.1080/21670811.2017.1345645, https:// doi.org/10.1080/21670811.2017.1345645

Dragano, N. and Lunau, T.: Technostress at work and mental health: concepts and research results. Current Opinion in Psychiatry 33(4), 407–413 (July 2020)

Forsvarsstaben (2007) Forsvarets fellesoperative doctrine. Oslo: Brødr. Fossum AS

Helkala, K., Knox, B., Jøsok, Ø., Lugo, R. and Sütterlin, S.: How Coping Strategies Influence Cyber Task Performance in the Hybrid Space. In: Proceedings of the HCI International 2016 - Posters' Extended Abstracts. Communications in Computer and Information Science. vol. 617, pp. 192–196 (2016)

Helkala, K., Knox, B.J. and Jøsok, Ø.: How the application of coping strategies can empower learning. In: 2015 IEEE Frontiers in Education Conference (FIE), El Paso, TX. pp. 1–8 (2015)

Jøsok, Ø., Lugo, R.G., Knox, B.J., Sütterlin, S. and Helkala, K.: Self-Regulation and Cognitive Agility in Cyber Operations. Frontiers in Psychology (2019)

Knox, B.J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R.G. and Sütterlin, S.: Socio-technical communication: The hybrid space and the OLB model for science-based cyber education. Military Psychology 30(4), 350– 359 (2018). https://doi.org/10.1080/08995605.2018.1478546, https://doi.org/10.1080/08995605.2018.1478546

Knox, B.J., Lugo, R.G., Helkala, K.M. and Sütterlin, S.: Slow Education and Cognitive Agility: Improving Military Cyber Cadet Cognitive Performance for Better Governance of Cyberpower. International Journal of Cyber Warfare and Terrorism (IJCWT). 2019, 9 (1), 48-66 9(1), 48–66 (2019)

NATO: Allied Joint Doctrine for Information Operations AJP-3.10. (2009) https://info.publicintelligence.net/NATO-IO.pdf

Nindl, B.C., Billing, D.C., Drain, J.R., Beckner, M.E., Greeves, J., Groeller, H., Teien, H.K., Marcora, S., Moffitt, A., Reilly, T., Taylor, N.A., Young, A.J. and Friedl, K.E.: Perspectives on resilience for military readiness and preparedness:Report of an international military physiology roundtable. Journal of Science and Medicine in Sport 21, 1116–1124 (2018)

Paul, R. and Elder, L.: Critical Thinking Competency Standards: A Guide for Educators. Foundation for Critical Thinking (2005)

Sellberg, C., Susi, T.: Technostress in the office: a distributed cognition perspective on humantechnology interaction. Cognition, Techology & Work 16, 187–201 (2014)

Shaw, M. and Black, D.W.: Internet Addiction: Definition, Assessment, Epidemiology and Clinical Management. CNS Drugs 22(5), 353–365 (2008)

Taylor, P.: Munitions of the mind: A history of propaganda from the ancient world to the present day. Manchester: Manchester University Press (2003)

United Kingdom Ministry of Defence: Allied Doctrine for cyberspace operations – AJP-3.20 (2020). https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320