Inland Norway
University of
Applied Sciences

Faculty of Social and Health Sciences

Øyvind Jøsok

PhD Dissertation

Cyber Operator Competencies

The Role of Cognitive Competencies in Cyber Operator Practice and Education

PhD in Child and Youth Participation and Competence Development
2020

Øyvind Jøsok

Cyber Operator Competencies

The Role of Cognitive Competencies in Cyber Operator Practice and Education

PhD Thesis

2020

Faculty of Social and Health Sciences

Inland Norway
University of
Applied Sciences

Printed by: Flisa Trykkeri A/S

Place of publication: Elverum

PhD Thesis in Child and Youth Participation and Competence Development no. 17

ISBN printed version: 978-82-8380-202-3

ISBN digital version: 978-82-8380-203-0

ISSN printed version: 2535-7433

ISSN printed version: 2535-7441

Abstract

The theme of this thesis is the role of cognitive competencies in cyber operator practice and education. Cyber operator practice is a new field of research where the importance and attention is growing rapidly. Research has accumulated a solid amount of knowledge about the technical skills required by a cyber operator. However, less is known about the *cognitive competencies* that support cyber operator proficiency. In order to gain insight into the cognitive demands of cyber operators, the cognitions of young cyber officers[1] attending the Norwegian Defence Cyber Academy have been studied. Findings contributes to the development of theory and evidence-based knowledge needed to develop educational guidelines for the cyber operator workforce.

This dissertation proposes and take steps towards validation of a conceptual framework, The Hybrid Space, that describes the cognitive work environment of military cyber operators. The Hybrid Space conceptual framework is introduced in the first article of this thesis and is used in all parts of the study. Methodological contributions include a method and a software to collect quantitative data on cyber operators' cognitive focus and assess cognitive agility. Cognitive agility is proposed as a competence and a measure of cyber operator performance. Empirical data collected during a cyber defence exercise support our theoretical assumption and helps to further develop The Hybrid Space conceptual framework.

Findings indicate that knowledge and understanding of cyberspace as a domain of operations and the cognitive competencies supporting cyber operator proficiency are limited. Cognitive agility is proposed as a cognitive competency and is associated with higher levels of self-regulation. These findings suggest that cognitive competencies can indeed support cyber operator performance. This thesis therefore contributes to cyber operator practice and education by suggesting that education and training would benefit from including the development of cognitive competencies alongside the technical education and training needed to become a cyber operator. In this way, this thesis adds new insight and perspective into the novel area of cyber operator practice. The results provide the first indications that cyber operator performance can be supported by the development of cognitive competencies during education.

[1] Cyber officer and cyber operator are used interchangeably throughout the articles and this extended abstract. The reason is that the students undergo the same education, but the position they later get determine their career path and the accompanying title. The use of the terms is maturing in both military and civilian sectors. As of now neither finite guidelines nor agreed upon norms exist that guide the use of the titles.

Sammendrag

Temaet for denne doktoravhandlingen er rollen til kognitive kompetanser i cyber operatør praksis og utdanning. Cyber operatør praksis er et nytt forskningsfelt som har fått stor oppmerksomhet de siste årene. Forskning på området har produsert kunnskap om hvilke tekniske kunnskaper og ferdigheter en cyber operatør må ha. Mindre kunnskap finnes om de kognitive kompetansene som en cyber operatør trenger for å kunne utøve sin praksis effektivt. For å få bedre innsikt i de kognitive kravene som cyber operatører stilles ovenfor har jeg studert unge cyber offiserer under utdanning på Forsvarets Ingeniørhøgskole[2] (FIH). Denne avhandlingen bidrar med kunnskap og empirisk grunnlag for å utvikle forskningsbasert utdanning for fremtidens cyber operatører.

Avhandlingen fremholder og starter validering et konseptuelt rammeverk, The Hybrid Space, som beskriver de kognitive kravene militære cyber operatører må forholde seg til i utøvelsen av sitt virke. Rammeverket blir introdusert i første artikkel av denne avhandlingen og blir brukt som konseptuelt fundament i resten av avhandlingen. Avhandlingen fremlegger også en metode og et dataverktøy som kan brukes til å samle inn kvantitative data om cyber operatørers kognitive fokus. Dette dataverktøyet kan også benyttes til å undersøke hvordan cyber operatører utviser kognitiv fleksibilitet over tid når de gjennomfører en cyber operasjon. Kognitiv fleksibilitet foreslås som et prestasjonsmål for cyber operatører. Empiriske data innhentet under en cyberforsvars øvelse bekrefter våre teoretiske hypoteser og bidrar til videre utvikling av det konseptuelle rammeverket.

Hovedfunnene indikerer at kunnskap om og forståelse for cyberspace som operasjonsdomene og rollen til kognitive kompetanser i cyber operatørens utførelse av cyber operasjoner er begrenset. Denne avhandlingen argumenter for at evne til fleksibel kognitiv manøver i operasjonsmiljøet, definert som 'cognitive agility', er en viktig kognitiv kompetanse for cyber operatører som kan predikeres ved å undersøke evne til selvregulering. Disse funnene indikerer at kognitive kompetanser kan bidra til å understøtte cyber operatørers prestasjon. Avhandlingen bidrar til cyber operatør praksis og utdanning ved å vise til at utvikling av cyber operatør kompetanse bør inkludere utvikling av kognitive kompetanser i tillegg til utvikling av tekniske kunnskaper og ferdigheter. Med disse funnene bidrar denne avhandlingen bidrar til ny innsikt og perspektiv på cyber operatør praksis og utdanning.

[2] Forsvarets Ingeniørhøgskole (FIH) endret i 2018 navn til Cyberingeniørskolen (CIS) og ble samtidig underlagt Forsvarets Høgskole (FHS).

Preface

This PhD always felt like a bold quest. But thanks to the people who have nurtured me with motivation and persistence, it has been equally a fun journey as a bold quest. Working with this thesis has been a journey into the future of a more digitized society and hybrid reality. Being forced to critically evaluate the promises and perils of an interconnected digitized society - and reflect upon how this influences people, has led me to value the people more and the technology less. For me, quality of life, happiness and harmony is all about the people I know and the relationships I nurture. This is where I collect my energy, motivation, optimism and persistence.

My late Grandmother always said; *"work hard, you can rest when you are dead[3]"*. A saying that pretty much sums up my upbringing on a small farm on the West coast of Norway. An upbringing I value and cherish to full extent and hope to pass to the next generation. Thank you, Mom and Dad, for giving me all your love, freedom and support I have ever needed. Thank you also to my siblings who shared the same invaluable upbringing - you mean everything to me.

Thank you to the Norwegian Defence Cyber Academy, where I started my military career, who allowed me to pursue this PhD while working as an instructor in leadership. Allowing me to use the annual Cyber Defence Exercise and allowing me access to the students as my main source of data has made this research possible. A special greeting to the new generation of cyber officers that have been studying at Norwegian Defence Cyber Academy during my years as an instructor. Without you, your ideas, your creativity, your thoughts and willingness - this project would not have been possible.

Thank you to my colleagues in my research group. Professor Stefan Sütterlin, for everything. Having access to you at any time has been a total pleasure. Professor Kirsi Helkala for daily support and for your persistence in making this happen. Dr. Ric Gregorio Lugo for always making me smile and laugh while doing statistical analysis, collecting data, developing ideas, writing or just hanging around.

Last but not least, an enormous thanks to the Knox family. I am in deep gratitude for the contributions from both of you. Without you Silje, the agreement and cooperation with Inland

[3] In Norwegian: *"Stå på stå på, i graven får du hvile"*.

University of Applied Sciences would not have seen daylight. Thank you for your persistence and engagement. You ensured it happened and then secured its survival. Ben, you merged the academic curriculum with the practical military subjects into the exercises at Norwegian Defence Cyber Academy. Years of hard work, ups and downs, only your level of grit could break through the ingrained codes of conduct and make something novel. You designed the Cyber Defence Exercise and all the other exercises at Norwegian Defence Cyber Academy. You co-developed The Hybrid Space and you believed in it harder than anyone else. We travelled the world with the Hybrid prophecy and a 'black snowman' that no one has yet disproved. What a ride. Invaluable contributions morning, day and evening, weekends and holidays. I owe you big time.

My PhD project was supported morally and financially by the Norwegian Cyber Defence Academy and the Norwegian Joint Headquarters. Thanks for giving me the necessary permission and support.

Thanks to the PhD Students and employees at the Child and Youth Participation and Competence Development research programme who have included me and expanded my academic horizon considerably. Special thanks to Professor Emeritus Harald Thuen who believed in my project and decided to put me on the programme. Without you all I wouldn't be so well versed in the extremely important area of children and young people's competence development; which I have come to value greatly.

Paul Ward, Joel Suss, Guler Arsal, Mass Soldal Lund, Odd Sveinung Hareide, Olav Kjellevold Olsen, Lena Westby, Pete Khooshabeh, Mathias Hedberg, Terje Ødegaard, Kyle Wilson and all the other people that have contributed with fortuitous encounters. Thank you.

Finally, this is a chance to recognize those who have travelled along with me on this journey. Thank you Linda - the love of my life and the best friend there is. You keep my feet on the ground and remind me every day that there is more to life than a PhD. I love you.

A final thanks to my family and friends – you are everything.

List of publications

The following articles are included as a part of this thesis:

Article 1: **Jøsok, Ø.**, Knox, B. J., Helkala, K., Lugo, R., Sütterlin, S., & Ward, P. (2016). Exploring the Hybrid Space Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations. In S. D. & F. C. (Eds.), Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience Lecture Notes in Computer Science (Vol. 9744, pp. 178-188): Springer, Cham. doi:https://doi.org/10.1007/978-3-319-39952-2_18

Article 2: Knox, B. J., **Jøsok, Ø.**, Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R. G., & Sütterlin, S. (2018). Socio-technical communication: The Hybrid Space and the OLB-Model for science-based cyber education. Military Psychology 30(4), 350-359. doi: 10.1080/08995605.2018.1478546.

Article 3: **Jøsok, Ø.**, Knox, B. J., Wilson, K., Helkala, K., Lugo, R. G., Sütterlin, S., & Ødegaard, T. (2017). Macrocognition applied to The Hybrid Space: Team environment, functions and processes in cyber operations. In S. D. & F. C. (Eds.), Augmented Cognition. Enhancing Cognition and Behavior in Complex Human Environments Lecture Notes in Computer Science (Vol. 10285, pp. 486-500): Springer, Cham. doi:https://doi.org/10.1007/978-3-319-58625-0_35

Article 4: **Jøsok, Ø.**, Hedberg, M., Knox, B. J., Helkala, K., Sütterlin, S., & Lugo, R. G. (2018). Development and Application of the Hybrid Space App for Measuring Cognitive Focus in Hybrid Contexts. In D. D. Schmorrow & C. M. Fidopiastis (Eds.), Augmented Cognition: Intelligent Technologies Lecture Notes in Computer Science (Vol. 10915, pp. 369-382). Cham: Springer. doi:https://doi.org/10.1007/978-3-319-91470-1_30

Article 5: **Jøsok, Ø.**, Lugo, R. G., Knox, B. J., Sütterlin, S., Helkala, K. (2019) Self-regulation and cognitive agility in cyber operations. Frontiers in Psychology 10(875). doi:10.3389/fpsyg.2019.00875.

Table of contents

Abstract i

Sammendrag iii

Preface v

List of publications vii

Table of figures xi

List of tables xi

1 Introduction 2

1.1 Aims and research questions 3

1.2 The Norwegian context 7

1.3 The research programme context 10

1.4 Central concepts 12

1.5 Structure of the thesis 15

2 State of art 16

2.1 Conceptualization of the cognitive work environment of cyber operators 17

2.2 Cyber operator practice 22

2.3 Cyber operator cognitive competencies 24

2.4 Research gaps in cyber operator practice and education 27

3 Theoretical perspectives 30

3.1 Social cognitive theory 30

3.1.1 Self-regulation 32

3.1.2 Functions and processes of self-regulation 33

3.1.3 Competence models 35

3.1.4 Application of social cognitive theory in this thesis 38

3.2 Macrocognition 39

3.2.1 Functions and processes of macrocognition 40

3.2.2 Application of macrocognition in this thesis 42

3.3 Summary of theoretical perspectives 42

4 Data and methodology 44

4.1 Part 1: Development and exploration of The Hybrid Space conceptual framework 44

4.2 Part 2: Developing a method and a software to collect empirical data 47

4.3 Part 3: Collecting and analyzing quantitative data on cyber operator cognitive agility and self-regulation. 50

4.4 Literature review 53

4.5 Validity and reliability 55

4.5.1 Validity and reliability in general 55

4.5.2 Part 1 56

4.5.3 Part 2 57

4.5.4 Part 3 58
4.5.5 Summary on validity and reliability 58
4.6 Researching young people 59
4.7 Ethical considerations 60
4.8 Methodological strengths and limitations 61
5 Summary of the articles 64
5.1 Article 1 64
5.2 Article 2 66
5.3 Article 3 68
5.4 Article 4 69
5.5 Article 5 70
6 Concluding remarks 72
6.1 Conceptual contributions 72
6.2 Methodological contributions 73
6.3 Empirical contributions 74
6.4 Implications 75
6.4.1 Implications for national policy makers 75
6.4.2 Implications for military education 75
6.4.3 Implications in a wider context 76
6.5 Limitations 77
6.6 Future work 79
References 80

Table of figures

Figure 1. 1: The Hybrid Space (Jøsok et al., 2016) 13

Figure 2. 1: Layers of cyberspace (Department of Defense, 2018) 19
Figure 2. 2: Cyberspace – domains and dimensions of the operational environment (Kampenes, 2018). 20
Figure 2. 3: The Lockheed Martin Cyber Kill Chain (Lockheed Martin, 2019) 23

Figure 3. 1: Triadic reciprocal determinism (Bandura, 1986) 31
Figure 3. 2: Social cognitive theory including The Hybrid Space 32
Figure 3. 3: Self-regulation subfunctions adopted from Bandura (1986) 33
Figure 3. 4: Hierarchy of competence 36
Figure 3. 5: Competence construct model on digital competencies (Ferrari, 2012) 37
Figure 3. 6: Macrocognition - Functions and processes (Macrocognition, 2016) 41

Figure 4. 1: Data collected during the 2016 CDX 47
Figure 4. 2: The Hybrid Space App participant window. 49
Figure 4. 3: Example data collected by the Hybrid Space App. 49
Figure 4. 4: Operationalization of The Hybrid Space movements. 50
Figure 4. 5: Experimental setup. 52
Figure 4. 6: Overview of validity and reliability constructs 56

Figure 5. 1: OLB pedagogy at the NDCA 67

List of tables

Table 1. 1: Overview of articles and findings 6

1 Introduction

This thesis investigates the role of cognitive competencies in cyber operator practice and education. A central presupposition is that the emergence of cyber operator practice is a direct consequence of the digitization of society. Digitization of society is an ongoing process where information and communications technology (ICT) is increasingly interconnected by wired and wireless networks, that in turn are connected to the internet at a global scale to aid communication and data exchange - creating cyberspace[4]. Today, cyberspace is an integral part of almost all human activity, in private and professional life and in every sector of society (Baker, 2016; Castells, 2010; Norman, 2017; Postman, 1993; Tapscott, 2014). Therefore, digitization of society is, in this thesis, understood as the merging of cyberspace and society, resulting in a 'digitized society' that is characterized by dependency on *"...digital technologies, software, platforms, media and social and digital networks for interaction, connectedness, both at work and in people's everyday lives"* (Fransson, 2016, p. 186).

As societies continue to transfer services, information, communications and infrastructure control into cyberspace to harvest the promises of digitization, perils such as new forms of digital dependencies and cybercrimes[5] are created. The interconnectedness of the physical world and cyberspace at all levels of society results in humans who now operate extensively in a hybrid environment[6] (Fransson, 2016). A hybrid environment is, in the context of this thesis, the environment that both military and civilian cyber operators operate in. This environment is characterized by a complex relationship between cyberspace and physical reciprocal determinants, requiring an interdisciplinary[7] research approach merging understanding of human behavior and cyber security to unravel (Pfleeger & Caputo, 2012).

Emergence of a cyber security workforce, consisting of cyber security professionals, military cyber officers and cyber operators is becoming apparent worldwide (Baker, 2016) as the

[4] Cyberspace is defined as; "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Department of Defence, 2018).

[5] Cybercrime refers to; "…any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network" (Cross, 2008, p. 11).

[6] Hybrid environment is in this thesis understood as a conflation of physical domains and cyberspace - and seen as a direct consequence of digitization of society.

[7] Interdisciplinary research is understood as: *"...a process of answering a question, solving a problem, or addressing a topic too broad or complex to be dealt with adequately by a single discipline or profession... IDS draws on disciplinary perspectives and integrates their insights through construction of a more comprehensive perspective"*(J. T. Klein & Newell, 1996, p. 3)

global demand for skilled cyber security professionals[8] increases (ISC, 2018). In Norway, it is assessed that by 2030 the lack of skilled cyber security professionals will be 4100 (NIFU, 2017). However, cyber operator tasks, competence requirements and performance are unresolved concepts lacking clear definition and guidelines to support selection, education and training (Dawson & Thomson, 2018; Sobiesk, Blair, Conti, Lanham, & Taylor, 2015).

While technical ICT competence is paramount to operate in cyberspace, human factor researchers argue to focus on developing multiple skill-sets rather than focus solely on technical proficiency (Buchler et al., 2018; Anita D'Amico, Buchanan, Kirkpatrick, & Walczak, 2016; Dawson & Thomson, 2018; Jabbour, 2010; Røislien, 2015; Tapscott, 2014). These theories of cyber operator competence rest on the notion that technical skills alone are not enough to perform, due to the human aspects and hybrid character of the cyber operator work environment (Buchler et al., 2016; Jøsok et al., 2016). However, most of these theories still lack empirical underpinning. Also research and understanding of the cognitive processes that support mastery of such hybrid environments and how contextual understanding contribute to cyber operator proficiency are scarce (Ben-Asher & Gonzalez, 2015).

1.1 Aims and research questions

The main goal of this project is to investigate the role of cognitive competencies in cyber operator practice and education applying a quantitative methodology, supported by literature review and concept development. This thesis has utilized The Norwegian Defence Academy's (NDCA) annual Cyber Defence Exercise (CDX) as its main source of data and its student participants as the inspiration and knowledgeable participants. The research is therefore situated in a military educational context and influenced by this practice. The main research question is: **What is the role of cognitive competencies in cyber operator practice and education?** This main question is further broken down into six research questions that are addressed across the articles:

RQ1: How can the cognitive work environment of cyber operators be described?
RQ2: How can dyadic interaction in The Hybrid Space be described?

[8] Cyber security professional is the most common used expression designating personnel who defend assets in the civilian sectors from the threats associated with cyberspace. The corresponding designator in the military sector is cyber operator. However, due to similarities in work environment and tasks they frequently are identified as a part of the same workforce (Baker, 2016; Newhouse, Keith, Scribner, & Witte, 2017).

RQ3: How can team interaction in The Hybrid Space be described?
RQ4: In what ways might cognitive competencies support cyber operator performance?
RQ5: How can The Hybrid Space conceptual framework be operationalized?
RQ6: What is the association between self-regulation and cognitive agility in The Hybrid Space?

These questions have guided the research presented in the articles through three parts:

1. Development and exploration of The Hybrid Space conceptual framework.
2. Developing a method and a software to collect empirical data.
3. Collecting and analyzing quantitative data on cyber operator cognitive agility.

The initial part of the project has been to develop the theoretical foundation of The Hybrid Space conceptual framework. The framework was first presented in 'Exploring the Hybrid Space - Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations' (Jøsok et al., 2016). Secondly, The Hybrid Space was utilized to describe dyadic interaction and explore the role of communication in cyber operator practice and education. The article 'Socio-technical communication: The Hybrid Space and the OLB-Model for science-based cyber education' (Knox et al., 2018) sheds light on how cyberspace challenges power relations by disrupting traditional competence structures and advocates the need for grounded communication to reduce the risks in safety-critical contexts. Third, The Hybrid Space was explored to include the team aspect. In the article 'Macrocognition applied to The Hybrid Space: Team environment, functions and processes in cyber operations' (Jøsok et al., 2017) cyber operator team functions and processes is discussed and it is argued that cyber operator work is best suited for study in a naturalistic environment.

The second part of this project has been to operationalize The Hybrid Space and develop a method to collect data on cyber operator cognitive focus. The article, 'Development and application of The Hybrid Space app for measuring cognitive focus in hybrid contexts.' (Jøsok, Hedberg, Knox, Helkala, Sütterlin, et al., 2018), presents the development and application of The Hybrid Space app - a software tool that was developed to collect and visualize self-reported cognitive focus of cyber operators in action. Article four also presents the operationalization of the cognitive agility construct.

The third part of this project has been to validate The Hybrid Space conceptual framework. Article five, 'Self-regulation and cognitive agility in cyber operations' (Jøsok, Lugo, Knox, Sütterlin, & Helkala, 2019) investigates cyber cadets' level of self-regulation and ability to manoeuvre in The Hybrid Space.

An overview of the articles and their contributions to answer the research questions is provided in table 1.1.

	Article 1	Article 2	Article 3	Article 4	Article 5
Title	Exploring the Hybrid Space -Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations	Socio-technical communication: The Hybrid Space and the OLB-Model for science-based cyber education	Macrocognition applied to The Hybrid Space: Team environment, functions and processes in cyber operations.	Development and application of The Hybrid Space app for measuring cognitive focus in hybrid contexts	Self-regulation and cognitive agility in cyber operations.
RQ	RQ1	RQ2, RQ5	RQ3, RQ4	RQ4, RQ5	RQ4, RQ5, RQ6
Published	Published in Lecture Notes in Computer Science, Vol. 9744	Published in Military Psychology, Vol. 30 nr. 4.	Published in Lecture Notes in Computer Science, Vol. 10285	Published in Lecture Notes in Computer Science, Vol. 10915	Published online in Frontiers in Psychology.
Method	Literature review of current perspectives of cyber operations, socio-technical systems and cyber physical systems.	Literature review of communication in safety critical context.	Literature review of teamwork in cyber operations and macrocognition.	Specification and development of a data collection software. Literature search on cyber operator performance.	Quantitative method. Data collection using The Hybrid Space App and questionnaires.
Findings	Current approaches to understanding cyberspace and its implications to military operations are insufficient. The importance of cyberspace raises the demands for structure and content of education and training, the need for a better understanding of the relationships between cyberspace and the physical domain and better understanding of the cognitive challenges to cyber operators. A growing number of researchers advocating for a varied skill-set amongst cyber operators. The Hybrid Space Conceptual Framework is presented.	Lessons from safety-critical socio-technical systems demonstrate the importance of communication in such contexts. The literature review identify a lack of research literature that focuses on the role of communication in military cyber operations. We conclude that educators of military cyber operators need to acknowledge the need to teach and train the non-technical competencies of cyber operators. The OLB-model is presented and contextualized by using NDCA as an example.	Inspired by the macrocognitive perspective this article advocates the need for studying cyber operators in their natural environment to mirror real-life demands. The literature review identifies three factors that can contribute to the breakdown of cyber operator team performance; team structure, team communication and information overload. Findings add facts to the notion of cyber operator work being cognitively demanding.	The literature search concludes there are no available methods that are designed to capture the cognitive focus of cyber operators as well as no agreed upon performance measures of cyber operator work. Development of the Hybrid Space app is presented, and its application is discussed. Cognitive agility is defined and operationalized as cognitive movements within the boundaries of The Hybrid Space.	The state of art review in this article concludes that cyber operator tasks, competence requirements, and performance are unsettled concepts that lack clear definition and guidelines to support selection, education, and training. The results from the experiment support the hypothesis by showing that self-regulation predicts cognitive agility in cyber operators.
Candidate contribution	ØJ contributed to the ideas, development and design of The Hybrid Space. ØJ contributed to preparation, drafting, necessary theory research, and write up of all parts of the manuscript. ØJ performed the final proof reading and co-presented the article at the conference. ØJ approved the final version of the article for publication.	ØJ contributed to the conceptual design and development of the OLB-Model. ØJ contributed to preparation, drafting, necessary theory research, and write up of all parts of the manuscript. ØJ approved the final version for publication.	ØJ contributed to the ideas, development and preparations of the article. ØJ contributed to drafting, necessary theory research, and write up of all parts of the manuscript. ØJ performed the final proof reading and presented the article at the conference.	ØJ contributed to the ideas, conceptual development and specification of the Hybrid Space App. ØJ contributed to preparation, drafting, necessary theory research, and write up of all parts of the manuscript. ØJ performed the final proof reading and co-presented the article at the conference.	ØJ contributed to all parts of the project from idea development to data collection, data analysis and data presentation. ØJ contributed to preparation, drafting, necessary theory research, and write up of all parts of the manuscript. ØJ performed the review process, final proof reading and all interaction with the editor and reviewers.

Table 1. 1: Overview of articles and findings

1.2 The Norwegian context

This study has been performed in the context of Norwegian military cyber operator practice and education. However, articles one to five refer mainly to international research - as few studies in the scientific area of cyber operator practice and education situated in the Norwegian context is to be found. As nations differ in how they comprehend and envision cyber operator practice and education, this section will elaborate on the Norwegian context by examining governmental and military policy documents to enable this study to be situated in this context.

Norway is currently the fourth most digitized country in the world (World Economic Forum, 2016), and the Government's strategy is to continue to utilize ICT to further develop all sectors of society to make everyday life simpler and to secure wealth and prosperity for all (Ministry of Local Government and Modernisation, 2016; Ministry of Finance, 2017). The Norwegian Government's recent cyber security vision implicitly state that a digitized society require ability to protect individuals, business and democracy against cyber threats: *"In Norway, it is safe to use digital services. Private individuals and companies have confidence in national security, and trust that the welfare and democratic rights of the individual are being safeguarded in a digitalised society"* (Norwegian Ministers, 2019, p. 7).

A recent study of how Norwegian sectors approach handling the effects of cyberpower[9] describes the situation as a 'Faustian bargain' where *"...dealing with the immediate vulnerabilities and insecurities arriving through cyberspace, displaces individuals and organizations ability to focus on long-term strategies"* (Knox, 2018, p. 9). This indication of a mismatch between the level of digitization and competence to master the effects of digitization is also a growing concern in relation to protecting the values of the nation state of Norway (Ministry of Justice and Public Security, 2017; Waterhouse, 2013). Threat assessments by the Norwegian Secret Services, The Norwegian Intelligence Service (2019), The Norwegian Police Security Service (2019) and The Norwegian National Security Authority (2019) stress that Norwegian businesses and Norwegian interests are under strain and that digitization in combination with globalization has created new arenas for crime intended for economic gain, spying and sabotage. The Norwegian Intelligence Service states that foreign intelligence gathering, influence and sabotage are the most pressing cyber threats

[9] Cyberpower is defined by Knox (2018) as *"...the capability to influence tangible and intangible assets through digital means"*. (p. 11)

against Norwegian interests, and warns that threat actors take advantage of and exploit human weaknesses in cyberspace (The Norwegian Intelligence Service, 2018):

> Data storage and processing is becoming intrinsic to all human activity, and our perception of reality is increasingly being conveyed through digital systems. Developments are not limited to infrastructure, industrial processes and service provision, but also include opinion formation and social interaction. The growing significance of cyberspace challenges physical borders and the structural balance of power. Cyber threats take advantage of technical vulnerabilities and human weaknesses in cyberspace. (The Norwegian Intelligence Service, 2018, p. 34)

Within the national borders of Norway several major cyber-attacks have been uncovered in the last few years. In 2018 the South-Eastern Norway Health Authority was targeted in a cyber operation, resulting in extensive loss of patient data to unknown attackers (Norwegian Police Security Service, 2018). The same year a cyber operation targeted against one or several County Governors in Norway was carried out, resulting in unavailable ICT systems and potential loss of data (Brombach, 2018). A more recent example is the targeted cyber operation against Norwegian Hydro (NRK, 2019). These examples illustrate some of the complexity of the current cyber threat environment, the vulnerability of critical national functions, the challenge of attribution and the low level of awareness associated with the challenges of digitization (MacDonnell, 2014). The security of a digitized society calls for a holistic approach and new forms of civil-military, private-public and international cooperation (Norwegian Ministers, 2019). On these grounds, the Lysne 2 report recently proposed to establish a Digital Border Defence (Lysne, 2016) to supplement the already established national Norwegian Computer Emergency Response Team (NorCERT).

In the military sector, the emergence of cyberspace poses new and novel challenges for military forces and military decision makers (Libicki, 2016). Utility of cyberspace in combination with other non-conventional means and conventional military power has led to new terms like ‘hybrid warfare’ (Caliskan, 2019; Renz, 2016), ‘non-linear warfare’ (Galeotti, 2014) and ‘multi-domain battles’ (Tan, 2016). The notion of hybrid warfare is substantially complexifying modern warfare and national security by blurring the lines between peace and war, challenging the concept of national borders and the role of sectors of government (Lysne, 2016; Maness & Valeriano, 2015; Ministry of Justice and Public Security, 2017). Reviewing the recent developments, it is clear that cyber warfare is a topic of global concern (Robinson, Jones, & Janicke, 2015). However, the use of cyberspace in military operations is still new, and poses both operational and research challenges (Borghetti, Funke, Pastel, & Gutzwiller, 2017; Choo, 2011; Jabbour, 2009; Rantapelkonen & Salminen, 2013).

Articles one to three of this thesis explores utility of cyberspace in the military context with focus on the emergence of cyber operator practice and education. Findings include that the increased utility of and reliance upon cyberspace in military operations has led to higher demand for qualified cyber personnel (M. Champion, Jariwala, Ward, & Cooke, 2014). This is demonstrated through investment in cyber defence units, cyber defence education (Caulkins, Badillo-Urquiola, Bockelman, & Leis, 2016; Newhouse et al., 2017) and NATO guidelines for defending cyber assets as a collective effort ensuring that NATO Article V is valid in case of cyberattacks (NATO, 2016a; The Ministry of Defence, 2014). By supporting the NATO cyber defence pledge Norway has acknowledged that qualified cyber operators is essential for any military force to be able to utilize cyberspace to support operations, to perform operations in and through cyberspace and to be able to protect increasingly complex civil-military value chains (Ministry of Justice and Public Security, 2017; NATO, 2016a).

Articles one to three find that the introduction of cyberspace as an operational domain is challenging how military power is employed and is associated with heightened complexity (Jøsok et al., 2016; Jøsok et al., 2017; Knox et al., 2018). At the same time articles one to five find that the competence profiles of cyber operators intended to govern and operate in cyberspace is still somewhat unclear (Jøsok, Hedberg, Knox, Helkala, Sütterlin, et al., 2018; Jøsok et al., 2016; Jøsok et al., 2017; Jøsok et al., 2019; Knox et al., 2018). Situating these findings in the Norwegian context discloses a situation where the need for cyber operators are acknowledged, but significant uncertainty of how cyber operator practice and education will be operationalized and developed are present. The Chief of Defence concludes in his advice on the further development of the Armed Forces that: *"The capability of the Armed Forces to conduct cyber operations to achieve effect, situational understanding and protection in the cyber domain is low"* (Chief of Defence, 2019, p. 31). Further he acknowledge that knowledge and expertise in cyber operations need to be strengthened and included in training and education in the Norwegian Armed Forces (Chief of Defence, 2019). However, as described in this extended abstract and in the articles of this thesis; the competence requirements and performance measures of cyber operator practice is currently inconclusive and focused towards technical proficiency. Therefore, this thesis primarily aims at informing

Norwegian policymakers, military decision makers and cyber operator education on the competence requirements beyond technical proficiency. Results will also inform cyber operators working for companies in civilian and private sectors like e.g. telecom or finance, as well as civilian educational institutions within the area of ICT and cyber security.

1.3 The research programme context

This study focusses on the role of cognitive competencies in cyber operator practice and education and is performed as a part of the research program: Children and Young People's Participation and Competence Development (BUK). This interdisciplinary research program acknowledge that digitization of society[10] changes and complexifies the practices, professions and communities that people engage in (BUK, 2010). Norwegians can still choose to communicate non-digitally with Governmental Services, but the option to be a digital bystander in society is gradually vanishing (Lysne, 2016). Every citizen in Norway, young and old, can access cyberspace and participate in and through cyberspace on a daily basis and consequently becomes a potential target to the threats of cyberspace (Fransson, 2016; Norwegian Ministers, 2019).

Adaptation to new complexities, in this case the threats of cyberspace, imply that people need to *"…continually revise and update their competences"* (BUK, 2010, p. 3). In the BUK research programme, competence development is described as an ongoing, life-long learning process in which individuals continuously assess, re-evaluate and develop their competence in interaction with their environment (BUK, 2010). The mediating role of digital technologies is one of BUK's focus areas. The programme description asserts that the use of new digital technology significantly contributes to societal complexity. BUK acknowledges that humans are born into a world characterized by digital information and communication technologies and that they live with technologies such as computers, the Internet, social media and cell phones more as a 'cultural form' than as pure technologies (BUK, 2010). The term 'digital natives' has been used to describe the product of 'growing up digital' and defines digital natives as consumers surrounded by technology being able to 'talk the digital language' (Prensky, 2001). However, labeling a generation as digital natives also sparked a notion of digital natives being abundantly digitally competent (Bennett, Maton, & Kervin, 2008;

[10] The Children and Young People's Participation and Competence Development research program acknowledges the *"…explosive development of a media and information society…"* (p. 3) as one of four societal tendencies that the design of the research program should be seen in light of (BUK, 2010). In this thesis this societal tendency is referred to as digitization of society.

Helsper & Eynon, 2010; Ståhl, 2017). A notion that has been disproved repeatedly (Bennett et al., 2008). Instead, competence construct models of digital competence suggest that being digital competent in a digitized society requires multiple skill-sets, not only technical user competence (Ferrari, 2012). A suggestion that mirrors the proposed competence requirements of cyber operators. The chosen social-cognitive theoretical framework (Bandura, 1986) harmonizes with the social-cultural approach adopted by the BUK PhD programme (BUK, 2010). In both theoretical frameworks' individuals are not separated from their environment but engage with the environment in such a way that the individual both influences and is influenced by participation in practices related to the environment. The above-mentioned potential similarities in competence construct models and theoretical framework opens up for findings in cyber operator competence requirements to inspire and inform research in the area of Children and Young People's Participation and Competence Development as a part of being enculturated as a digital citizen.

This thesis indicates that cognitive competencies are important in cyber operator practice and that these competencies can be subject to development in education. The project meets key objectives for the research programme by presenting a versatile conceptual framework that can help access and research the complexities related to cyber operator practice; and develops new knowledge and understanding of the competencies related to coping with the cognitive demands in a digitized society. Applying these findings can help augment cyber security and cyber operator education beyond the military sector, as the digitized society demands more civil-military cooperation and civilian and military cyber operators are a part of the same workforce.

National educational institutions at all levels and sectors are starting to embrace digital skills and programming as important competencies for all citizens. Proposing development of cognitive competencies as an important contributor to master a digitized society could also contribute to development of such educational programs - at least it should be further explored to help augment the concept of digital competence in a broader sense than merely being able to use digital tools. Cognitive competencies are related to the ability to adapt to complex environments and results from this study imply that cyber operator education at university level would benefit from focus on such competencies in undergraduate education. The interdisciplinary approach of this project contributes to the programme's aim to help the breaking down of polarities between different research traditions and disciplines (BUK, 2010). Together with the other research in the BUK programme, these aspects of competence can help create new, holistic and interdisciplinary expertise in the field of child and youth participation and competence development.

1.4 Central concepts

This section will introduce two central concepts of this thesis. First, The Hybrid Space conceptual framework that are purposively developed for and used in all parts of this study; describing the cognitive work environment of cyber operators. Second, the concept of cognitive competencies will be introduced and defined to make clear the meaning of the concept and its application in this thesis.

1.4.1 The Hybrid Space

The Hybrid Space (See figure 1.1: The Hybrid Space) is introduced and described in article one (Jøsok et al., 2016). The conceptual framework describe that cyber operators work in a hybrid environment where both cyberspace and physical environmental cues are present (A. D'Amico & Whitley, 2008; Dawson & Thomson, 2018; Lathrop, Trent, & Hoffman, 2016). Their work environment is also characterized by a multi-layered sociotechnical system of people, organizations, nation states, computers and networks making cyber operations a cognitively intense task (McNeese et al., 2012). The Hybrid Space conceptual framework describes the hybrid character of the military cyber operator work environment and defines the cognitive space available for agile manoeuvre (See figure 1.1). The Hybrid Space framework allows the cyber operator to engage in strategic thinking while performing cyber operator tasks on a tactical level and it allows for cyber-physical sense-making traversing the cyberspace and physical domains. In article two and three, The Hybrid Space conceptual framework is developed to include the communication and team aspect (Jøsok et al., 2017; Knox et al., 2018), two important aspects of cyber operator work (Dawson & Thomson, 2018; McNeese et al., 2012). In article four The Hybrid Space conceptual framework is enabling development of The Hybrid Space application that is put to use in article five (Jøsok, Hedberg, Knox, Helkala, Sütterlin, et al., 2018; Jøsok et al., 2019).

The Hybrid Space conceptual framework allows for investigation and research interventions into the cognitive domain of cyber operator work. The cyber operator is situated in the center of The Hybrid Space to draw attention to the human as the converging point of sense-making and understanding of cause and effect in this space. The bi-directional arrows visualize the reciprocal relationship between the cyber operator and the different parts of the cognitive space. In the conduct of cyber operator practice, the operator has to continually relate to the physical environment, i.e. communicating with team members, receiving tasks, sharing information and conceptualizing physical components of the mission. At the same time the operator has to engage in cyberspace domain tasks i.e. network surveillance, coding, computer input/output (See chapter 2 and 4 for description of tasks). The cognitive position on the x-axis denotes the level of immersion into one or the other domain and subsequent movement in-between the extremities designates the need to support sense-making and situational understanding. The x-axis movements would continually be supported by low-level and high-level analysis and synthesis to further support sense-making and situational understanding. Low-level, referring to the need to dive into the details of a mission objective and perform in-depth malware analysis or coding. The strategic perspective on the y-axis continually supports the low-level analysis by providing the overall context in which the offensive or defensive operation is performed. The subsequent movement on the y-axis therefore designates the need to support situational understanding by shifting cognitive focus between low-level and high-level sense-making (See figure 4.1 for an example).

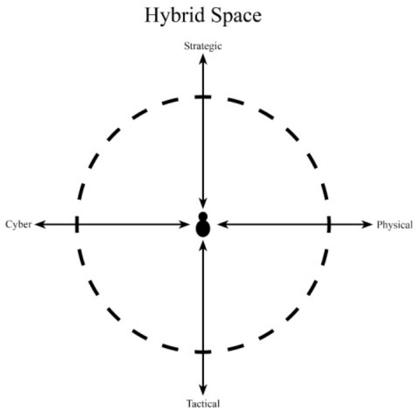


Figure 1. 1: The Hybrid Space (Jøsok et al., 2016)

The Hybrid Space conceptual framework is central to the understanding of the cognitive work environment of cyber operators and allows for understanding of the environmental influence on personal factors and behavior as a reciprocal process. The conceptualization of cyber operator practice and the role of cognitive competencies is further discussed in chapter 2 of this extended abstract as well as in articles one to five.

1.4.2 Cognitive competencies

The Hybrid Space conceptual framework implies that competencies needed to master the cyber operator work environment are strongly related to cognitive abilities. In article one this association was first proposed (Jøsok et al., 2016). Further, articles two and three find that cyber operator work is cognitive demanding (Jøsok et al., 2017; Knox et al., 2018). Therefore, the focus of this thesis is on the cognitive competencies of cyber operators.

A cognitive competency can be defined as: *"...a psychological construct that cannot be directly observed but can be inferred from an individual's behaviour or performance on content-relevant tasks"* (Wang, 1990, p. 219). In social cognitive theory, cognitive competencies are of vital importance in mastering complex environments and Bandura proposes that *"...the more uncertain the environmental information, the more one has to rely on inferential thought for guidance"* (Bandura, 1986, p. 39). However, given the same environmental conditions *"...people who have the capabilities for exercising many options and are adept at regulating their own behavior will have greater freedom than will those who have limited means of personal agency"* (Bandura, 1986 p. 36). Grounded in Banduras theory of regulating behavior as a pathway to performance in complex environments, and situated in the context of cyber operator practice, this study investigates if it is possible to distinguish between cyber operators that are more or less cognitive agile in The Hybrid Space. Article four discuss how cyber operator cognitive focus in The Hybrid Space can be operationalized and propose cognitive agility as a performance measure that can distinguish between operators based on their exercised level of cognitive movement (Jøsok et al., 2017). Article five define and discuss cognitive agility as a potential performance measure in cyber operator practice in context of the empirical data presented in the article by discussing the association between self-regulation and cognitive agility (RQ6). Support is found for the hypothesis that higher levels of self-regulation predict cognitive agility (Jøsok et al., 2019).

The main research question of this thesis focus on the role of cognitive competencies in cyber operator practice and education and must be understood in this context. Cognitive competencies are related to the ability to adapt to, and influence, a hybrid, complex, dynamic and intangible environment defined by The Hybrid Space, in an effective way, in order to perform deliberate actions so as to achieve operational goals in and through cyberspace. The ability to do so relies on the ability to obtain situational understanding of the environment, orient and evaluate the courses of action available, exercise possible actions in conjunction with an overall plan and evaluate the outcome in order to update situational understanding and to adjust the next course of action. One specific cognitive competency that is developed and discussed throughout this thesis is cognitive agility.

1.5 Structure of the thesis

This PhD consists of five articles and this extended abstract of six chapters. The chapters of this extended abstract aim to contextualise, conceptualize and bind the totality of this project together as one. This introductory chapter places this study in the Norwegian and Military context as well as in the context of the PhD programme. It also introduces the most central concepts developed and employed for the purpose of this research project. Chapter 2 gives an overview of the current state of art in cyber operator practice and education. In chapter 3, theoretical perspectives on social cognitive theory and macrocognition are presented and the application in this thesis are briefly discussed. Chapter 4 describes the research process in three parts and lays out the methods applied, and the data collected as well as discussing methodological and ethical issues confronted during the research process. Chapter 5 presents a short summary of the results and discussions in the five articles. Chapter 6 provides the contributions of this thesis, implications and concluding remarks regarding the limitations and future research opportunities identified.

2 State of art

This state of art chapter presents a literature review that was limited to include perspectives on the cognitive work environment of cyber operators, perspectives on cyber operator practice and perspectives on cyber operator cognitive competencies. This review augments the literature reviews performed in preparations of articles one to five. How the findings inform the research questions is explained throughout the chapter.

The intent of this chapter is to present the current status of the research literature within the field cognitive competencies in cyber operator practice and education, in such a way that it helps answer the research questions. Research question one, two and three are concerned with describing the cognitive work environment of cyber operators and how cyber operators engage in dyadic and team interaction. These perspectives are partly covered by the literature reviews performed as a part of preparing articles one, two and three. In this chapter sections 2.1 and 2.2 will inform the three first research questions. Research question four and five are concerned with cyber operator performance and cognitive agility. These perspectives are partly covered by the literature review performed in preparation of article four and five. In this chapter section 2.3 will mainly inform research question four. Section 2.4 will outline how this thesis contribute to fill the research gap identified in the articles and in this state of art chapter. In this way this chapter, in conjunction with the literature reviews in the articles, inform the main research question.

In order to capture recent research developments, a literature review based on keyword search was performed in early 2019 to inform the writing of this chapter. In this literature review the keywords used were variants of cyber operator competencies and cyber operation. These variants were: ‘Cyber operator competencies’; ‘Cyber competencies’; ‘Cyber operator’; ‘Cyber operation’; ‘Cyber power’; ‘Cyber warfare’; ‘Cyber security’; ‘Cyber psychology’; ‘Cyber’; ‘Cyberspace’; ‘Digital competencies’. In the search for relevant literature the Norwegian ORIA search engine was used. This search engine includes a range of research databases, journals and online research resources. In addition, I performed the same keyword search on Google Scholar and common internet search engines, allowing the discovery of articles not indexed in digital libraries. Due to the interdisciplinary nature of the subject, journals from disciplines such as Psychology, Pedagogy, International Relations, Law and Defence were included as relevant sources. In addition, a snowballing methodology (Lecy &

Beatty, 2012) was utilized in order to locate relevant sources not returned by the keyword searches. This was performed by analyzing the references of the most relevant and frequently referenced articles returned by the keyword search. The research articles were assessed for relevance in accordance with the method outlined in chapter 4.

The state of art chapter will continue by presenting the result from the literature review in following order; First conceptualizing the cognitive work environment of cyber operators, second the recent developments in cyber operator practice and third cyber operator cognitive competencies. Finally, this thesis contribution to filling the identified gaps are outlined.

2.1 Conceptualization of the cognitive work environment of cyber operators

Reviewing the literature on cyber operator cognitive work environment and competencies reveals inconsistencies in the use of terms, definitions of those terms and challenges in conceptualizing cyberspace as an operational domain (Kuehl, 2009; Robinson et al., 2015). However, it is important to note also that conceptualization of cyberspace, both in civilian and military domains, is an ongoing discourse that continues to advance in knowledge and understanding (Kello, 2013; Libicki, 2016; Tikk-Ringas, Kerttunen, & Christopher, 2014). Consequently, this review is crossing the military and civilian boundaries as cyberspace is often referred to as a ‘global commons’ (Jabbour, 2009; Kuehl, 2009) or a ‘global socio-technical-economic system’ (Dombrowski & Demchak, 2014) not limited to military prerogatives.

In a comprehensive review of the available definitions of cyberspace, Kuehl (2009) concludes that definitions indeed help advance the conceptual understanding of cyberspace. However, he also claims the available definitions lack the power to capture the uniqueness of cyberspace. A central argument for Kuehl is that many definitions fail to recognize that cyberspace is more than computers and information (Kuehl, 2009). Kuehl offers his definition of cyberspace:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and

> interconnected networks using information-communication technologies. (Kuehl, 2009, p. 27)

To this day, elements of Kuehl's definition can be found in most attempts at defining cyberspace (Department of Defence, 2018; Joint Chiefs of Staff, 2018; NATO, Draft), making it one of the most influential contributions in conceptualizing cyberspace. In his definition, Kuehl includes the electromagnetic spectrum as a part of cyberspace, an inclusion that is still debated. Nye (2013) also includes the electromagnetic spectrum when he defines cyberspace as: *"Internet of networked computers but also intranets, cellular technologies, fiber cables, and space-based communications"* (p. 8). However, in this definition Nye fails to capture cyberspace as an operational domain. A broader definition of cyberspace that highlights the human and organizational aspects is presented by Sobiesk et al. (2015):

> A global ever evolving domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers – as well as people, organizations, and processes – which create a dimension of risks, adversaries, and opportunities. (p. 44)

In a meta discussion of defining cyberspace Robinson et al. (2015) propose four aspects of cyberspace that a definition should reflect:

- An operational space: People and organizations use cyberspace to act and create effects, either solely in cyberspace or across into other domains.
- A natural domain: Cyberspace is a natural domain, made up of electromagnetic activity and entered using electronic technology.
- Information based: People enter cyberspace to create, store, modify, exchange and exploit information.
- Interconnected networks: The existence of connections allowing electromagnetic activity to carry information.

As a result of the challenges in capturing the essence of cyberspace in one definition, several authors argue that the conceptualization of cyberspace can be best achieved through the visualization of layers of activities, due to the portrait of cyberspace as a *"…unique hybrid regime of physical and virtual properties"* (Nye, 2014, p. 3). This seems to derive from a development where cyberspace is more often viewed as an operational space and therefore the human factor receives more attention (Duggan, 2016). One example is Dawson & Thomson (2018) who describes the cyberspace as: *"A multi-disciplinary joining of computer science, economics, law, psychology, and engineering. It encompasses not only the networking of online devices together, but how humans interact and are influenced by these activities"* (p. 1). Consequently, cyberspace can be presented as consisting of layers (Dawson & Thomson, 2018; Libicki, 2016; Nye, 2010). The most updated model that exists is the one found in Joint Publication 3-12 Cyberspace Operations (Department of Defense, 2018). This model describes cyberspace as consisting of three distinct yet interrelated layers; the physical layer, the logical layer and the cyber-persona layer (See figure 2.1: Layers of cyberspace). A similar layered model is also found in the NATOs new Joint Doctrine for Cyberspace Operations, AJP 3-20, however this publication is still in a process of being ratified by the NATO nations. Both representations are clearly inspired by, Libicki's (2016) semantic, syntactic and physical layer model.

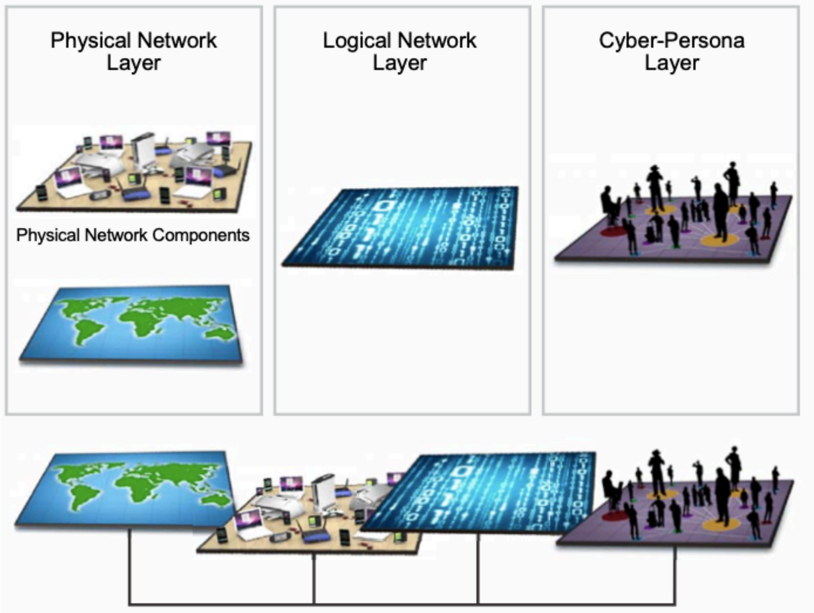


Figure 2. 1: Layers of cyberspace (Department of Defense, 2018)

This visualization in layers provides cyberspace with a physical layer, a logical layer and an information layer which are all interrelated. In addition, cyberspace enables the other domains in the operational environment by providing means of exchanging information. Finally, cyberspace is also interrelated with the cognitive domain where *"...the people who use the connectivity and the content to affect cognition and do the different things that people do with information"* (Kuehl, 2009, p. 8). In one way the conceptualization of cyberspace in layers simplifies the cyber operator work environment by limiting the conduct of cyber operations to the logical layer (NATO, Draft). In another way it complexifies the cognitive work environment by exposing the dependencies of the layers between domains and dimensions.

One way of presenting the 'fit' of cyberspace is across the domains and dimensions of the operational environment (See. Figure 2.2: Cyberspace – domains and dimensions of the operational environment). This visual representation exposes the challenge noted by most subject matter experts of cyberspace: As a part of the operational environment the *"…cyber domain overlaps with others, notably the physical (e.g., servers, lines of communication, network topology) and information (e.g., files stored on defended network(s) and servers, control of access to data as per policies) domains"* (Veksler et al., 2018, p. 1), it crosscuts the air, sea, land and space domains (Conti, Nelson, & Raymond, 2013), it is considered a part of the information environment (Department of Defense, 2018), but also has a physical and logical layer (Department of Defense, 2018; NATO, Draft), it affects the cognitive dimension (Libicki, 2016) and is an integral part of the operational environment (Kuehl, 2009).

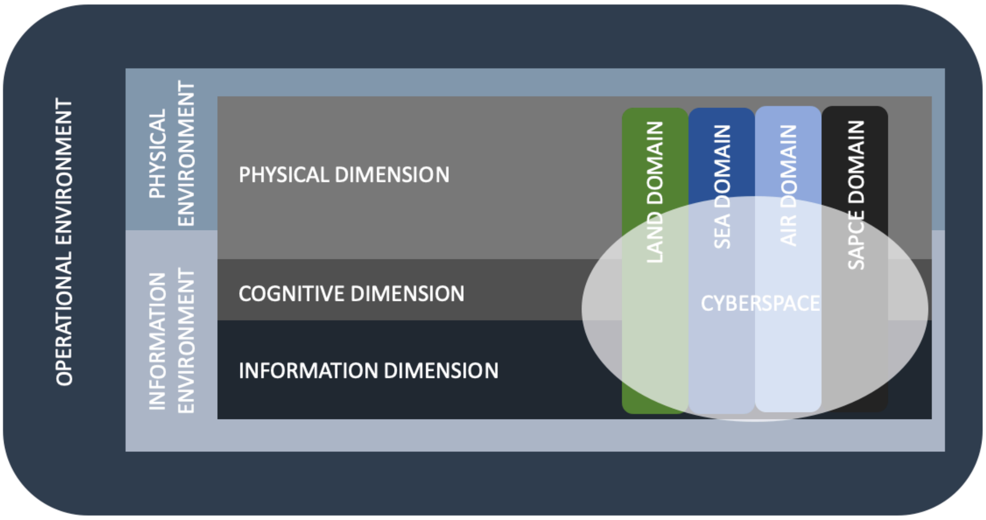


Figure 2. 2: Cyberspace – domains and dimensions of the operational environment (Kampenes, 2018).

The layers of cyberspace as well as the interrelationship of the other domains and dimensions of the operational environment, extend the cognitive space available for manoeuvre, as understanding of the complexities of cyberspace as a part of an operational environment is a huge effort. Therefore, many researchers acknowledge that the cognitive demands of the cyber operator are high due to the complexity of the operational environment and growing range of decision making possibilities for either party involved in a military conflict (Limnéll & Salonius-Pasternak, 2016).

Nye (2014) also points to the fact that cyberspace lacks a regime of governance. The existing governance structures are scattered and characterized by either separated technical issues like for example, protocols, programming and applications or broader issues such as security, human rights and development. Novel to cyberspace is that actors both within cyberspace and outside cyberspace play a vital role in cyber governance (Nye, 2014). This situation is captured in the Norwegian context by the Cyber Security Strategy:

> Digital services and products are often developed by private companies or research and development communities. A substantial part of Norway's critical digital infrastructure is owned and operated by private companies. Consequently, important decisions related to the development of – and security in – cyberspace are made by commercial, non-state actors, i.e. outside the conventional intergovernmental arenas. As a result, the role of the authorities in the development of cyberspace is limited, which in turn calls for an extensive public-private partnership. (Norwegian Ministers, 2019, p. 9)

Adding that cyberspace is argued to be subject to more rapid change than other domains (Nye, 2010) and the laws of cyberspace are only existing as non-binding guidelines in the Tallinn Manual (Schmitt, 2017) result in the cyber operator work environment being complex and disputed in many ways. Nevertheless, cyber operators have to relate to this complexity in one way or another.

As cyberspace now is widely accepted as an operational environment (NATO, 2016b) it is changing how information is created, stored, modified, exchanged and exploited. This affects and transforms operations in the other domains and the employment of instruments of power (Naím, 2013). Consequently, holding cyberpower has become a crucial goal for any sovereign nation state (Kuehl, 2009). Kuehl (2009) defines cyberpower as *"…the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power"* (p. 37). Holding cyberpower means holding the ability to enter cyberspace by means of technology and the competence to utilize that technology to achieve defined operational objectives. With that technology constantly changing, sustaining cyberpower requires an agile approach to updating also the competence to utilize that technology (Dawson & Thomson, 2018; Jabbour, 2009; United Kingdom Ministry of Defence, 2015).

Cyberspace is a young operational domain and as of now its characteristics are not fully understood, nor are the effects across the instruments of power, both offensive and defensive. This is reflected in the available literature where some elevate the cyber threat by highlighting the potential serious damage cyber conflict could inflict (Clarke & Knake, 2010; Kello, 2013). While others argue that the cyber threat is severely inflated and disconnected from reality (Lindsay, 2013; Maness & Valeriano, 2015). Most experts see cyber-attacks as a supplement effector in military operations rather than an overwhelming weapon in inter-state wars (Nye, 2010). Nevertheless, in reviewing the evidence of emergence of cyber warfare Robinson et al. (2015) conclude that cyber warfare is a topic of global concern and identify nine research challenges in cyber warfare. Conceptualizing cyber warfare and conducting cyber warfare as two of them. They also confirm the multi-disciplinary multidomain nature of cyber related issues by noting that;

> …for anyone attempting to approach the field of cyber warfare, there is a challenge in gathering an understanding of all the issues involved, how they relate to each other, what the current state of research is and where future research is required. (Robinson et al., 2015, p. 71)

This is also a prominent challenge when performing research into the area of cyber operator practice.

2.2 Cyber operator practice

The sole purpose of the cyber operator practice is to enable the conduct of cyber operations (Trent, Hoffman, Leota, Frost, & Gonzalez, 2016). Cyber operations are defined as *"... the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace"* (Department of Defense, 2018, pp. II-3) or as *"Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives"* (NATO, Draft). These definitions highlight that cyber operations can be offensive and defensive in nature and that they pertain to both military and civilian sectors. In the military sector as a part of a military campaign and in the civilian sector as defensive operations helping enterprises to keep their business running.

Lockheed Martin has analyzed the process of conducting a cyber operation and presents the 'Cyber Kill Chain' as a tool for cyber operators to perform better in defensive cyber operations (Hutchins, Cloppert, & Amin, 2011) (See figure 2.3: The Lockheed Martin Cyber Kill Chain).

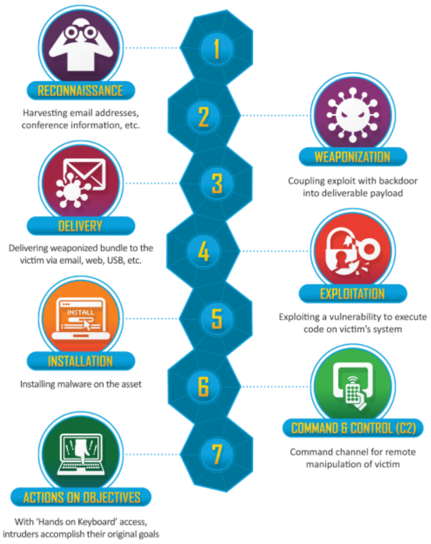

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 2. 3: The Lockheed Martin Cyber Kill Chain (Lockheed Martin, 2019)

While a cyber operator engaging in offensive cyber operations would have to conduct the activities described in Lockheed Martin's Cyber Kill Chain (Hutchins et al., 2011), cyber operators engaging in defensive cyber operations would engage in activities aimed at stopping the adversary from completing the operation. However, the Cyber Kill Chain fails to take into account cyber operations as a part of joint operations were other assets are utilized in conjunction with cyberpower to achieve the desired end state. The Cyber Kill Chain therefore fails to recognize the cyber operators' reciprocal relation to the wider socio-technical system (STS) of a military campaign as pointed out in article one (Jøsok et al., 2016). The notion of integrating cyber operations into joint operations are discussed both in military literature and research literature by a variety of authors (Gutzwiller, Fugate, Sawyer, & Hancock, 2015; Jabbour, 2009; Kott, Ludwig, & Lange, 2017; Mihai-Ştefan, 2017; Poirier & Lotspeich, 2013; Robinson et al., 2015; Siroli, 2018; Trent et al., 2016; US Army, 2010; Williams, 2014). However, conducting cyber operations as a part of joint operations presents challenges. Calling for cyber effects will most likely not find a ready response, nor guarantee an effect at all, and as Libicki points out: *"…those who call likely have less idea what the art of the possible is"* (Libicki, 2016, p. 142). Other challenges include short effectiveness of cyber weapons, conducting effective battle damage assessment and plausible deniability of effectiveness by the target (Libicki, 2016). The cyber operator engaged in defensive cyber operation is also presented with challenging tasks as he is searching for the needle in the haystack (Veksler et al., 2018). The defensive cyber operator might also be required to produce and present a recognized cyber picture[11] and to assess future developments in the cyber threat picture, based on available threat actor information and the strategic operational environment. This means that cyber operator practice involves continually cooperation with peers and communication activities with commanding officers at higher levels as outlined in article two and three of this thesis (Jøsok et al., 2017; Knox et al., 2018).

Military cyber operator practices are progressing towards understanding cyber capabilities and cyber effects (Khooshabeh & Lucas, 2018; Mancuso et al., 2014). Contemporary understanding of cyber operator practice recognizes the technical nature of cyber operations but also the goal of cyber operations to influence the operational environment by supporting the achievement of military effects. Employing offensive measures while simultaneously retaining own capability of utilizing cyberspace (frequently referred to as ensuring freedom of movement in cyberspace) by employing defensive measures, sums up the current notion of the essence of military cyber operator practice. This thesis applies an integrated view on cyber operations, meaning cyber operator practice needs to be understood, analyzed and researched as a part of a joint operation or as a part of a business operation. The consequence of such an integrated view is that the context of the operation also determines what can be considered a successful cyber operation and not, based on achievements of overall operational goals.

2.3 Cyber operator cognitive competencies

There is consensus in the research community that operating in the cyber domain requires a technical computer science proficiency as this is a necessary prerequisite to enter into the cyber domain and operate within it (Gutzwiller et al., 2015; Jabbour, 2010; Lathrop et al., 2016; Sobiesk et al., 2015). As a result, the existing research on cyber operator competencies has been predominantly focused on technical skills (Borghetti et al., 2017; Dawson &

[11] Recognized cyber picture refers to a complete depiction of the operational area, the cyber domain, aiming at providing the operational level commander with situational understanding of the military cyber domain. Nations and militaries are in the process of developing cyber pictures. No commonly available best practice is available.

Thomson, 2018). However, as outlined in article one two and five (Jøsok et al., 2019; Knox et al., 2018), a growing number of authors are advocating for a more diverse, varied and multidomain skill set as the work environment of cyber operators is better understood.

Adnan, Just, Baillie, & Kayacik (2015) proposed a work practices model for network security professionals founded upon mapping activities identified from multiple reviewed empirical studies. Through a process of merging, splitting, naming, remaining and rearranging, they identified the following ten work practices: Configuration and maintenance, threat analysis, network security assessment, incident detection (incl. monitoring, received notifications, data correlation, triage), incident analysis (incl. incident verification, artefact handling, incident assurance), incident response (incl. incident containment and forensic analysis), feedback (incl. internal feedback and external feedback), security policy development, training and awareness. Adnan et al. (2015) comprehensive review addresses the tasks of cyber operator work and confirms the prerequisite of technical skills required to perform. These technical skills are referred to as 'requisite foundational knowledge' by Goodall, Lutters, & Komlodi (2009). Goodall et al. (2009) also identify the need for the foundational knowledge to be supplemented by 'situated expertise' in the operational environment – acknowledging that to a large extent *"…it is not about the technical skills or domain knowledge, but about being familiar with the environment being defended"* (Goodall et al., 2009, p. 11). Consequently Goodall et al. (2009) argue that ability to defend from contemporary cyber-attacks involves both operational environment expertise and novel non-predefined problem-solving activities. Successful defence also depends upon the understanding of adversary skills, motivation and abilities (Krawczyk, Bartlett, Kantarcioglu, Hamlen, & Thuraisingham, 2013). An argument that is supported by Buchler et al. (2018) who contend that cyber operator tasks include both human and technical aspects and *"…is heavily reliant upon the decision-making capabilities and skill-sets of defenders to overcome attackers"* (Buchler et al., 2018, p. 3). However, none of these research contributions succeed in pinpointing specific or general cognitive competencies capable of supporting cyber operator performance.

Situational awareness[12] is one of the more general prerequisites that have been widely agreed to be essential in cyber analyst individual and team performance, but not well studied (Tadda & Salerno, 2010). Support for this claim can be found in Stevens-Adams et al. (2013) that

[12] Understanding of the environment is often addressed as obtaining cyber situational awareness through utilizing a three stage (perception, comprehension and projection) situational awareness model (Endsley, 2000).

found that operators trained in narrative-based training were able to use software tools more efficiently in terms of gaining situational awareness, as opposed to the participants that received tool-based training. Lathrop et al. (2016) also reflect these arguments when they advocate that cyber security and information technology solutions are not sufficient for cyber operations. According to Lathrop et al. (2016) cyber operations are not only focused on the malware, but include assessment of the intent, tactics, techniques and procedures of the human behind it, and that decision-making support relies on attribution and understanding of the adversary. This explains why cyber operators tasks are often described as varied, non-routine and involve perception and comprehending large amounts of information (Erbacher, Frincke, Wong, Moody, & Fink, 2012). In addition a feature of cyber operator work environment is potential lack of external feedback (Lugo et al., 2016) requiring cyber operators to take actions to gain anticipated outcomes projected into the future. Increased importance of the understand function, i.e., achieving a nuanced understanding of both the operating environment and own strengths and vulnerabilities, has also been put forward as a critical competency by several authors and official documents (Ben-Asher & Gonzalez, 2015; UK MOD, 2015). In line with Goodall et al. (2009), they address the need for this knowledge to be situated in the current operational environment, as tasks and priorities might vary in relation to operational demands.

The available research literature confirms that cyber operators are subject to high cognitive load. This is due to the information intensive character of work like network surveillance (D'Amico, Whitley, Tesone, O'Brien, & Roth, 2005), organizational factors of a network enabled operations environment (Buchler et al., 2016), and the need to perform low level analysis and high level analysis continuously (McClain, Silva, Aviña, & Forsythe, 2015). Other necessary activities such as internet searches to retrieve information to support analysis and discussions to support comprehension adds to the information load and cognitive load (Silva et al., 2014). Champion, Rajivan, Cooke, & Jariwala (2012) found that high information load could result in lack of communication between team-members impacting team effectiveness and performance, suggesting that strategies for mitigating negative effects should be a part of cyber operator training as proposed in article three in this thesis (Jøsok et al., 2017). Article three also define complex learning activities as a part of cyber operator functions. In cognitive load theory mitigation of limitations in cognitive processing, e.g. working memory, during complex learning activities can be reduced by instructional design (Kalyuga & Singh, 2016). Working memory is in cognitive load theory often conceived as a mental workspace that can be defined as; *"…a processing resource with limited capacity involved in the storage of information while simultaneously manipulating information for brief periods of time"* (Anmarkrud, Andresen, & Bråten, 2019). Therefore, the premise of cognitive load theory is a limitation in cognitive capacity that require reduction in cognitive load by controlling the environment. This is in opposition to this thesis that accepts the complexity of the environment and proposes education and training of cognitive competencies as a pathway to better performance.

A growing body of research addresses the cyber operator cognitive competencies indirectly, however little research is to be found addressing the cognitive competencies directly. Some exceptions exists, such as D'Amico et al. (2005) who have developed a three stage (Detection, Situation assessment and Threat assessment) cognitive data fusion model based on interviews with information assurance analysts working in cyber defence practice. The accompanying work flow diagram depicts the need for traversing from tactical to strategic considerations while moving through the three stages of cognitive data fusion to build situational awareness and to take appropriate action (D'Amico et al., 2005). However, understanding of the cognitive processes that supports effective cyber operator work is limited (Ben-Asher & Gonzalez, 2015; Forsythe, Silva, Stevens-Adams, & Bradshaw, 2013; Lathrop et al., 2016; Mancuso et al., 2014).

2.4 Research gaps in cyber operator practice and education

The literature review of section 2.1 reveals that conceptualizing the cognitive work environment of cyber operator practice is a prominent challenge. Reference is made to inconsistencies in the use of terms and defining the related terms proves challenging to most authors as cyberspace involves both technical and operational aspects and have unresolved legal and governance issues that further complexifies the cognitive work environment of cyber operators. Examples are found in research literature that suggest the characteristics of cyberspace are not fully understood nor are the effects across the instruments of power. In fact, conceptualization of the mentioned areas is ongoing while the practice is established and in effect. Efforts to conceptualize cyberspace through the visualisation of layers and across the dimensions and domains of the operational environment are present, but holistic frameworks describing cyber operator cognitive work environment are missing. Article one of this thesis acknowledges the complexities of cyber operator work environment that are outlined above and frames the complexities in The Hybrid Space conceptual framework (Jøsok et al., 2016). In this way the combined literature review of this thesis along with the conceptual framework informs research question one. Further article two and three acknowledge that the complexity of cyber operator work require effective communication and teamwork as is cannot be performed in isolation by one operator (Jøsok et al., 2017; Knox et al., 2018). These articles inform research question two and three by introducing the OLB-model for safe and efficient communication and including the macrocognitive perspective to help describe team interaction in cyber operations. The combined contribution is a collection of tools available for researchers to start conceptualizing cyber operator cognitive work environment.

The literature review presented in section 2.2 informs the current state of art in cyber operator practice. Cyber operators perform offensive and defensive cyber operations and cyber operations are defined as actions in or through the cyberspace intended to achieve predefined objectives. The stages of a cyber operation can be illustrated by the Cyber Kill Chain. However, the integration of cyber operations as a part of joint military operations is not in a mature state, cyberpower competence is lacking in the command chain and cyberspace situational awareness is a challenging concept. The main contribution of this thesis to advance in understanding of military cyber operator practice is strengthening the notion of cyber operations to be more than just an ICT issue performed by a technical proficient operator. The Hybrid Space conceptual framework describes the requirement for a successful cyber operator to relate to and understand the wider operational environment and be able to work in a team and communicate with both peers and superiors. In article one we find the current socio-technical system (STS) and cyber-physical system (CPS) frameworks not taking these factors into account (Jøsok et al., 2016), hence The Hybrid Space helps fill this gap by taking into account the wider STS offering a framework that can help establish clarity in the hybrid environment of cyber operator practice. The combined contribution of section 2.2 and articles one, two and three helps answer research questions one through three and lays the foundation for answering question four and five.

The literature review in section 2.3 informs the current status in research on cyber operator cognitive competencies. Cognitive competencies are defined in section 1.4.2 of this extended abstract to involve adaptation and influence of the hybrid environment defined by The Hybrid Space. Operating in and through cyberspace requires technical proficiency. This proficiency must be supported by domain expertise, situated expertise and comprehensive situational awareness including intent, tactics and procedures of the people behind. In military cyber operations, the need to obtain cross-domain situational understanding of the operational environment leads researchers to propose a range of skill sets including highly developed technical skills (e.g., coding, programming, analysis, etc.), considerable macrocognitive skills (perception, interpretation, evaluation) and effective interpersonal and psychological skills (perspective taking, communicative skills, for instance to convey mission impact information to a commander). Cognitive competencies needs are addressed indirectly by many authors. However, in-depth description and empirical underpinning of the cognitive competences mentioned in the research literature are scarce. Article four and five of this thesis helps fill this gap by proposing a specific cognitive competency; cognitive agility (Jøsok, Hedberg, Knox, Helkala, Sütterlin, et al., 2018; Jøsok et al., 2019). Further the articles utilize The Hybrid Space to develop a method and presents a software to collect data on cyber operator cognitive agility. Finally, applicability of the method and software are validated by performing an empirical study on cyber operator cognitive agility, presented in article five. The combined contribution helps answering research question four, five and six.

3 Theoretical perspectives

Two main theoretical perspectives serve as a guide throughout this thesis. The first perspective is social cognitive theory. Social cognitive theory is applied to help understanding the reciprocal relationship between the cyber operator and environment and framing the role of cognition. Focus is on one of social cognitive theory's core concepts; self-regulation. Self-regulation is chosen because of its status as a well-researched cognitive construct that is known to predict performance in complex environments (Bandura, 1997). The second perspective is macrocognition. Macrocognition is concerned with understanding cognitive adaptations to complexity and was included as a part of this thesis to help clarify the implications of researching cyber operators during a cyber defence exercise.

The intent of the present chapter is to explain the development in application of theory throughout the work with this thesis. In section 3.1 I will first present the core concepts of social cognitive theory and clarify how my reasoning when approaching the research questions is grounded in this theory. I will illustrate and explain how social cognitive theory and self-regulation is developed to help answer the research questions and explore the notion of competence in a social cognitive framework. Then I will explain how cognitive agility was developed and related to self-regulation. In section 3.2 I will introduce the macrocognitive perspective and explain how this perspective informed the work with article three and the design of the research experiment.

3.1 Social cognitive theory

According to social cognitive theory humans are neither propelled by inner forces, nor controlled by external stimuli (Bandura, 1986). Human functioning is explained as a triadic reciprocal relationship between behavior, personal factors and the environment (See figure 3.1: Triadic reciprocal determinism). The triadic relationship is not unique to this theory in particular but is also found in other theories that adopt a systems perspective of the world. For instance, Pierce's work on pragmatism (Ayer, 1968) and Mead's work on symbolic interactionism (Carter & Fuller, 2015) also adapt a resembling triadic view. Bandura claims that determinism can be analyzed in terms of this triadic reciprocity, and that this can clarify how people are influenced by, and are influencers of their environment (Bandura, 1986).

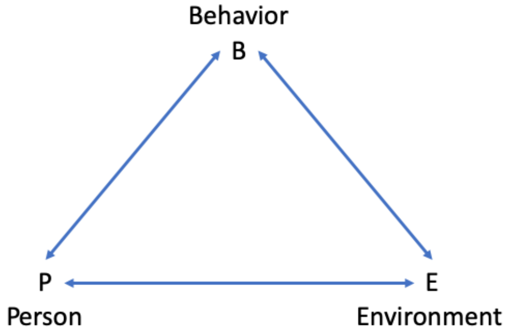


Figure 3. 1: Triadic reciprocal determinism (Bandura, 1986)

The first part[13] of this project is characterized in chapter 4 as creative and exploratory, lacking application of a rigorous overall theoretical framework. However, when starting to design an experiment and compiling the articles into one product the need for an overall framework became clear. A common denominator of the three first articles and the three first research questions is the focus on the cyber operator, the environment and cognition; a focus that is echoed in social cognitive theory. However, social cognitive theory is developed to describe human functioning in a physical environment (Bandura, 1986). Application in the cyber operator context required developing the theory to include what has been defined in the introduction of this extended abstract and in article five as a *hybrid environment* (Jøsok et al., 2019). Also, the behavior aspect of the triadic relationship had to be expanded to include the potential for cyberspace behaviors[14]. Figure 3.2 visualizes how the triadic framework of social cognitive theory was augmented by The Hybrid Space to include cyberspace behaviors and Hybrid Space characteristics.

[13] Defined in section 1.1 as: Development and exploration of The Hybrid Space conceptual framework.

[14] Cyberspace behaviors are the sum of actions within a defined timeframe, performed by the cyber operator in and through cyberspace that form patterns in the cyberspace environment.

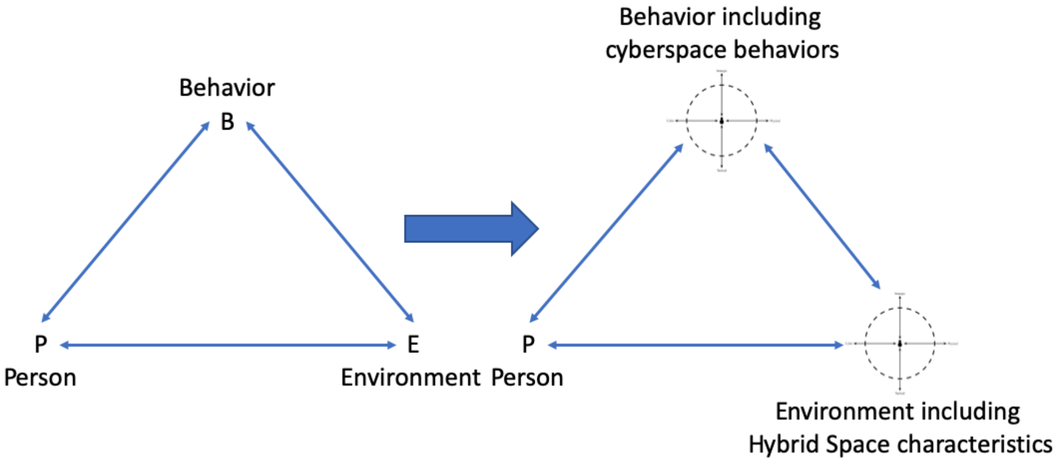


Figure 3. 2: Social cognitive theory including The Hybrid Space

When social cognitive theory was developed to include aspects from The Hybrid Space it enabled advancement in the project. In addition to providing an overall mode of thinking when approaching all research questions, social cognitive theory also provided a well-developed theory that can be used to analyze causes of human decision-making and behavior (Bandura, 1986). Further it enabled reflection on research question four as social cognitive theory allow for behavior performed in absence of immediate external rewards or punishment (Bandura, 1986), which is one of the characteristics of cyber operator practice as described in chapter 2. Also it was a promising way ahead to understand cognitive laden cyber operator work as social cognitive theory acknowledge that actions are initially shaped by thought and the subsequent cognitive constructions guide actions in the development of proficiencies (Bandura, 1997). Finally, the theory offered insight into research question six as self-regulation receives substantial attention in social cognitive theory.

3.1.1 Self-regulation

Self-regulation is defined within the scope of the social cognitive perspective in various ways. See e.g.: (Barutchu, Carter, Hester, & Levy, 2013, p. 1; Baumeister, Heatherton, & Tice, 1994; Baumeister & Vohs, 2007, p. 115; Cetin, 2015, p. 95; Moilanen, 2007, p. 835). In developing the self-regulation questionnaire employed in this thesis, the following definition is used; *"Self-regulation is the ability to develop, implement, and flexibly maintain planned behavior in order to achieve one's goals"* (Brown, Miller, & Lawendowski, 1999). From this selection of definitions, along with the discussion on self-regulation provided in article five, one can deduce that self-regulation is (at least) concerned with the individual capacity to monitor own responses (thoughts, actions, feelings) to internal and environmental cues, judge the response according to contextual demands and personal standards, inhibit dysfunctional behaviors, preserve positive goal oriented behaviors and continue to adapt flexibly to the evolving reciprocal relationship between behavior and environment. The last part emphasizing that self-regulation also has been said to be concerned with attaining goal-oriented behavior, even if the pathways are blocked or initial behaviors fail to succeed, which means that self-regulation also is a process that extends over time (Lerner et al., 2011).

Article five discuss self-regulation and proposes it as a well-researched concept that offers the possibility to be measured reliably, that is trainable and have potential to inform training of cyber operators to make better use of own self-regulatory resources (Jøsok et al., 2019). The sources of self-regulation are believed to emerge from and depend on general cognitive processes like self-observation of one´s behavior and its effects, judgmental processes of exercised behavior in relation to environmental and personal standards, and affective self-reactions (Bandura, 1986; Bandura, 1991). Little research however has paid attention to cognitive self-regulation resources over time (Barutchu et al., 2013). Nevertheless, Bandura advocate that self-regulation operates through a set of sub functions, self-observation, judgmental processes and self-reaction presented in figure 3.3: Self-regulation subfunctions (Bandura, 1986).

3.1.2 Functions and processes of self-regulation

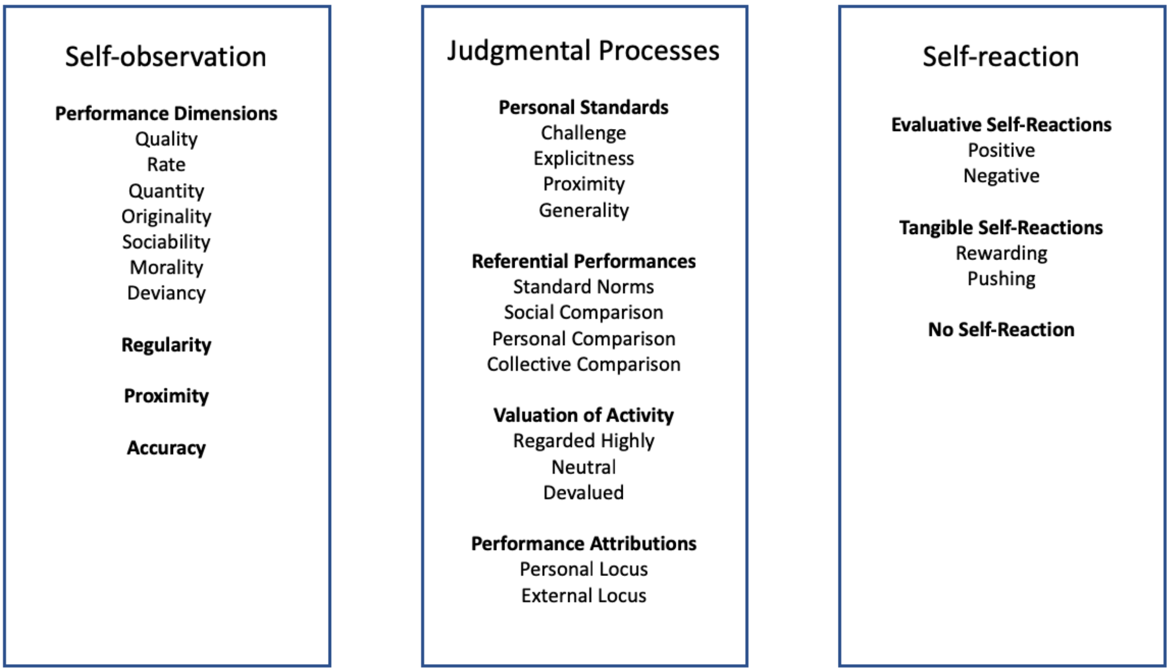


Figure 3. 3: Self-regulation subfunctions adopted from Bandura (1986)

Based on Banduras (1986) description of self-regulation functions one can deduce that any regulation of behaviors has to be grounded in observation of the need to do so (See figure 3.3: Self-regulation subfunctions). Secondly, this self-observation has to be measured up against some standards of behavior (judgmental processes). Finally, the reaction has to be interpreted in order to evaluate the effectiveness of the behavior (self-reaction). Regulation can be understood as the change one brings to behavior, in line with some standard such as an ideal, code of conduct or goal which means both to override and change affective response, or to amplify and prolong beneficial behavior (Baumeister & Vohs, 2007). Behavior in this sense does not necessarily equal physical action, but includes; *"…cognitive, behavioral, temperamental, and socioemotional components as it involves focusing and maintaining attention, initiating or inhibiting actions, thoughts, and emotions as well as monitoring the results, to achieve a particular goal"* (Jaramillo, Rendón, Muñoz, Weis, & Trommsdorff, 2017, p. 2). Baumeister et al. (1994) emphasize three resembling ingredients of self-regulation; standards, monitoring and willpower. However, Baumeister also raises the need for a fourth component, motivation, as critical presupposition to engage in self-regulatory behavior (Baumeister & Vohs, 2007). This is consistent with social cognitive theory where motivation is a fundamental part of self-regulation primarily emerging from internal standards and self-evaluative reactions to own actions (Bandura, 1986).

Performing self-regulation is a process that includes behavioral management in three phases (Zimmerman & Labuhn, 2012). According to Artuch-Garde et al. (2017) these phases are:

1) *forethought and planning phase, including aspects of task analysis and setting specific task-related goals;*
2) *performance monitoring phase, including use of strategies and resources on the task, as well continuous examination of their effectiveness and of one's progress toward the goals established;*
3) *reflection on performance phase, which is evaluation of what one has done or what can be improved, managing emotions that are triggered by the results, and then using self-reflection to begin the cycle anew.*

These processes emphasize the importance of cognition in all phases of self-regulation. First in the anticipatory phase where the recognized goals and outcome expectancies are produced by forethought; second in the process of continuous evaluation of employment of strategies and resources by cognitive monitoring, and finally evaluation of perceived causes of success and failure by performing retrospective reasoning.

The above description of self-regulation, grounded in the triadic relationship of social cognitive theory, defined and understood as a set of subfunctions and a performed as a sequential process informs research question six and provides a theoretical foundation to advance with research question four and five. Together with the discussion on the relationship between self-regulation and performance in article five (Jøsok et al., 2019), this lay the foundation for linking cognitive competencies and cyber operator performance.

3.1.3 Competence models

The traditional concept of competence in a social-cultural point of view consists of three elements: knowledge, skills and attitudes (BUK, 2010). In social cognitive theory this traditional view is described as *"…mainly a matter of developing social, cognitive and behavioral skill"* (Bandura, 1986, p. 244). Competence is also argued to be an intangible concept as it is described as an underlying characteristic that is related to effective performance in a job (Boyatzis, 1982) or other real-life settings (Hartig, Klieme, & Leutner, 2008). Social cognitive theory advocates for a proactive and mastery oriented view on competence, where both the skills and the personal self-beliefs are essential to ensure optimal use of capabilities (Bandura, 1986). In particular efficacy beliefs is held as important contributors to development of cognitive competencies and in turn cognitive competencies as important in adapting to and changing the environment (Bandura, 1997). However, Bandura (1990) summarizes that *"…there is a marked difference between possessing knowledge and skills, and being able to use them well under diverse circumstances, many of which contain ambiguous, unpredictable, stressful elements"* (p. 315).

As this PhD thesis is concerned with cyber operator practice and education, identifying and describing competencies is a core objective. Nitsch et al. (2015) identify two types of competence models that can inform identification and description of competencies: models of competence levels and models of competence structures. Models of competence levels help understand individual stages of competencies development and models of competence structure help identify the general competence structure in a certain domain (Nitsch et al., 2015).

According to Getha-Taylor, Hummert, Nalbandian, and Silvia (2013) development of competencies move through four stages. These four stages are unconscious incompetence, conscious incompetence, conscious competence, unconscious competence (See figure 3.4: Hierarchy of competence). The stages suggest that individuals are first unaware of how little they know, then they become aware and can develop new skills. They become conscious of the skill and know how to do something. Eventually they can exercise the skill with little to no conscious effort. Getha-Taylor et al. (2013) contend that the emphasis on competencies vs. knowledge, skill and attitude in contemporary society *"...reflects rapidly changing environments that require skills extending beyond the boundaries of any one job and that indicate an individual's ability to adapt and learn"* (p. 143). This observation is consistent with descriptions of cyber operator practice outlined in chapter 2. However, in order to utilize this competence level model for cyber operator education, the competencies need to be identified.

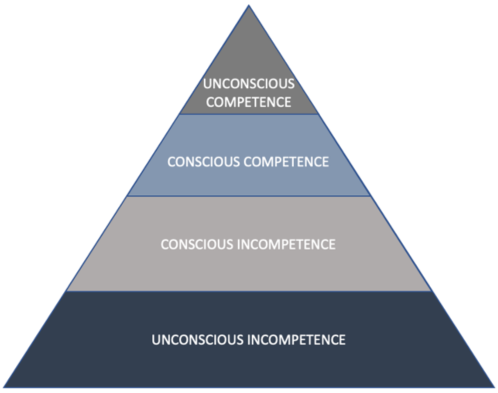


Figure 3. 4: Hierarchy of competence

Competence structure models explicitly describing the competence structures of cyber operators are hard to find, but frameworks addressing digital competence in the educational domain might guide future developments. Ferrari (2012) presents a review of 15 frameworks that address development of digital competence that potentially can inform cyber operator competencies. Ferrari (2012) report on three areas: a definition of digital competence, the identification of competence areas and a discussion of the levels. The proposed definition of digital competencies is built on different learning domains (knowledge, attitudes and skills) and spreads across several competence areas:

> Digital Competence is the set of knowledge, skills, attitudes (thus including abilities,

> strategies, values and awareness) that are required when using ICT and digital media to perform tasks; solve problems; communicate; manage information; collaborate; create and share content; and build knowledge effectively, efficiently, appropriately, critically, creatively, autonomously, flexibly, ethically, reflectively for work, leisure, participation, learning, socialising, consuming, and empowerment. (Ferrari, 2012, p. 12)

In resemblance with the presupposition of this thesis, Ferrari (2012) advocate that having technical skills at the core of a digital competence model does not give enough importance to other equally relevant aspects. He suggests that digital competence should be understood as a multi-faceted concept, and that technical operations should be considered like any other component of the framework. See Figure 3. 5: Competence construct model on digital competencies (Ferrari, 2012).

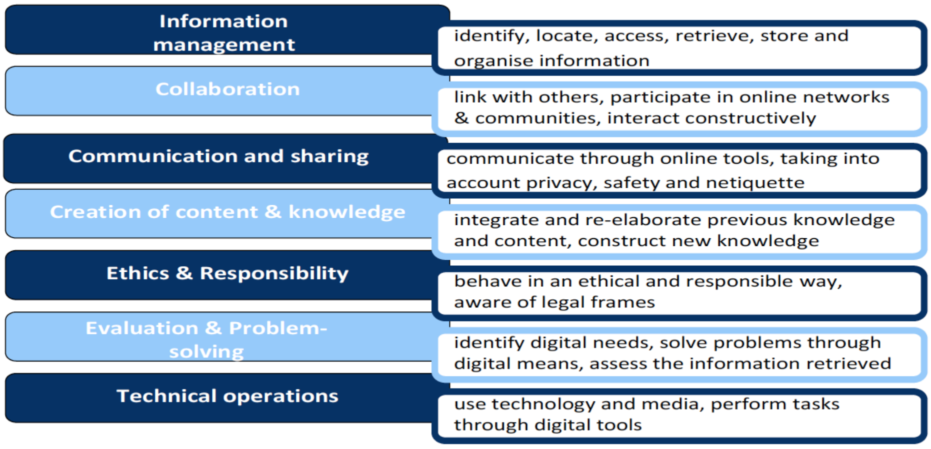

Information management
identify, locate, access, retrieve, store and organise information
Collaboration
link with others, participate in online networks & communities, interact constructively
Communication and sharing
communicate through online tools, taking into account privacy, safety and netiquette
Creation of content & knowledge
integrate and re-elaborate previous knowledge and content, construct new knowledge
Ethics & Responsibility
behave in an ethical and responsible way, aware of legal frames
Evaluation & Problem-solving
identify digital needs, solve problems through digital means, assess the information retrieved
Technical operations
use technology and media, perform tasks through digital tools

Figure 3. 5: Competence construct model on digital competencies (Ferrari, 2012)

The leap from cyber operator cognitive competencies to digital competencies can be considered a large one. However, similarities in description of competence structures are interesting to note and the possibility for digital competence models to inform cyber operator education cannot be dismissed. Competence structure models form the basis for the analysis of competence levels, as the general structure needs to be known before different levels can be identified (Nitsch et al., 2015). As outlined above and in chapter 3, the social-cognitive tradition view competencies as more than knowledge, skills and attitudes. In defining competencies, the scope of these can vary from highly specific competencies in narrow domains to broadly conceptualized key competencies (Hartig et al., 2008). Taking into account that both existing competence models of digital competence and research literature on cyber operator competencies indicate that the competence constructs facilitates cyber operator performance are multi-faceted, this thesis try to identify and assess broadly conceptualized key cognitive competencies. These key cognitive competencies can *"... facilitate the acquisition and use of specific competencies"* (Hartig et al., 2008, p. 7). In cyber operator practice and education, the need for well-founded competence assessments is evident. Research concerning theoretically as well as empirically sound models of competence structures, competence levels, and competence development is required.

3.1.4 Application of social cognitive theory in this thesis

Employing social cognitive theory as the overall theoretical framework, both in this extended abstract and in the published articles, provided a mode of thinking that enabled me to advance in answering the research questions. Social cognitive theory was amended to account for hybrid environments and potential for cyberspace behaviors. However, part two[15] of this project required attention to measuring cyber operator performance to enable answering research questions four and six. In absence of other performance measures in cyber operations self-regulation was a promising way to quantify cyber operator performance. This section will outline how linking cognitive competencies and cyber operator performance was performed by developing the cognitive agility construct.

In part two of this project, as a part of methods development, a hypothesis was formed that cyber operators able to exercise extended cognitive freedoms, i.e. being able to move effortlessly within The Hybrid Space, would show better performance. This hypothesis is inspired and grounded in Banduras social cognitive theory where he describes that given the same environmental conditions *"...people who have the capabilities for exercising many options and are adept at regulating their own behavior will have greater freedom than will those who have limited means of personal agency"* (Bandura, 1986 p. 36). The development of cognitive agility, a proposed cognitive competence associated with performance in The Hybrid Space that is presented in articles four and five (Jøsok, Hedberg, Knox, Helkala, Lugo, et al., 2018; Jøsok et al., 2019), is a direct consequence of this insight.

[15] Defined in section 1.1 as: Developing a method and a software to collect empirical data.

Cognitive agility was first defined in this research context by Knox, Lugo, Jøsok, Helkala & Sütterlin (2017) as *"…cognitive focus movements, aka. cognitive agility…"* (p. 334). In article four of this thesis, the construct was expanded and defined as *"…the ability to be attentionally flexible, where flexible expansion and contraction of cognitive focus allows for both panoramic and selected attention in The Hybrid Space"* (Jøsok, Hedberg, Knox, Helkala, Sütterlin, et al., 2018, p. 371). Cognitive agility was further developed and is in article five defined as made up of cognitive flexibility, cognitive openness and focused attention (Jøsok et al., 2019). In article five we also successfully associate self-regulation and cognitive agility. The measurement of cognitive agility is cyber operator self-reported cognitive position in The Hybrid Space over time. Operationalization of cognitive agility in The Hybrid Space is therefore x-axis and y-axis and total movement as well as quadrant change over time as explained in article four and five. Reporting a position in The Hybrid Space is reporting a focus of cognition. The articles in this thesis also propose metacognitions as important for cyber operator performance. While cognitive agility is cognitive movement in The Hybrid Space these cognitions, i.e., the process of moving over time, are supported by metacognitions embedded in the functions and processes of self-regulation as explained in this chapter.

Development of the cognitive agility construct was enabled by employing research on social cognitive theory and self-regulation as outlined in this chapter and in article five. It was a vital element in part two, and a prerequisite for completing part three[16] of this project. Defining cognitive agility as a cognitive competency and linking it to performance on cyber operators through self-regulation is essential to answering research question three, four and five.

3.2 Macrocognition

The macrocognition[17] perspective was introduced in article three to aid the study of cognitive processes in a natural cyber operator work environment, to guide the development of method in article four and to frame the design of the experiment in article five. The macrocognition perspective emerged from naturalistic decision making (NDM) studies and its primary goals of research are to understand cognitive adaptations to complexity and studying the mapping between cognitive work and real-world demands to inform theory development (Ward et al.,

[16] Defined in section 1.1 as: Collecting and analyzing quantitative data on cyber operator cognitive agility.

[17] Macrocognition is subject to a variety of definitions that resemble each other by the commonality of explaining cognition in natural environments. For definitions see for example; (Fiore et al., 2010; Hoffman & McNeese, 2009; G. Klein et al., 2003; G. Klein & Wright, 2016).

2017). This mode of thinking originates from Brunswick's work on ecological validity where he argues that design of experiments should be representative of the organisms ecology or habitat (Hammond, 1998) which also implicitly emphasize the triadic relationship between person, behavior and environment. The macrocognition perspective therefore harmonizes with the overall social cognitive theoretical framework. While social cognitive theory is utilized in this thesis to theoretically underpin cyber operator performance and to develop cognitive agility, macrocognition informs the development of method and experiment as well as provides motivation to study cyber operator cognitions during a cyber defence exercise.

The environmental conditions of interest in macrocognitive research is often associated with vague goals, organizational constraints, high stakes, and levels of experience not easily captured in controlled laboratory settings (G. Klein & Wright, 2016). In discussing the macrocognitive environment, G. Klein et al. (2003) identified a series of features that form the context in which naturalistic decision making normally takes place. These features are amongst others: ill-defined goals and ill-structured tasks, uncertainty, ambiguity, missing data, shifting and competing goals, dynamic and continually changing conditions, action-feedback loops (real-time reactions to changed conditions), time stress, high stakes, multiple players, organizational goals and norms, and experienced decision makers (G. Klein & Klinger, 1991). This list of features resembles very much the prerequisites for The Hybrid Space conceptual framework described in article one (Jøsok et al., 2016). Therefore, in article three the macrocognitive perspective is juxtaposed with The Hybrid Space to explore how the two can augment each other with focus on cyber operator teamwork and cognitive adaptation to cyber operator work environment. Article three disclose that in available research literature, there is a common acknowledgement of the contested environment in which cyber operations are performed (Jøsok et al., 2017). Especially high stakes, ill-defined goals and tasks, information load, uncertainty and dynamic conditions are common features (see e.g. (M. A. Champion et al., 2012; Forsythe et al., 2013; Knott et al., 2013; Lathrop et al., 2016; Mancuso et al., 2014)).

3.2.1 Functions and processes of macrocognition

G. Klein (2007) argues that complex settings require a more adaptive philosophy that breaks with the fixed goal and fixed roles and tasks paradigm. Klein calls for a flexible execution that appreciates the process of setting goals, learning and discovery through planning and eventually redefining goals based on new insight into newly discovered, earlier invisible, relationships and dependencies (G. Klein, 2007). To attain these goals the macrocognition perspective provides a range of supporting functions and processes presented in figure 3. 5: Macrocognition - Functions and processes.

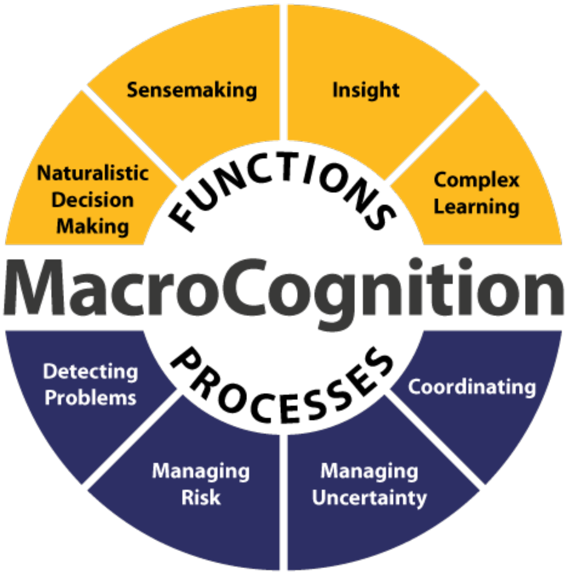


Figure 3. 6: Macrocognition - Functions and processes (Macrocognition, 2016)

The distinction between functions and processes is both for pragmatic and theoretical purposes (G. Klein et al., 2003). While the functions of macrocognition is referring to what experts do in complex environments, the processes are supporting the functions, making them more effective. This mindset of macrocognition makes it more a perspective than a theory or framework. Critique of NDM and macrocognition have been raised because of less concern for testing hypothesizes, normative and/rational models and precision. The macrocognitive perspective is more focused on plausibility, descriptive models and formulating useful models. Holding the macrocognition perspective up against the descriptions of cyber operator cognitive work environment provided in the state of art chapter reveals that cyber operators indeed engage in the functions and processes shown in figure 3.6 Macrocognition - Functions and processes; e.g. Adnan et al. (2015) description of work practices are examples of practices that require cyber operators to engage in macrocognitive functions and processes. Gaining situational awareness and situate the work practices in the current context can also be argued to require cyber operators to engage in macrocognitive functions and processes as these are defined within the macrocognition perspective.

3.2.2 Application of macrocognition in this thesis

An effect of a more digitized society is changes in the nature of work activities towards more cognitively oriented work (Bandura, 1997; Ward et al., 2017). Employing the macrocognitive perspective in this thesis to explore cyber operator cognitive competencies, helps mapping and understanding the relation between a complex environment and the corresponding cognitive demands. The macrocognitive perspective is focused on environments that are highly interactive and comprised of multiple agents and artefacts. This description is consistent with the characteristics of The Hybrid Space as described in articles one to three in this thesis. Macrocognition acknowledges these features of cognitive work systems and the fact that it presents significant challenges to scientific methodology and theory, and to subsequent design of reliable work methods and the technologies that shape them (Ward et al., 2017). In part three of this project the annual CDX at the NDCA served as the research arena. The macrocognition perspective motivated to utilize this arena because of its embracement of environmental complexity in research and critique of controlled laboratory research experiments. The macrocognitive perspective serves a purpose to connect some of the challenges in cyber operator practice exposed by The Hybrid Space and connect those to cognitive competencies. In this sense, the macrocognitive perspective contributes to this thesis by adding perspectives on methodology that supported the development of the cognitive agility construct and allowed for performing an experience without rigorous control of the environmental conditions. The field of macrocognition is also argued to be well suited for addressing cognitive training requirements (G. Klein & Wright, 2016). Therefore, it can inform the connection between experienced subject matter experts and the education and training of novices and practitioners.

3.3 Summary of theoretical perspectives

In this chapter I have outlined how social cognitive theory and macrocognition have been employed to pursue the research questions in this PhD project through its three parts.
Social cognitive theory provided the overall theoretical framework that facilitated exploration of The Hybrid Space, enabled investigating how and in what ways and to what extent cyber operators' performance is supported by cognitive competencies and to develop the cognitive agility construct. The macrocognitive perspective motivated to undertake an experimental research approach, this applied and non-limiting view on the environment and provides grounds for understanding how cognition adapts to complex hybrid environments. In concert

with the theory employed in the articles of this thesis, these perspectives facilitate better understanding of the cognitive demands of cyber operator practice as well as providing inspiration to how cognitive competencies these can be researched.

4 Data and methodology

The work with this thesis disclosed that the research field of cyber operator practice and education lacks a coherent set of methods, principles, rules and regulations. Also, as outlined in this extended abstract, the core concepts of cyberspace and cyber operator practice are either disputed or in a process of being formed. Therefore, investigating the role of cognitive competencies in cyber operator practice and education required a substantial amount of literature review and concept development in order to comprehend problems associated with the main research question. Further, to be able to perform empirical data collection on cyber operator cognitive competencies, both method and metrics had to be developed. In this chapter I make the methodological and ethical challenges visible by scrutinizing my methodological foundation and exposing the ethical challenges I have confronted in this project.

The introduction to this thesis outlines how the research questions have guided the research progress through three parts. In this chapter I will first explain the methodological challenges and solutions relating to each part in sections 4.1, 4.2 and 4.3, before giving consideration to methodological considerations relating to literature reviews in section 4.4, validity and reliability of the research in section 4.5, ethical considerations and my role as a researcher in sections 4.6 and 4.7. Finally, I will sum up the chapter and offer some reflections on the methodological strengths and limitations of this study in section 4.8.

4.1 Part 1: Development and exploration of The Hybrid Space conceptual framework

The first part of this project can be characterized as a creative and exploratory phase of research, where a combination of methods were employed. The question of how to educate the next generation of cyber officers; triggered a journey were I in power of being an instructor at the NDCA engaged in conversations with students and subject matter experts, observed practice and explored literature on the matter. This process resulted in the development of The Hybrid Space conceptual framework. The methodological weakness of this early stage of research is lack of a stringent methodological approach. However, whether such early stages in novel research can actually be methodologically sound is questioned. As Knutsen (2016) points to in his critique of the hypothetic deductive method; the hypothesis has to come from somewhere, and this ‘place’ is best characterized by a fluid process over time. In this respect, the development of The Hybrid Space framework can better be characterized as an inductive approach where coincident and formal research methods worked together in the first stages of hypothesis and conceptual development. The main effort of this initial part can be described as utilizing the scientific *"…way of thinking that leads us towards testable explanations of what we observe in the world around us"* (Coolican, 2014, p. 6). What we observed in the world around us was captured in The Hybrid Space conceptual framework. The next step was to scientifically underpin and disseminate it.

The first literature review was performed by keyword search for the word "cyber" and the results were manually screened for relevance in accordance with the description in section 4.4. Further, the search was expanded to include 'socio-technical systems' and 'cyber physical systems' as these seemed promising areas of research to inform the scientific underpinning of The Hybrid Space. Internet search engines, open access online journals and Google Scholar were used in this initial stage to search for relevant literature. Challenges identified were first a lack of scientific literature addressing cyber operator practice with focus on psychological factors and second the results returned originated from many different scientific areas. Literature assessed as capable of underpinning The Hybrid Space mainly originated from military journals, governmental and military concept papers and human factors research including psychology journals with a substantial amount stemming from conferences proceedings. This sparked the idea of disseminating The Hybrid Space at a conference instead of in a journal as the thematic of cyber operator competencies clearly were more discussed in such venues as well as offering the opportunity to get instant feedback on The Hybrid Space framework. Two conferences were considered; Human-Computer Interaction and Applied Human Factors and Ergonomics. The Human Computer Interaction Conference was chosen as its focus is in the intersection of computer science and behavioral sciences.

The two following articles, two and three, aimed at populating The Hybrid Space employed a more stringent methodology. Both articles utilize the method of literature review combined with discussion and observations done in the educational context of the NDCA. In these articles the official online databases available at Inland Norway University of Applied Sciences and Google Scholar were used to find relevant literature.

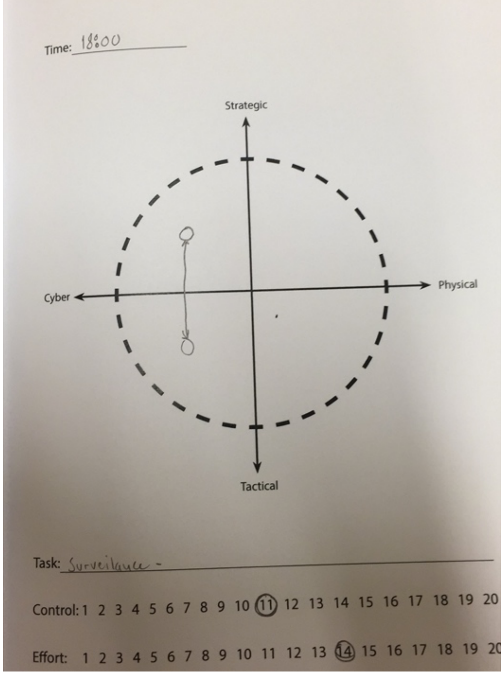
Article two utilizes cognitive engineering methodology to design the OLB-model. Cognitive engineering is a method using cognitive psychology to develop models that can support cognitive processes (Lee, Kirlik, & Dainoff, 2013). Development of the OLB-model was inspired by Morrow and Fischer (2013) description of the role of communication in socio-technical systems. The literature review performed in preparation of article one informed the initial stages of developing the model. A new literature review was performed to include aspects of cyber operator communication in teams and with superiors in the military hierarchy. Keywords included 'team communication', 'safety-critical communication' and 'communication in sociotechnical systems'. Results were manually screened, and a snowballing methodology was applied to identify additional relevant literature. A snowballing technique was chosen as it is capable of producing a network of relevant articles and *"…facilitates insights into the broad context of the research instead of the narrow set of publications that are returned in keyword searches"* (Lecy & Beatty, 2012, p. 5). Article three includes a review of the current state of art of the macrocognitive perspective. Keywords included in preparation of this article was simply; "macrocogniton". Then literature with relevance for hybrid environments and cyber operator practice were selected to inform the article. In addition, relevant literature identified in preparation of article one and two were also used to contextualize macrocognition in the military cyber operator context. While article three was found suitable for the Human Computer Interaction conference, two journals were considered for article two. These were Journal of Military Studies and Military Psychology. Military Psychology was assessed as most appropriate as its aims to include research on psychological principles within a military environment.

A methodological challenge in these first articles is the sheer number of terms used in scientific communities to explain cyberspace and cyber operator practice related questions. Performing the search in such a way that it produced relevant hits proved a monumental challenge. Authors might refer to cyberspace as the digital, cyber, internet, online, social media, electronic communication or other terminologies associated with cyberspace, making the selection of literature time consuming and less accurate. Therefore, employing a snowballing methodology became necessary to gain insight into the research area of interest as the result from the keyword searches were assessed to be fragmentary. The lesson learned is that cyberspace is still young and undeveloped conceptually, resulting in methodological weaknesses in any form of literature review in the area of cyberspace and consequently cyber operator practice and education.

4.2 Part 2: Developing a method and a software to collect empirical data

The first part of this project introduced the notion of cognitive agility as a potential performance measure in cyber operator practice. Part two, disseminated in article four, describes the process of developing method and metrics to enable the conduct of the experiment. This was achieved by designing a software, The Hybrid Space app, tailored to collect data on cyber operator cognitive focus and operationalizing The Hybrid Space framework to enable assessment of cyber operator cognitive agility. This work enabled answering research question four and five.

In the process of building The Hybrid Space app, first a literature search was performed to disclose alternative ways in which cognitive data could be collected. No specific keywords were used, but an exploratory approach identifying the available methods for measuring cognitive focus in cyber operator was applied. Also the book; Research Methods for Cyber Security (Edgar & Manz, 2017) was used to gain an overview of methods to assess. As discussed in article four, no available methods that could inform the capturing of cognitive focus in context of The Hybrid Space were identified. Consequently, metrics and methods had to be developed. The 2016 CDX was utilized to explore ways of capturing data on cognitive focus in The Hybrid Space with a paper and pencil procedure (See figure 4.1: Data collected during the 2016 CDX).


Time: 18:00

Strategic
Cyber
Physical
Tactical

Task: Surveilance -

Control: 1 2 3 4 5 6 7 8 9 10 [✓ 11] 12 13 14 15 16 17 18 19 20

Effort: 1 2 3 4 5 6 7 8 9 10 11 12 13 [✓ 14] 15 16 17 18 19 20

Figure 4. 1: Data collected during the 2016 CDX

Figure 4.1 shows an example of data collection on cyber operator cognitive focus during the 2016 CDX. This operator is reporting at 1800 hours that he is engaged in surveillance and that he is traversing between tactical and strategic considerations in the cyber sphere of The Hybrid Space. A cyber operator reporting the task surveillance means that he, as a part of his team, is responsible for monitoring the network by using a software named 'kibana'. The software can be adjusted and tuned by the operator to capture abnormalities in the network that could indicate efforts to gain unauthorized access to the network (aka cyber-attack). The CDX is designed so that the network activities performed by the attacker team is aligned with an overall strategic and operational context framed by written and oral scenario injects. This might explain why this cyber operator is traversing on the y-axis; to make sense of the activity in the network with the evolving strategic context. The operator also has indicated the level of control and effort on a scale from 1 to 20. These data were not analyzed as a part of this PhD to narrow the scope of this project. Note that the possibility to indicate multiple locations is not supported by The Hybrid Space app where only one location can be indicated at a time. Based on what was learned from this exercise we developed The Hybrid Space app. A spiral lifecycle methodology[18] was used to design and develop the software and to address the security aspects of using an online software to collect data. The motivation for developing this software was to make data collection more efficient and to automatize data handling. This was a direct outcome of lessons learned from data collection during the 2016 CDX[19].

The Hybrid Space app participant window is shown in figure 4.2. This interface enables the participant to log in using a unique identification number and password. Research participants use the participant window to mark their cognitive focus and indicate their perceived level of control by sliding the sliders right or left before submitting their data. In the comment field they indicate the task they are currently engaged in.

[18] A spiral lifecycle methodology is characterized by repeated iteration of four software development phases. These are; determine objectives; evaluate alternatives; develop software and evaluate/plan next phase.

[19] The data from the 2016 CDX is not included as a part of this thesis but was an important steppingstone to gain experience with gathering and analysing data utilizing The Hybrid Space conceptual framework.

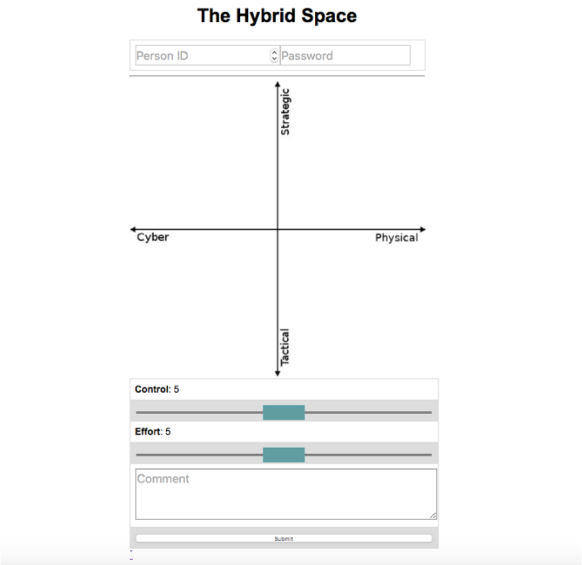
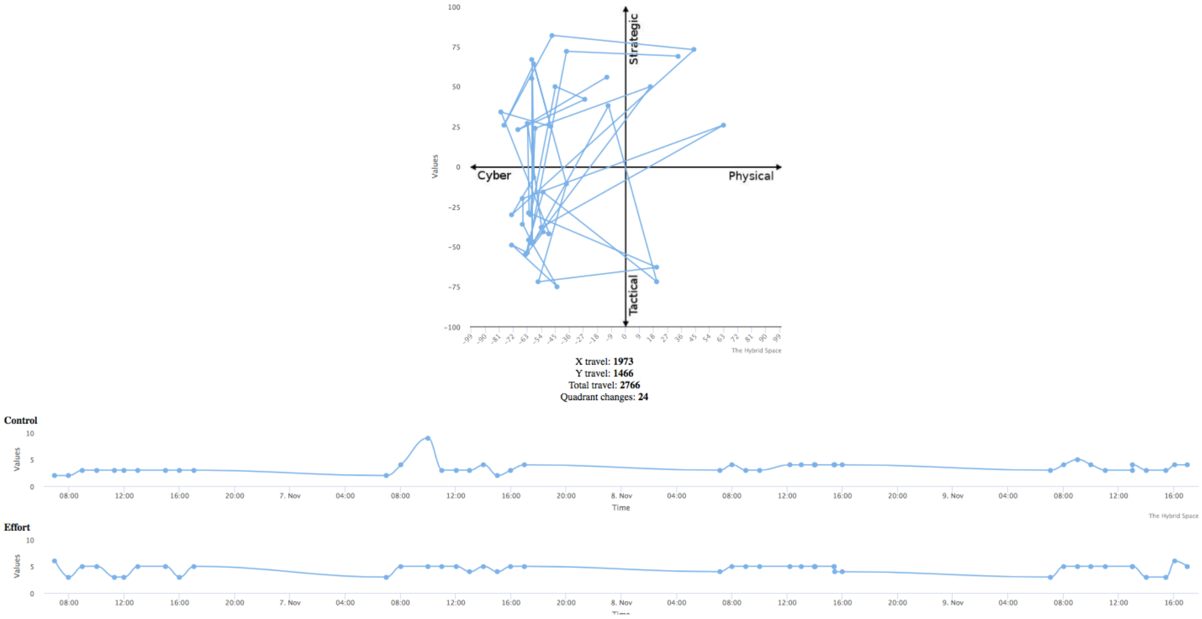


Figure 4. 2: The Hybrid Space App participant window.

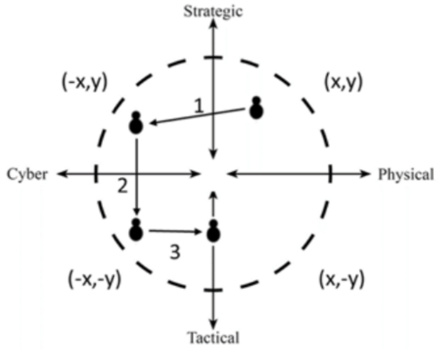
The researcher view with examples of data collected is shown in figure 4.3. The software also includes a visual representation of the data collected that is useful for interpreting data and presents the opportunity for visual analysis. Note that also the cognitive movements over time is automatically computed and indicated as; x travel, y travel, total travel and quadrant change. These are referred to in article five and this extended abstract as cognitive agility indicators or metrics. Datasets can also be exported to comma-separated values (CSV) or excel format to enable further statistical analysis.



X travel: **1973**
Y travel: **1466**
Total travel: **2766**
Quadrant changes: **24**

Figure 4. 3: Example data collected by the Hybrid Space App.

Article four also includes the operationalization of cognitive movements (see figure 4.4) in The Hybrid Space that are used to measure cyber operator cognitive agility in article five.



Movement in the Hybrid Space: (1) operator reporting quadrant change (x,y) to (-x,y); (2) operator moving along the y-axis; (3) an operator reporting movement to an axis but not crossing to other quadrant

Figure 4. 4: Operationalization of The Hybrid Space movements.

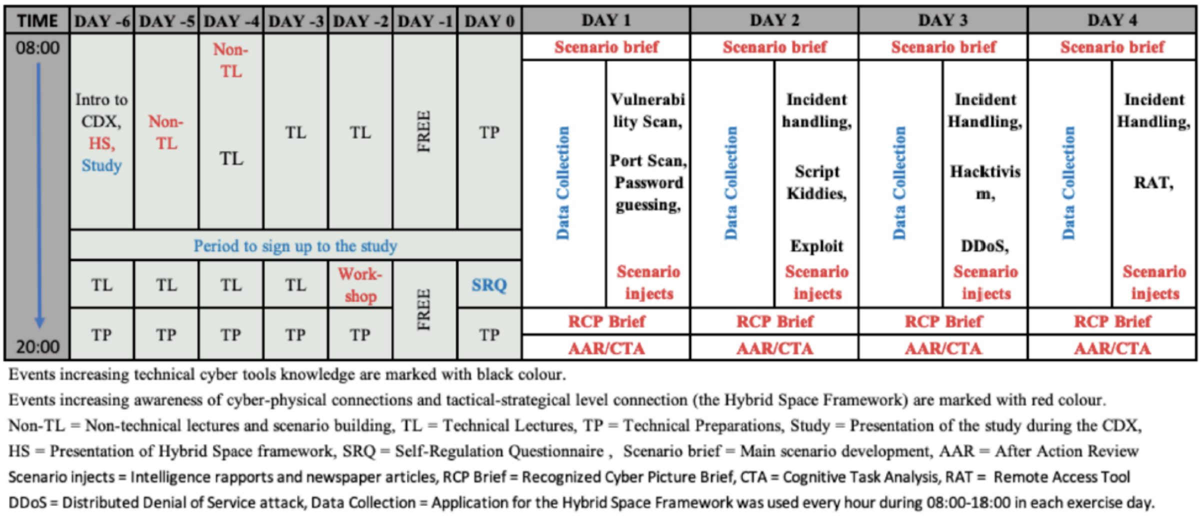
The Hybrid Space app is the result of a methodological challenge, and a methodological challenge in itself. The strengths of digitizing data collection are that it provides a more versatile data collection and presents swift and flexible opportunities for visualization and analysis of data. The methodological issues of self-reporting cognitive data are common to answering questionnaires on self-regulation employed in this research and will be discussed as a part of addressing validity and reliability of data in section 4.5. The article was found suitable for dissemination in the Human Computer Interaction conference.

4.3 Part 3: Collecting and analyzing quantitative data on cyber operator cognitive agility and self-regulation.

Part three of this project builds on the literature reviews from part one and two as well as the developed method and software presented in article four and section 4.2. However, in preparation of article five a literature review was performed by keyword search covering aspects of “cyber operator tasks” “cyber operator performance” and “cognitive agility”. The results were manually screened for relevance in accordance with the description in section 4.4. The results informed the writing of article five.

Based on the assessed strengths of the macrocognitive perspective as outlined in chapter 3, the research arena decided was the annual CDX at the NDCA. During this exercise the cyber cadets work in teams to defend a network from cyber-attacks. This was the first stage in the research process where I formally interacted with students to recruit research participants. The aim of the project was presented to the whole cohort the first week of the exercise (See article five or figure 4.5 for an overview of the experiment components and timetable of the quantitative data collection). In this session The Hybrid Space framework was presented. This was a necessity because of the need to apply the framework as a part of the research. However, when presenting the framework there is a risk of instilling thought processes in the participants minds that earlier did not exist. A common concern, especially for qualitative research, is not to impose the researchers views on the participants in the study (Punch, 2002). The risk of producing a Hawthorne effect[20] in such respect is evident. To mitigate the chance of such an effect, the participants were encouraged to register their location as correctly as possible without adjusting the answer to what they think is correct or preferred by the researcher. After the presentation they were given the information in written form and a consent form, they then had six days to evaluate if they wanted to participate. The 23 cyber cadets who chose to participate signed and handed in the consent form. The participants first answered (Day 0 as indicated in figure 4.5) an online questionnaire consisting of the Self-Regulation Questionnaire (SRQ), used to evaluate self-regulatory ability through self-report (Brown et al., 1999). They then indicated their cognitive focus in The Hybrid Space in The Hybrid Space app every full hour during the four days of the CDX (Day 1-4 as indicated in figure 4.5). The participants used their own computers to access The Hybrid Space app making the research less resource intensive. The experimental set up is shown in figure 4.5 and in article five (Jøsok et al., 2019).

[20] Hawthorne effect is often referred to as the observer effect. In research contexts involving observation this is a delicate matter, as observation in itself leads individuals to modify aspects of their behavior as a response to being observed. In the context this PhD, introducing The Hybrid Space framework and asking cadets to mark their position will trigger thought processes on their position and most likely influence the way they mark their location.



TIME	DAY -6	DAY -5	DAY -4	DAY -3	DAY -2	DAY -1	DAY 0	DAY 1	DAY 2	DAY 3	DAY 4
08:00	Intro to CDX, HS, Study	Non-TL	Non-TL TL	TL	TL	FREE	TP	Scenario brief Data Collection Vulnerability Scan, Port Scan, Password guessing, Scenario injects	Scenario brief Data Collection Incident handling, Script Kiddies, Exploit Scenario injects	Scenario brief Data Collection Incident Handling, Hacktivism, DDoS, Scenario injects	Scenario brief Data Collection Incident Handling, RAT, Scenario injects
	Period to sign up to the study										
	TL	TL	TL	TL	Work-shop	FREE	SRQ				
20:00	TP	TP	TP	TP	TP		TP	RCP Brief	RCP Brief	RCP Brief	RCP Brief
								AAR/CTA	AAR/CTA	AAR/CTA	AAR/CTA

Events increasing technical cyber tools knowledge are marked with black colour.
Events increasing awareness of cyber-physical connections and tactical-strategical level connection (the Hybrid Space Framework) are marked with red colour.
Non-TL = Non-technical lectures and scenario building, TL = Technical Lectures, TP = Technical Preparations, Study = Presentation of the study during the CDX,
HS = Presentation of Hybrid Space framework, SRQ = Self-Regulation Questionnaire , Scenario brief = Main scenario development, AAR = After Action Review
Scenario injects = Intelligence rapports and newspaper articles, RCP Brief = Recognized Cyber Picture Brief, CTA = Cognitive Task Analysis, RAT = Remote Access Tool
DDoS = Distributed Denial of Service attack, Data Collection = Application for the Hybrid Space Framework was used every hour during 08:00-18:00 in each exercise day.

Figure 4. 5: Experimental setup.

To ensure the anonymity of the participants, they were given a unique identification number for both the online questionnaires and The Hybrid Space app. After the completion of both, the data was imported into SPSS for further statistical analysis. Correlations and regression analysis were performed with self-regulation as the independent variable and cognitive movements entered as dependent variables. The alpha levels for testing the hypothesis was set at the 0.05 level. Due to a small sample size a restrictive wording in accordance with Mukaka (2012) were used in article five to explain the correlations. The relationship between movement in The Hybrid Space and self-regulation was investigated using Pearson product-moment correlation coefficient. Linear regression was used to assess the ability of self-regulation to predict cognitive movement in The Hybrid Space. Cognitive agility indicators were set at as dependent variables, and self-regulation total scores were set as independent variable. Finally, scatterplots were generated to visualize the results. Details on statistical analysis and further description of method can be found in article five (Jøsok et al., 2019).

In preparation of article five, four journals were considered for publication. These were Journal of Military Studies, Military Psychology, Nordic Journal of Digital Literacies and Frontiers in Psychology. Frontiers in Psychology was chosen because it is ranked as a level 2 journal by the Norwegian Centre for Research Data and at the time had a special research topic titled: ‘Mastering Cyberpower: Cognitive Sciences and The Human Factor in Civilian and Military Cyber Security.’

4.4 Literature review

The literature reviews of this thesis were based on keyword search assisted by a snowballing methodology. Both the reviews performed in preparation of the articles as well as this extended abstract followed the methodology described in this section. However, the keywords varied slightly in the different articles as these have different focus areas, and has been accounted for in methodology description of respectively part one, two and three in this chapter. In all cases the returned results were manually screened for relevance. In relevant literature the references were inspected to allow for further identification of informative sources in accordance with the snowballing methodology described by Lecy and Beatty (2012). In both cases, only the most relevant articles were included based on the following criteria:

- The source directly addresses at least one specific aspect of cyber operator competence or aspects of cyber operator work environment able to inform the answering of one or several of the research questions.
- The source is not directly related to the cyber operator work environment or competencies but provides information about cyberspace related human practice and education (both military and civilian).

Further, the sources were analysed based on their origin and publication channel. Sources from publication channels ranked at level 1 and 2 by the Norwegian Centre for Research Data were included. Sources from other publication channels were manually judged by their origin and relevance. Sources from a well-respected organization or author were ranked higher than one from a lesser known entity. Particularly sources from non-ranked military journals, official governmental reports and reports from international non-governmental institutes were given high ranking. Sources that were perceived as highly relevant to the topic were included above the lesser relevant sources. Finally, sources more recently published were given a higher ranking than older ones.

Application of the keyword search methodology does not guarantee that multiple researchers will collect the same bodies of articles. Especially in an interdisciplinary research effort such as cyber operator education and practice (Caulkins et al., 2016; Newhouse et al., 2017) were there is a limit to the amount of perspectives to include. Relevant literature to inform the research questions of this study was identified in a variety of scientific disciplines. I found this to be challenging traditional frameworks of how to perform a rigorous literature review.

I.e. performing a keyword search within a defined scientific discipline to uncover the current state of art within that area. This challenge is captured by Leech, Dellinger, Brannagan, and Tanaka (2010) that discuss the challenge of researchers limiting their works by placing it in a qualitative or quantitative framework to avoid mixing paradigms and methodologies. They propose that pragmatic approaches collaborating and mixing epistemological views can be viewed as a strength and produce quality research, however few validation frameworks are available to assist evaluating such research efforts (Leech et al., 2010). In accordance with their proposed validation framework, the literature reviews performed as a part of this project can be evaluated as a part of their foundational element. Then the questions to be answered is if the literature is appropriate of the purpose of the study, if the literature inform the purpose, design, measurement, analysis and inferences, and if the quality of the review is satisfactory (See Leech et al. (2010) for a complete list of questions).

Since 2015, when the work on this thesis started, several new journals have been established as a response to the interdisciplinary nature of cyber security. One example is the Journal of Cybersecurity that is *"...premised on the belief that computer science-based approaches, while necessary, are not sufficient to tackle cybersecurity challenges. Instead, scholarly contributions from a range of disciplines are needed to understand the varied aspects of cybersecurity"* (Journal of Cybersecurity, 2020). Therefore, there is reason to believe that future research would have more interdisciplinary resources available than this study had. These interdisciplinary resources are a promising way forward as they will contribute to ease the search for literature within the area of cyber operator practice. Future literature research into cognitive competencies in cyber operator education and practice should include databases that represent both military and civilian domains as well as both educational and psychological domains. Highly relevant interdisciplinary journals in the area, such as the Journal of Cybersecurity, should be identified, included and manually searched for relevant articles. To limit the number of returns and to raise relevance of content, I would also recommend restricting searches to articles published after approximately the year of 2010 because of the rapid development of cyberspace and its application in a digitized society. Lastly, future research should also apply a coding scheme that is capable of extracting the relevant data or content to the topic of interest. These actions would ensure what (Boote & Beile, 2005) describe as a *"...more substantive, thorough, sophisticated literature review"* (p. 3) capable of underpinning a substantive, thorough, sophisticated research.

4.5 Validity and reliability

Disseminating scientific research includes giving consideration to the rigor of the research to expose the measures taken by the researcher to ensure the quality of the study (Heale & Twycross, 2015). This section will address the question of validity and reliability of the three parts of the study. First, I will outline validity and reliability in general before discussing each part successively. In part one the validity of The Hybrid Space will be discussed. In part two the validity and reliability of the Hybrid Space app and the cognitive agility construct will be discussed. In part three the validity and reliability regarding the conduct of the experiment, analysis of data and findings will be discussed.

4.5.1 Validity and reliability in general

Validity is associated with a well-grounded research method employing means capable of accurately measuring what they are intended to measure (Golafshani, 2003; Silverman, 2014). Reliability is associated with the ability to replicate the results in the same situation on repeated occasions under similar methodology, e.g. the repeatability of the study (Heale & Twycross, 2015). Validity determines truthfulness of the research results and can be divided in two types; experiment and test validity (Heffner, 2018). Experiment validity can further be divided into two main categories, internal and external. Internal validity refers to the extent the results of the study can be explained by the casual relationship between the independent and depended variables. External validity refers to the extent the findings can be generalized (Heffner, 2018). Further, assessing validity of a specific test can according to Cronbach and Meehl (1955) be divided into two categories; content validity and criterion validity. Content validity corresponding to if the inventory or concept are capable of measuring what it aims to measure and if it is grounded in theoretical concepts. Criterion validity corresponding to the inventory or concepts are related to an existing measure and if it can predict performance or another criterion (Cronbach & Meehl, 1955). Reliability determines the consistency of results and consist of two main categories; internal and external. Internal is concerned of to which extent a measure is consistent within itself, and external to which a measure varies form one use to another (Heffner, 2018). An overview of validity and reliability constructs as it is applied in this study is provided in figure 4.6.

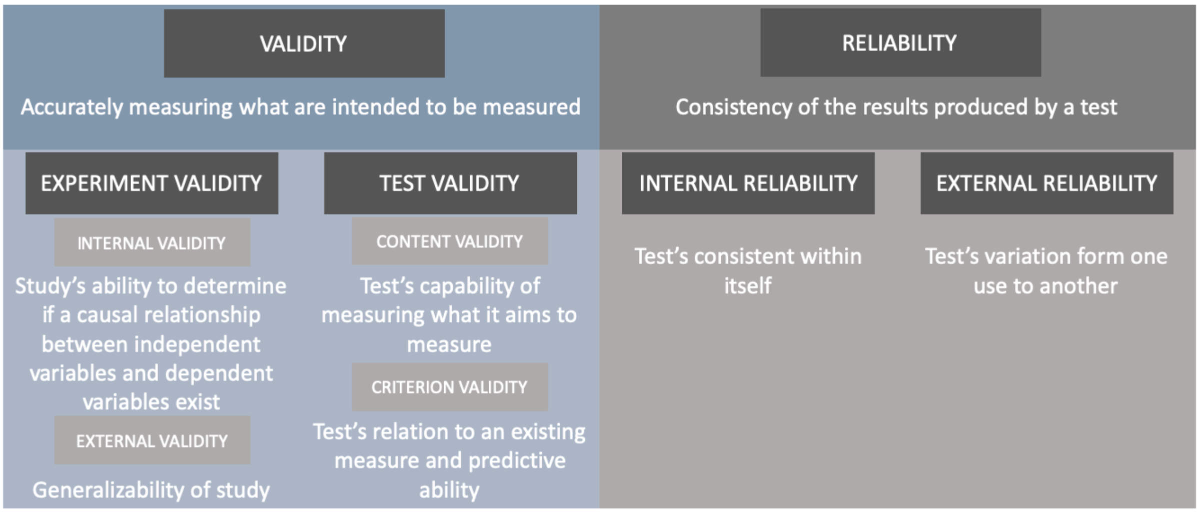

VALIDITY
Accurately measuring what are intended to be measured
RELIABILITY
Consistency of the results produced by a test
EXPERIMENT VALIDITY
TEST VALIDITY
INTERNAL RELIABILITY
EXTERNAL RELIABILITY
INTERNAL VALIDITY
Study's ability to determine if a causal relationship between independent variables and dependent variables exist
EXTERNAL VALIDITY
Generalizability of study
CONTENT VALIDITY
Test's capability of measuring what it aims to measure
CRITERION VALIDITY
Test's relation to an existing measure and predictive ability
Test's consistent within itself
Test's variation form one use to another

Figure 4. 6: Overview of validity and reliability constructs

4.5.2 Part 1

The Hybrid Space is not a test or measure in itself. However, it is proposed to represent the reality of the cyber operator cognitive work environment in article one (Jøsok et al., 2016). The question then becomes to what extent The Hybrid Space actually is capable of representing reality, and how it further contributes to or reduces the validity of the research. Therefore, the validity of The Hybrid Space must be addressed. Cronbach and Meehl (1955) places the validity of constructs within the content validity category and describes it as a complex question where the testing of validity must be capable of demonstrating the phenomenon investigated actually exist. Golafshani (2003) describes a construct in the context of validity as; *"…the initial concept, notion, question or hypothesis that determines which data is to be gathered and how it is to be gathered"* (p. 599). Construct validity therefore entails demonstrating the power of The Hybrid Space to framing cyber operator cognitive work environment. The development of The Hybrid Space is explained in chapters 1 and 4 and is grounded in existing theory in article one. However, taking the limitations outlined in this chapter into account, only the descriptions found in the literature on cyber operator work environment and own experience from education underpins the validity of The Hybrid Space conceptual frameworks to framing cyber operator cognitive work environment. However, considerable consistency regarding the complexity of cyber operator work environment exists in the literature and considerable insecurity about cyber operator practice and work environment exists both in the practice field and the scientific research area. It is therefore, at this time, impossible to claim that The Hybrids Space accurately represents the cognitive work environment of cyber operators. However, as a part one of the project four workshops were arranged in different sectors (i.e. Norwegian Ministry of Foreign Affairs, Sparebank 1 Accounting, Norwegian University of Science and Technolgy and The Norwegian Armed Forces Cyber Defence Staff) where The Hybrid Space was presented and discussed. All workshops gave feedback that the framework made sense, partly confirmed the challenges described with digitization and added insight enabling the further improvement of the framework prior to dissemination in article one. The OLB-model is not used in further research in this thesis, and therefore its validity will not be discussed.

4.5.3 Part 2

Validity of The Hybrid Space app is determined by whether it truly measures what it is intended to measure. As described in this chapter and elaborated in article four (Jøsok, Hedberg, Knox, Helkala, Lugo, et al., 2018), it is designed to measure the cognitive focus of cyber operators. As The Hybrid Space app participant window (See figure 4.2) is similar to all participants, the validity of the measurement cognitive focus will be dependent on the participants understanding of The Hybrid Space conceptual framework and interpretation of own cognitive focus in relation to the framework. According to Nevo (1985) the face validity (a part of content validity) is high if the purpose of the test is clear, even with naïve participants, and accordingly low if the test is unclear. As The Hybrid Space app is unique it is not tested or rated by other operators or subject matter experts yet this reduces the validity of the app. Also, the low number of participants and data points collected makes testing of content validity in this study difficult. However, The Hybrid Space app is made available for anyone and along with data presented in article five, this enables future studies to assess validity of The Hybrid Space app. The participants understanding of The Hybrid Space and their ability to identify own cognitive focus and indicate that accurately remains the major validity issues. To mitigate such causes of errors the framework was presented to the participants in day -6 (See figure 4.5) and a discussion amongst the participants were facilitated to establish common understanding.

Cognitive agility is measured by four metrics as shown in figure 4.4. Given that The Hybrid Space is representing the cyber operator cognitive work environment accurately and the cyber operator is accurately reporting cognitive location in the Hybrid Space app, content validity of cognitive agility in terms of cognitive movements in The Hybrid Space can be argued to be high. E.g. The Hybrid Space app is capable collecting data on cyber operator cognitive focus. Reliability of The Hybrid Space app cannot be assessed as a part of this study as it does not perform controls of its internal reliability nor have external data to control for external reliability.

4.5.4 Part 3

Part three of this study utilizes the CDX as the research arena as described in section 4.3. Employing a macrocognitive perspective and performing research in natural settings presents challenges to both validity and reliability because of its openness to include context and complexity. As in all behavioral sciences, the dilemma between internal validity by high levels of standardization versus ecological (external) validity and generalization has to be addressed. However, also controlled experiments also involve many compromises. Controlled experiments restrict context and often use tasks with well-defined goals and raise doubts about whether findings can be associated with natural settings (Ward et al., 2017). The macrocognitive perspective offers unique opportunities for discoveries and is therefore suitable for exploring complex and emerging phenomenon such as cyber operator competencies. However, it is also impossible to claim that the research arena contributes to enhance validity and reliability of this study.

The empirical part of this study, disseminated in article five, examines the relationship between self-regulation and cognitive agility. The empirical data on cognitive agility is collected in a non-controlled macrocognitive environment as defined in section 3.2, using the Hybrid Space app. Independent variable data is collected by the SRQ online questionnaire (See article five for description of the SRQ (Jøsok et al., 2019)). According to Brown et al. (1999) the SRQ is considered both valid and reliable with a high test-retest reliability for the total SRQ score ($r = .94$, $p < .0001$), high internal consistency of the scale ($\alpha = .91$) and strong convergent validity with concomitant measures. Cognitive agility is a novel measure and due to a lack of control group external reliability cannot be assessed.

4.5.5 Summary on validity and reliability

The section above outline a series of validity and reliability issues related to the concept and methods of this study. Other aspects that influence the validity of the project includes performance indicators and availability of a control group. There is currently no performance scale to assess good or bad performance of cyber operators. Additionally, there is no control group available, as the NDCA was the only higher education in Norway at the time of data collection that educates cyber operators.

The overall reliability of the study is impossible to assess, and the study is hard to replicate because of the lack of control group, research conditions (CDX) and the macrocognitive approach. The overall internal validity of the study is also difficult to assess as it depends on a series of concepts and methods outline above. This makes also the external validity of the study hard to assess. However, the experiment was outlined in article five as a pilot study and could both inspire and inform further research into cyber operator practice and education. Experience form this study suggest that subject matter expert assessment of performance is difficult as observing cyber operator behavior is challenging. Future studies should consider using cyber operators self-assessed performance as a measure of performance.

4.6 Researching young people

The Children and Young People's Participation and Competence Development (BUK) interdisciplinary research program is focused on the field of development of young people in the society of today and tomorrow (BUK, 2010). The participants in this project are between the age of 19 and 28 and they are selected to undergo a military education or have completed their military education. Many methodological issues are the same in research with young people as with adults (Heath, Brooks, Cleaver, & Ireland, 2009). In the context of this research project there are reasons to think that this is the case but there is one difference: the young people that are my informants have grown up with cyberspace, while adults have been gradually introduced to cyberspace. The speed of this change has been startling, and until recently research into young people’s worlds did not imply their digital activities, challenging social scientists to ‘keep up’ with the ubiquity of cyberspace in people’s lives (Yamada-Rice, 2017). It seems appropriate to assume that growing up with cyberspace as an integrated part of society create different experiences and competencies, thoughts and reflections about the pros and cons of digitization than generations prior to cyberspace. Therefore in the context of this project it is fruitful to apply an understanding of young people as similar to adults but who possess different competencies (Punch, 2002). Since the research participants are in the higher part of the definition of young people, no specific measures were taken because of their age during this research.

4.7 Ethical considerations

Research ethics have gained extensive attention over the last decades (David, Tonkin, Powell, & Anderson, 2005). Research ethics have been criticized for being reduced to filling out forms and seeking clearance from an ethics committee, with informed consent, anonymity and confidentiality as the key strands instead of sparking a process of reflection upon ethical issues in the research design (Allen, 2005; Farrell, 2005; Heath et al., 2009). Alderson (2005) describe that for the formal requirements may contribute to reducing research ethics to an afterthought or the last hurdle in planning a project. In order to mitigate the potential negative effects of mindless application of rules and forms and come to view ethics as a strength and include it as a part of the whole research process (Heath et al., 2009), researchers have to make the ethical challenges visible and ethics need to be reflected upon and viewed as a strength rather than a limitation (Allen, 2005).

Most of the challenges with regards to research ethics are subject to strict procedures employed by the national ethics committee, the Norwegian Centre for Research Data, the research institutions own ethical standards and the standards of the science tradition one adheres to. This project is approved by the Norwegian Centre for Research Data and has been performed in accordance with the research strategy of the Norwegian Defence Cyber Academy. The experiment was carried out anonymously, participation was voluntarily, and students could withdraw at any time. However, during the research process there are also other aspects that involving ethical dilemmas, both obvious and hidden, that I now will account for.

In this project the obvious ethical challenges, are mainly concerned with the ethical aspects regarding the age of the participants, the context where the research is preformed, the role and potential influences of the researchers presence, the modes of communication with the participants when recruiting and gathering data and various aspects when processing the data. As argued in section 4.6, the age of the participants is not an issue that involves major ethical challenges. Nevertheless, I want to underline that all participants are handled with the outmost respect. The context of the experiment is that of a cyber defence exercise as a part of the military education. This context implies the rules and norms of the military profession. While the military profession traditionally is associated with a strict hierarchy, this specific CDX emphasizes trust between participants and superiors. This is in the acknowledgment of the theme of article two, the need for a grounded communication in complex environments (Knox et al., 2018). It is difficult to say if military profession culture influenced research results, but in terms of ethical questions I am confident that the relationship between students and exercise control, as well as between participant and researcher was respectful. This was also emphasized in the recruitment of participants, that the participation was voluntarily and that they could withdraw from the study at any time with no questions asked.

During the experiment I had a double role. I was responsible for developing the scenario of the exercises and was doing research. My rank at the time was second lieutenant and I therefore ranked well above the rank as cadet. However, developing the scenario was completed beforehand and my interaction with the students in the role as an exercise facilitator limited itself to the morning scenario briefing as showed in Figure 4. 5: Experimental setup. The rest of the day I had the role as a researcher receiving results from the student via The Hybrid Space app. If this dual role influenced the research is difficult to say, but any social science researcher is dependent upon a mature ethical mental model and a well-developed reflexivity[21]. Principles I try to adhere to and practice in my research.

4.8 Methodological strengths and limitations

The major methodological strength of this thesis is that it contributes to methodology in cyber operator practice by offering a framework, a method of collecting and analyzing data and validates the approach. However, this can also be considered a challenge with this study as it both defines the framework in use, and validates the same framework in a specific practice, by a special group of participants. Such an approach would be more exposed for experimenter bias, which also has to be considered a potential weakness of the study. A further weakness in this sense, is the lack of a control group to compare results with and a lack of other studies utilizing the same methodology. However, even if the relatively low number of participants makes the findings hard to generalize, a strength is that the collected data is easily analyzed and show significant results between the dependent and independent variables. This contributes to validating the developed and proposed methodology of the study and paves the way for future research efforts to enhance the proposed methodology.

[21] Reflexivity is achieved through *"detachment, internal dialogue and constant (and intensive) scrutiny of the process through which the researcher constructs and questions his/her interpretation of field experiences"* (Davis, Watson, & Cunningham-Burley, 2017, p. 128).

The major limitation of the study is the difficulty of understanding both the context of cyber operator work environment and the relationship to cognitive competencies in combination with few theoretical and methodological frameworks to develop understanding and experiments from. I study a complex phenomenon with vague definitions and few validated methods to employ. Specifically, the challenge with defining performance as addressed in part one of the study and measuring performance as addressed in part two of the study is a limitation merging from the lack of available methods to define and measure these.

In this project I have tried to understand the role of cognitive competencies in cyber operator practice and education by applying a social cognitive and macrocognitive framework. By exposing my methodological foundation, I have made reference to my overall mode of thinking and accounted for my methodological choices. Every part of the research process is subject to ethical challenges, both obvious and hidden. Solving these challenges implies sound ethical judgement and high levels of reflexivity applied by the researcher in every part of a project.

5 Summary of the articles

In this chapter I summarize the findings in the five articles and explain how the findings contribute to answering the research questions.

5.1 Article 1

Exploring the Hybrid Space Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations (Jøsok et al., 2016). This article was published as a book chapter in 'Lecture notes in Computer Science' Volume 9774 and presented at the 10th International Conference on Augmented Cognition as a part of the 18th International Conference on Human Computer Interaction in Toronto, Canada in July 2016.

The first article of this thesis presents The Hybrid Space conceptual framework. The framework was developed in the context of military cyber operator education with the intent to allow for investigation of the role of cognitive science in cyber operations. In this article we discuss the consequences for individual cognition when adapting to higher levels of digitization and the following consequences when forced to operate in a complex hybrid space with human and technological assets and agents. The theoretical grounding of this article is interdisciplinary, combining knowledge from the fields of cyber security, psychology, leadership, expertise, military and organizational theory.

The article comprises of an introduction to The Hybrid Space conceptual framework supported by a literature review of the status of cognitive science in cyber operations that underpins the relevance of The Hybrid Space. In the literature review we identify three aspects that guide the work in this PhD project.

First, the literature review revealed that introduction of terms with the prefix cyber is emerging in military literature. This is attributed to acknowledgement of the cyberspace as an operational domain and a heightened awareness of cyber related matters in strategy and policy articles as well as in budgets and education, training and exercises. We find that the heightened awareness is materializing in terms like cyber power, cyberspace operations and cyber deterrence emerging in an effort to describe and highlight the importance of related activities. With grounding in the first part of the literature review we posit that future military personnel, in all branches, will encounter the raised complexity of joint military operations with cyberspace as the key enabler. We argue that the constant change and complexity of cyberspace raise the demands for the structure and content of education and training, the need for a better understanding of the relationships between cyberspace and the physical domains and better understanding of the cognitive challenges cyberspace presents.

Second, we identified that current approaches to understanding cyberspace and its implications to military operations are insufficient. The research areas of cyber-physical systems and socio-technical systems are discussed in light of The Hybrid Space conceptual framework. Both research approaches are found to be limiting to describe the role of cyberspace in military operations. We therefore advocate for a more holistic understanding of cyberspace that acknowledge the two existing approaches and include them as a part of The Hybrid Space conceptual framework. The following discussion exposes that the integration of cyberspace into military operations presents a research gap that concerns more than just understanding cyberspace from a technological or human factor view. We conclude that the current situation is characterized by a lack of understanding of the human factors.

Third, the literature review reveals a growing number of researchers advocating for a varied skill-set amongst cyber operators. However, what exactly the varied skill-set are, over and above the technical proficiency needed to enter and operate in cyberspace, are not defined sufficiently to implement these in education and training. We discuss the application of The Hybrid Space conceptual framework as a tool capable of framing the complex work environment of young cyber operators and hypothesize the cognitive demands and corresponding skill-sets needed to master such environments. We posit that operating in The Hybrid Space requires cognitive competencies like metacognition, self-regulation and cognitive agility.

We propose a framework - The Hybrid Space conceptual framework - allowing for the research and application of psychological concepts in assessment, training and action. This article therefore contributes to answer the first research question by presenting a conceptual framework capable of describing the cognitive work environment of cyber operators. However, we conclude that more research into the non-technical competencies is needed.

5.2 Article 2

Socio-technical communication: The Hybrid Space and the OLB-Model for science-based cyber education. (Knox et al., 2018). The article was published in the journal of Military Psychology in July 2018.

In this article we present the Orientate, Locate, Bridge (OLB) Model which extends The Hybrid Space conceptual framework presented in article one by applying it to develop the OLB-Model. We utilize The Hybrid Space as a blueprint to investigate communicative challenges between different military ranks when performing cyber operations. The OLB-Model is proposed as a tool capable of mitigating the identified and discussed communicative challenges. Application of the OLB-Model in cyber operator education and training at the NDCA is dicussed.

The article comprises of an introduction to the OLB-Model supported by a literature review of the role of communication in safety-critical contexts. Applications of the OLB-Model in cyber operator education are presented.

The literature review discloses that lessons from safety-critical, socio-technical systems demonstrate the importance of the human factor and communication. The review does not identify any lessons or models within the research literature that focus on the role of communication in military cyber operations. Consequently, in this article we identify a need to study communication in the context of cyber operations. With support from the literature review we specifically identify a mutual need for perspective-taking skills between communication partners to understand others' need for information, their mental workload, and awareness concerning one's own momentary cognitive states and susceptibilities, as well as available strategies to adapt to the communication partners' preferences. Common ground theory provides the theoretical framework for understanding these elements of successful social interaction where partners are able to co-construct a shared mental model that can support a shared consciousness. Based on the abovementioned aspects we present the three stages of the OLB-Model and show the important role of grounded communication by exemplifying a young cyber operator presenting a recognized cyber picture to a senior non-technical officer during the three phases:

Phase 1: Orienting—momentary metacognitive awareness of one's cognitive location in The Hybrid Space.
Phase 2: Locating—accurately judge the communication partners' cognitive location in The Hybrid Space.
Phase 3: Bridging—adapting content and style to ensure grounding for appropriate communication to construct a shared mental model of the current situation.

We further disclose how the NDCA scaffolds its curriculum to educate cyber operators to communicate efficiently in cyber operations, as shown in figure 5.1: OLB pedagogy at the NDCA.

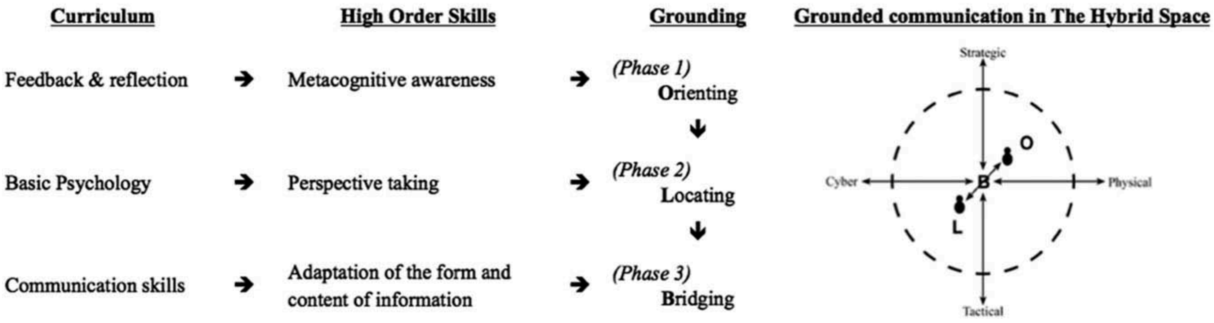


Figure 5. 1: OLB pedagogy at the NDCA

In this article we also provide examples of how application of the OLB-Model can improve grounded communication in hybrid and multi-domain environments, better regulatory behaviors and improve team communications.

We conclude that educators of military cyber operators need to acknowledge the need to teach and train the non-technical competencies of cyber operators. To improve communication, we show how enhanced metacognitive skills and mutual perspective-taking competencies can be included in education. We also show how The Hybrid Space conceptual framework can be used to locate communication partners within a cognitive space determined by tactical/strategic and cyber-physical/sociotechnical dimensions. In this way article two answers research question two by proposing the three-phase OLB model to describe dyadic interaction in The Hybrid Space. This article also informs research question five as it shows a way of operationalizing The Hybrid Space conceptual framework.

5.3 Article 3

Macrocognition applied to The Hybrid Space: Team environment, functions and processes in cyber operations (Jøsok et al., 2017). The article was published as a book chapter in 'Lecture notes in Computer Science' Volume 10285 and presented at the 11th International Conference on Augmented Cognition as a part of the 19th International Conference on Human Computer Interaction in Vancouver, Canada in July 2017.

In this article we discuss the environment, functions and processes of cyber operator teams. The article builds on findings and insights from articles one and two - and populates The Hybrid Space by including team aspects. In this article we discuss the role of macrocognition in cyber operator teams during CDXs, as part of their bachelor's degree education. We present the macrocognitive framework and discuss the role of macrocognition in The Hybrid Space context. Application of the macrocognitive framework during conduct of CDXs at the NDCA is discussed.

The literature review of cyber operator teams reveals a focus on utilizing technology to aid individual cyber operators for better sense-making and decision making. Little research is found addressing the team dynamics of cyber teams, despite the fact that lessons from other performance critical domains reveal that team dynamics are essential to performance. We therefore conclude that there is a limited understanding, and a research gap, concerning team functions and processes in cyber operations, despite the fact that cyber operators are working in teams.

The environment described by The Hybrid Space conceptual framework is found to resemble the features of a macrocognitive environment. Therefore, the two frameworks are juxtaposed to gain a better understanding of the functions and processes that occur in hybrid and macrocognitive environments. In this way we use research in the area of macrocognition and discuss the applicability to cyber operator teams.

The literature review identifies three factors that can contribute to the breakdown of cyber team performance; team structure, team communication and information overload. These factors are discussed in the context of the macrocognitive framework. We conclude that the complexities of The Hybrid Space are found to require cross-domain reciprocal collaboration between team members as well as a flexible team structure that can adapt to changing goals or demands. Formal hierarchy and information load are found to limit the communication between team members. Lack of communication limits performance of the team and should be accounted for in educational and training efforts. We propose utilizing new educational paradigms that empower students and foster a collaborative and creative learning environment. Examples and experiences from conducting CDXs at the NDCA are discussed.

Article three answers research question three by describing team interaction in The Hybrid Space, informs research question four by identifying factors that contribute to breakdown of cyber operator performance.

5.4 Article 4

Development and application of The Hybrid Space app for measuring cognitive focus in hybrid contexts (Jøsok, Hedberg, Knox, Helkala, Sütterlin, et al., 2018). The article was published as a book chapter in 'Lecture notes in Computer Science' Volume 10915 and presented at the 12th International Conference on Augmented Cognition as a part of the 20th International Conference on Human Computer Interaction in Las Vegas, Nevada in July 2018.

In this article we present the operationalization of cognitive agility by utilizing The Hybrid Space conceptual framework. The article presents the development of a self-report software, The Hybrid Space app, to help capture, visualize and analyze the cognitive focus of individuals and teams operating / conducting cyber operations. Further, an example describes the context in which the software was applied to capture cognitive focus of a cohort of cyber cadets at the NDCA participating in a four-day CDX. Examples of collected data are presented and the applicability of the software is discussed.

This article defines cognitive agility as; *"…the ability to be attentionally flexible, where flexible expansion and contraction of cognitive focus allows for both panoramic and selected attention in The Hybrid Space"* (p. 2). The literature review on how to capture cyber operator thinking processes concludes that there are no available methods that are designed to capture the cognitive focus of cyber operators when performing cyber operations. Hence, in this article we utilize The Hybrid Space as a tool to capture the cognitive focus of cyber operators. The operationalization of the cognitive movements is presented as in figure 4.4. The Hybrid Space app is described and the necessary instructions to download and apply the software are made available free of charge. Example data captured with the software during the 2017 CDX performed at the NDCA is presented (See figure 4.3).

The Hybrid Space app is a tool providing the researcher with a developed software and method of capturing and visualizing momentary cognitive focus and the dynamics of individuals in Hybrid Space contexts. Compared to other methods of cognitive data collection like CTA, fMRI or EEG[22], using The Hybrid Space app gives access to new and qualitatively different data on individual cognitive dynamics with a minimum of intrusion. The software further provides the opportunity to visualize the cognitive agility of cyber operators and teams for research, training and feedback purposes. The Hybrid Space app provides necessary computation options of variables and displays various measures of movement in The Hybrid Space, on individual and group level. Applicable contexts and further development are discussed.

Article four contributes to answering research question four by presenting the cognitive agility construct as a potential performance measure in cyber operations and in this way linking cognitive competencies and cyber operator performance. This article also helps answering research question five as it makes use of The Hybrid Space framework in design of the Hybrid Space app and the development of a method to collect and analyze cyber operator cognitive data.

5.5 Article 5

Self-regulation and cognitive agility in cyber operations (Jøsok et al., 2019). The article was published online in the Frontiers in Psychology Journal in April 2019.

In the fifth article we aimed to put the developed theory and methodology to use by investigating the association between self-regulation and cognitive agility in The Hybrid Space.

We extend the knowledge developed in the previous articles by using The Hybrid Space conceptual framework, revealing individual and team cognitive location in The Hybrid Space,

[22] CTA: Cognitive task analysis. fMRI: Functional magnetic resonance imaging. EEG: electroencephalogram

investigating cognitive agility in relation to self-regulation through operationalization of The Hybrid Space and The Hybrid Space App.

The state of art in this article concludes that cyber operator tasks, competence requirements, and performance are unsettled concepts that lack clear definition and guidelines to support selection, education, and training. We advocate that proper education and training of such personnel requires new insight into the competencies that are beyond cyber specific technical skills, in order to govern the complexity of operating in a cyber-physical hybrid environment.

The research project presented in this article contributes to the debate on military cyber personnel competencies by discussing how cyber defence operator's level of self-regulation can contribute to their performance in operations. We hypothesized that higher levels of self-regulation predict higher levels of cognitive agility as measured by cognitive movement in The Hybrid Space conceptual framework.

The results support the hypothesis by showing that self-regulation predicts cognitive agility in cyber operators when performing defensive cyber operations during a CDX. As found in the first article of this thesis, theories of cyber operator competencies highlight that cyber operators need a varied skill-set and competencies beyond technical proficiency to perform well. Results are in line with theories of cyber operator competencies, and we contribute to cyber operator competence profiles by confirming that cyber operators' self-regulation is associated with performance in cyber operations. This work highlights the need to focus on developing cyber operators' cognitive competencies as pathways to better performance.

Article five answers research question six by associating self-regulation and cognitive agility in The Hybrid Space. This article also lay the foundation for answering research question four by providing empirical evidence for the connection between cognitive competencies and cyber operator performance. Finally, the findings in this article informs research question five by giving a concrete example of how The Hybrid Space can be operationalized.

6 Concluding remarks

The challenge to cyber operators is to have the technological fidelity to conduct cyber operations and simultaneously understand the operational environment in which they operate. As the aim in this thesis is to uncover the role of cognitive competencies, the result informs the future direction of education of cyber operators. There is reason to believe that the role of cognitive competencies is to support the cyber operator in all parts of performing cyber operations through better self-regulation and cognitive agility. Self-regulation might be a key cognitive competency that supports exercise of other cognitive competencies that can in turn, support cyber operator performance. Cognitive agility is proposed as specific cognitive competency associated with cyber operator performance.

The combined literature reviews in articles one to six in concert with chapter 2 of this extended abstract have outlined the prior research efforts into cyber operator competencies. In this thesis I document research gaps in the areas of; cyber operator cognitive work environment; cyber operator practice; and description and empirical underpinning of cyber operator cognitive competencies. This thesis contributes to the research community by directing attention to the role of cognitive competencies in cyber operations and can guide future research by providing a conceptual framework capable of framing cyber operator cognitive work environment and enabling research on cyber operator performance. Additionally, this PhD can inform education and training of this new category of personnel by employing the framework, models, methodology and theory developed as a part of this project.

In this final chapter I present the main contributions and implications in this PhD. Presentation of the contributions are divided into three sections; conceptual, methodological and empirical. I also discuss the limitations and possibilities for further research.

6.1 Conceptual contributions

The first part of this project is concerned with development and exploration of The Hybrid Space conceptual framework. The Hybrid Space conceptual framework is developed to capture the complexity of cyber operator work environment and through articles one to three, I populate The Hybrid Space in order to describe the cognitive work environment of cyber operators. This includes describing dyadic interaction and team interaction in The Hybrid

Space. Throughout the PhD project I employ The Hybrid Space conceptual framework to develop the understanding of cyber operator practice and the implications for military operations and national security. In article two The Hybrid Space is specifically utilized along with principles of cognitive engineering to develop the OLB-model; capable of mitigating communicative challenges in cyber operations through application in education and training. In article three The Hybrid Space is utilized in conjunction with the macrocognitive perspective to describe cyber operator team interaction and inform development of realistic cyber operator training.

The conceptual contributions therefore contribute to answer the first research question by presenting a conceptual framework capable of describing the cognitive work environment of cyber operators. In this way article two answers research question two by proposing the three-phase OLB model to describe dyadic interaction in The Hybrid Space. Article three answers research question three by describing team interaction in The Hybrid Space and informs research question four by identifying factors that contribute to breakdown of cyber operator performance.

6.2 Methodological contributions

The second part of this project is concerned with developing a method and a software to collect empirical data on cyber operator cognitive competencies. To achieve this objective, I have in this thesis attempted to make a methodological contribution in how to study cognitive competencies of cyber operators. This effort required a review of existing methodological frameworks and tools as well as an assessment of their applicability. However, the absence of established methodology in cyber operator competency research required the development of new methodology and tools to be able to capture the necessary data.

The major methodological contribution in this respect was the development and application of the Hybrid Space app. In order to make data collection possible, this software was specified, programmed and put to use as a part of this thesis. This development is thoroughly documented in article four and chapter 4 of this extended abstract. Collected data was analyzed and disseminated in article five. The software is made available online for anyone who wants to use it and can be customized and put to use in further research.

The second methodological contribution is the cognitive agility construct. The first part of this project revealed that the complexities and insecurities of the cyber operator work environment means that there are currently no established performance measures for cyber operators. This implies that competence requirements are difficult to carve out in the absence of measurements of success. In this thesis, I have reviewed the current status of performance measures and available tools to measure cyber operator effectiveness and critiqued these for being too technically focused. Assessing cognitive competencies therefore required development of a method to capture cognitive focus and operationalize cognitive manoeuvre in order to be able to analyze individual cyber operator performance. The cognitive agility construct was developed to operationalize performance of cyber operators. Development of the construct is presented in chapter 3 and articles four and five. In article five, I validate that this approach is capable of producing statistically significant results.

The two abovementioned methodological contributions help answer research question five by make available the Hybrid Space app and the accompanying method to collect and analyze cyber operator cognitive agility. Research question four is answered by linking cognitive competencies and cyber operator performance by developing the cognitive agility construct. These are important contributions to a new area of research with few established methodologies.

6.3 Empirical contributions

The third part of this project is concerned with collecting and analyzing quantitative data on cyber operator cognitive agility. In article five, the proposed importance of cognitive agility was empirically validated by employing a well-researched cognitive construct: self-regulation, grounded in social cognitive theory. Individual level of self-regulation was associated with cognitive agility and cyber operator performance. Even with the limitations of a naturalistic research environment and the issue of measuring cyber operator performance discussed in chapter 4, the results give strong indications that the cognitive competencies that aid the operator in regulating own thoughts and actions are associated with performance. These results are important as empirical underpinned knowledge about the role of the cognitive competencies of cyber operators is absent from the research literature. The empirical data has contributed to knowledge and understanding about the relationship between cognitive competencies and cyber operator practice and education that can inform policy makers, education and competence development of this and related practices.

6.4 Implications

Given how this thesis addresses an issue that is highly relevant for politicians, professionals and individuals, in Norway and beyond, I find it important to include some possible implications of this thesis. I therefore describe some of those implications for national policy makers, military education and competence development of citizens of society before ending with addressing limitations and future work.

6.4.1 Implications for national policy makers

In a digitized society, cyberspace is an integral part of almost all human activity. Cyber operator practice is a result of the need for nations to be able to project cyber power and defend from foreign cyber power projection. From a national security perspective, policy makers need to acknowledge the perils of digitization, as well as the promises offered. The digitization optimism present in contemporary society, might obfuscate other imperceptible aspects and long-term unintended consequences of a highly digitized society. Already exposed consequences include the possibility for foreign powers to influence elections and threaten democracy in and through cyberspace as well as digital economies which are highly dependent on cyberspace to function. This can make policy makers aware of the need to decide to invest in efforts to defend citizens and society against cyber-attacks. This thesis shows that effective defence against such threats, include investment in people and competencies in addition to investment in technology.

6.4.2 Implications for military education

Cyberspace adds a new domain to warfare that also melds with the traditional domains. The intangible and complex nature of cyberspace requires in depth technical competence to operate in, but it also reduces the distance between the strategic and tactical level; challenging the codes of conduct in the traditional military hierarchy. For the employment of cyber power to be effective, tight cooperation between strategic, operational and tactical level is required. This forces senior commanders to bridge with young cyber operators in ways that were inconceivable few years ago, because cyber operators potentially hold power to influence events at operational and strategic level in and through cyberspace. The literature reviews in article one to three support this argument and advocate for the need to develop the strategic appreciation of cyber operators situated at the tactical level, as well as to re-educate senior commanders in the utility of cyber power.

Traditionally, military recruits have been selected on the basis of physical and mental aptitude. While some parts of the military still require traditional selection strategies, it is hard to find arguments that support the same need for cyber operators. Their aptitude for conducting cyber operations and manoeuvre in The Hybrid Space first and foremost is based on cognitive competencies and technical proficiency. I have shown in this thesis that cognitive competencies could be a future pathway for the selection and training of cyber personnel. Article two and three present specific suggestions on how cognitive competencies can be implemented into cyber operator education and training to augment the development and application of technical competence. While the research in this thesis cannot conclude decisively the role of cognitive competencies in cyber operator practice an education, it is a promising way forward that future research should explore. If self-regulation acts as a core competency that supports the cyber operator performance, this could potentially be included in the selection, education and training of cyber operators.

6.4.3 Implications in a wider context

While this study has been performed in the context of Norwegian military cyber operator practice and education, and results inform development of these practices; the combined contributions of this thesis can also inspire and inform a wider audience. As defined in the introduction of this thesis; the cyber security workforce consists of both military and civilian cyber operators. The findings, conclusions and implications presented could therefore also inform civilian cyber operator practice and education in Norway and beyond. Especially since the tasks that military and civilian cyber operators perform share many of the same characteristics, and that defence from cyber threats in a national security perspective requires extensive civil-military and private-professional cooperation. Such cooperation would benefit from applying similar conceptual frameworks.

Research efforts in civilian cyber operator practice and education could apply the methods developed in this thesis. However, this would require a reframing of the context from military operations to business operation. The Hybrid Space app can be adjusted accordingly as outlined in article four. E.g. changing the tactical and strategic legend on the y-axis to other suitable legends to frame the cognitive environment of the corresponding context.

As discussed in this thesis, education and professional qualifications of cyber officers is difficult to describe due to the complexity of the work environment, the pace of change in cyberspace, the lack of performance measures and the cognitive nature of work. This can also be argued to be characteristics valid for a wider audience in a digitized society. The omnipresence of cyberspace in contemporary society, the intangible characteristics of cyberspace, the rapid developments in the cyber technology and application of that technology exposes all digital citizens to cyber-attacks and influence activities. In light of these factors, insights from working with this thesis include that the competence requirements of digital citizens at all ages are rapidly changing. In my opinion being a competent digital citizen require more than the ability to operate digital artefacts. This thesis suggests self-regulation as one cognitive competence that potentially could augment the education of digital citizens. And the proposed similarity in competence structures of cyber officers and digital citizens in chapter 3 might suggest that research in the two areas can inform each other.

6.5 Limitations

Advancing towards the end of this thesis, I will first address some of the overall limitations of this thesis before addressing the question of future directions of cyber operator competence research.

A widely addressed challenge, within the area of cyber operations and cyber operator competencies, is that there are no unifying definitions of the concepts. Further there are a number of similar terms used interchangeably, none with clear definitions. The definitions offered by researchers are often very broad, with the intent of covering all aspects of a concept, or very specific failing to cover the different elements of the concept. This situation is very limiting to this thesis, as a researcher has to define concepts to be able to advance in the research process, however knowingly with vague definitions. As stated in chapter 4, this limitation become visible in The Hybrid Space as it cannot be stated a model or clear representation of reality but has to be considered a conceptual framework.

A variety of issues relating to cyberspace are presenting researchers with research challenges. One is the complexities and intangible nature of cyber operator work environment, which makes it challenging to understand and to research. As discussed in chapter 4, a variety of scientific traditions are combined in cyber operator practice. Therefore, one of the most elaborated challenges is the need for interdisciplinary research efforts. This currently seems the most rewarding way to approach the challenges presented. However, it also complexifies research as several traditions have to be joined to be able to advance in knowledge, adding complexity to the process as ontological and epistemological beliefs also are juxtaposed. Combining the factors mentioned above creates significant methodological challenges to research on cyber operator practice. One example is that to inform conceptual understanding of the cyber operator environment literature reviews has to include several areas of research. Something that reduces consistency of findings and hence must be considered a limitation.

A lack of established theory and methodology within the area of cyber operator practice is a limitation. In this thesis this is mitigated by augmenting theory and developing methodology. However, it has to be considered a limitation as the applied theory is one of a kind for this project and the applied methods are not validated by other researchers. One example is the cognitive agility construct that is proposed as cognitive competency that can quantify cyber operator performance. While this thesis proposes cognitive agility as a performance measure, this cannot be concluded decisively because of the limited number of participants in this research.

The conduct of the experiment by utilizing the annual CDX at the NDCA is not a limitation on its own, but the fact that the experimental conditions would be almost impossible to regenerate by other researchers would by many be defined as a limitation. Also, the special category participant of this study would be hard to find elsewhere. This also makes it impossible to generalize the result to a larger population.

The ability to project cyberpower and to defend against foreign cyberpower is an issue of national security and often subject to secrecy and strictly guarded capabilities. Therefore, gaining access to research cyber operator practice and getting the necessary clearance to disseminate results will be a limitation and a research challenge not only for this thesis, but for any research into cyber operator practice for many years to come.

6.6 Future work

The disseminated results and the research gaps identified in this thesis inform future research possibilities. Future research should venture into the challenge of describing cyber operator practice better in order to lay the foundation for advanced understanding and research into this area. One possibility is to decompose and analyze cyber operator tasks by utilizing cognitive load theory and utilize established cognitive load methodology, alone or in conjunction with The Hybrid Space app, to advance in understanding of the cognitive requirements of different tasks. A possible research area is how to perform interdisciplinary research on cyber operator competence and should include the development of research methodology, methods and metrics. Future research could aim at finding out how cognitive aptitude can inform selection and how development of cognitive competencies can be implemented in cyber operator education, including evaluation of the effectiveness of different content and pedagogy.

References

Adnan, M., Just, M., Baillie, L., & Kayacik, H. G. (2015). Investigating the work practices of network security professionals. I*nformation and Computer Security, 23*(3), 347-367. doi:https://doi.org/10.1108/ICS-07-2014-0049

Alderson, P. (2005). Designing ethical research with children. In A. Farrell (Ed.), *Ethical Research with Children* (pp. 27-36). United Kingdom, Berkshire: Open University Press, McGraw-Hill.

Allen, G. (2005). Research ethics in a culture of risk. In A. Farrell (Ed.), *Ethical Research with Children* (pp. 15-26). United Kingdom, Berkshire: Open University Press, McGraw-Hill.

Anmarkrud, Ø., Andresen, A., & Bråten, I. (2019). Cognitive Load and Working Memory in Multimedia Learning: Conceptual and Measurement Issues. *Educational psychologist, 54*(2), 61-83. doi:https://doi.org/10.1080/00461520.2018.1554484

Artuch-Garde, R., González-Torres, M. d. C., de la Fuente, J., Vera, M. M., Fernández-Cabezas, M., & López-García, M. (2017). Relationship between Resilience and Self-regulation: A Study of Spanish Youth at Risk of Social Exclusion. *Frontiers in Psychology, 8*(612). doi:https://doi.org/10.3389/fpsyg.2017.00612

Ayer, A. J. (1968). *The Origins of Pragmatism - Studies in the Philosophy of Charles Sanders Pierce and William James.* London, Melbourne, Toronto: MacMilllan and Co ltd.

Baker, M. (2016). *Striving for effective cyber workforce development.* Pittsburg, PA: Carnegie Mellon University Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_473577.pdf

Bandura, A. (1986). *Social Foundations of Thought & Action - A Social Cogntive Theory.* New Jersey: Prentice Hall.

Bandura, A. (1997). *Self-Efficacy - The Exercise of Control.* New York: W.H. Freeman and Company.

Barutchu, A., Carter, O., Hester, R., & Levy, N. (2013). Strength in Cognitive Self-Regulation. *Frontiers in Psychology, 4*(174). doi:https://doi.org/10.3389/fpsyg.2013.00174

Baumeister, R. F., Heatherton, T. F., & Tice, D. M. (1994). *Losing control: How and why people fail at self-regulation.* San Diego, CA: Academic Press.

Baumeister, R. F., & Vohs, K. D. (2007). Self-Regulation, Ego Depletion, and Motivation. *Social and Personality Psychology Compass, 1*(1), 115-128. doi:https://doi.org/10.1111/j.1751-9004.2007.00001.x

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in human behavior, 48*, 51-61. doi:https://doi.org/10.1016/j.chb.2015.01.039

Bennett, S., Maton, K., & Kervin, L. (2008). The 'digital natives' debate: A critical review of the evidence. *British Journal of Educational Technology, 39*(5), 775-786. doi:https://doi.org/10.1111/j.1467-8535.2007.00793.x

Boote, D. N., & Beile, P. (2005). Scholars Before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation. *Educational Researcher, 34*(6), 3-15. doi:https://doi.org/10.3102/0013189X034006003

Borghetti, B., Funke, G., Pastel, R., & Gutzwiller, R. (2017). Cyber Human Research from the Cyber Operator's View. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 61*(1), 350-350. doi:https://doi.org/10.1177/1541931213601569

Boyatzis, A. R. (1982). *The competent manager: A model for effective performance.* New York: Wiley.

Brombach, H. (2018, 27th of December 2018). Fylkesmannen i flere fylker utsatt for nettverksangrep [County Governors exposed to cyber attack]. *Digi.no.* Retrieved from https://www.digi.no/artikler/fylkesmannen-i-flere-fylker-utsatt-for-nettverksangrep/454456

Brown, J. M., Miller, W. R., & Lawendowski, L. A. (1999). The self-regulation questionnaire. In L. Vandecreek & T. L. Jackson (Eds.), *Innovations in clinical practice: A source book, Vol. 17.* (pp. 281-292). Sarasota, FL, US: Professional Resource Press/Professional Resource Exchange.

Buchler, N., Fitzhugh, S. M., Marusich, L. R., Ungvarsky, D. M., Lebiere, C., & Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. *Frontiers in Psychology, 7*(937), 937. doi:https://doi.org/10.3389/fpsyg.2016.00937

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L. (2018). Cyber Teaming and Role Specialization in a Cyber Security Defense Competition. *Frontiers in Psychology, 9*(2133). doi:https://doi.org/10.3389/fpsyg.2018.02133

BUK (2010). *Child and Youth Participation and Competence Development.* Lillehammer: Lillehammer University College

Caliskan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis, 35*(1), 40-58. doi:https://doi.org/10.1080/14751798.2019.1565364

Carter, M. J., & Fuller, C. (2015). Symbolic interactionism. *Sociopedia.isa, 1*, 1-17. doi:https://doi.org/10.1177/205684601561

Castells, M. (2010). *The Rise of the Network Society* (Second ed. Vol. 1): Wiley-Blackwell.

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016). Cyber workforce development using a behavioral cybersecurity paradigm. *2016 International Conference on Cyber Conflict,* 1-6. doi:https://doi.org/10.1109/CYCONUS.2016.7836614

Cetin, B. (2015). Academic motivation and self-regulated learning in predicting academic achievement in college. *Journal of International Education Research (JIER), 11*(2), 95-106. doi:https://doi.org/10.19030/jier.v11i2.9190

Champion, M., Jariwala, S., Ward, P., & Cooke, N. J. (2014). Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 310-314. doi:https://doi.org/10.1177/1541931214581064

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-based cyber defense analysis. *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support,* 218-221. doi:https://doi.org/10.1109/CogSIMA.2012.6188386

Chief of Defence (2019). *Forsvarssjefens Militærfaglige Råd [Chief of Defence Military Advice to The Secretary of Defence]*. Norwegian Armed Forces Retrieved from www.forsvaret.no

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731. doi:https://doi.org/10.1016/j.cose.2011.08.004

Clarke, R. A., & Knake, R. K. (2010). *Cyber war - The next threath to national security and what to do about it.* New York: Harper Collins Publishers.

Conti, G., Nelson, J., & Raymond, D. (2013). Towards a cyber common operating picture. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1-17. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6568383&isnumber=6568361

Coolican, H. (2014). *Research Method and Statistics in Psychology* (Sixth ed.). London: Psychology Press.

Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin, 52*(4), 281-302. doi: https://doi.org/10.1037/h0040957

Cross, M. (2008). *Scene of the cybercrime* (Second ed.). Burlington, MA: Syngress, Elsevier.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*(3), 229-233. doi:https://doi.org/10.1177/154193120504900304

D’Amico, A., Buchanan, L., Kirkpatrick, D., & Walczak, P. (2016). Cyber Operator Perspectives on Security Visualization. Advances in Human Factors in Cybersecurity. *Advances in Intelligent Systems and Computing, 501*, 69-81. doi:https://doi.org/10.1007/978-3-319-41932-9_7

D’Amico, A., & Whitley, K. (2008). The Real Work of Computer Network Defense Analysts. In J. R. Goodall, G. Conti, & K.-L. Ma (Eds.), VizSEC 2007: *Proceedings of the Workshop on Visualization for Computer Security* (pp. 19-37). doi:https://doi.org/10.1007/978-3-540-78243-8_2

David, T., Tonkin, J., Powell, S., & Anderson, C. (2005). Ethical aspects of power in research with children. In A. Farrell (Ed.), *Ethical Research with Children.* United Kingdom, Berkshire: Open University Press, McGraw-Hill.

Davis, J., Watson, N., & Cunningham-Burley, S. (2017). Disabled children, ethnography and unspoken understandings - The colloborative construction of diverse identities In P. Christensen & A. James (Eds.), *Research With Children - Perspectives and Practices* (Third ed.). New York: Routledge.

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology, 9*(744). doi:https://doi.org/10.3389/fpsyg.2018.00744

Department of Defence (2018). *DOD Dictionary of Military and Assoiated Terms.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Dombrowski, P., & Demchak, C. C. (2014). Cyber war, cybered conflict, and the maritime domain. *Naval War College Review, 67*(2), 70-96. Retrieved from http://www.jstor.org/stable/26397758

Duggan, P. (2016). To Operationalize Cyber, Humanize the Design. *Small Wars Journal*. Retrieved from http://smallwarsjournal.com/jrnl/art/to-operationalize-cyber-humanize-the-design

Edgar, T. W., & Manz, D. O. (2017). *Research Methods In Cyber Security*. Cambrigde, MA: Syngress, Elsevier.

Endsley, M. R. (2000). Theoretical underpinnings of situation awareness: A critical review. In M. R. Endsley & D. Garland (Eds.), *Situation awareness analysis and measurement* (Vol. 1, pp. 24). Mahwah, NJ: Lawrence Erlbaum Associates.

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., & Fink, G. (2012). A Multi-Phase Network Situational Awareness Cognitive Task Analysis. *Information Visualization, 9*(3), 204-219. doi:https://doi.org/10.1057/ivs.2010.5

Farrell, A. (2005). Ethics and research with children. In A. Farrell (Ed.), *Ethical Research with Children* (pp. 1-14). New York: Open University Press, McGraw-Hill

Ferrari, A. (2012). Digital competence in practice: An analysis of frameworks. European Commission. Joint Research Centre. doi:https://doi.org/10.2791/82116

Fiore, S. M., Rosen, M. A., Smith-Jentsch, K., Salas, E., Letsky, M., & Warner, N. (2010). Toward an understanding of macrocognition in teams: predicting processes in complex collaborative contexts. *Human Factors, 52*(2), 203-224. doi:https://doi.org/10.1177/0018720810369807

Forsythe, C., Silva, A., Stevens-Adams, S., & Bradshaw, J. (2013). Human Dimension in Cyber Operations Research and Development Priorities. *International Conference on Augmented Cognition, 8027*, 418-422. doi:https://doi.org/10.1007/978-3-642-39454-6_44

Fransson, G. (2016). Manoeuvring in a digital dilemmatic space: making sense of a digitised society. *Nordic Journal of Digital Literacy, 11*(3), 185-201. doi:https://doi.org/10.18261/issn.1891-943x-2016-03-04

Galeotti, M. (2014, 6th of July). The ‘Gerasimov Doctrine’ and Russian Non- Linear War. Retrieved from https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Getha-Taylor, H., Hummert, R., Nalbandian, J., & Silvia, C. (2013). Competency Model Design and Assessment: Findings and Future Directions. *Journal of Public Affairs Education, 19*(1), 141-171. doi:https://doi.org/10.1080/15236803.2013.12001724

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. The *Qualitative Report, 8*(4), 597. Retrieved from: http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology & People, 22*(2), 92-108. doi:https://doi.org/10.1108/09593840910962186

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. (2015). The human factors of cyber network defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 59*(1), 322-326. doi:https://doi.org/10.1177/1541931215591067

Hammond, K. R. (1998). *Ecological Validity*. Then and Now. Department of Psychology, University of Colorado Retrieved from http://www.brunswik.org/notes/essay2.html

Hartig, J., Klieme, E., & Leutner, D. (2008). *Assessment of Competencies in Educational Contexts.* Göttingen: Hogrefe & Huber Publishers.

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence Based Nursing, 18*(3), 66-67. doi:https://doi.org/10.1136/eb-2015-102129

Heath, S., Brooks, R., Cleaver, E., & Ireland, E. (2009). *Researching Young People's Lives.* London: Sage Publications Ltd.

Heffner, C. (2018). Variables, Validity, and Reliability. *In Research Methods.* Retrieved from https://allpsych.com/researchmethods/

Helsper, E. J., & Eynon, R. (2010). Digital Natives: Where Is the Evidence? *British Educational Research Journal, 36*(3), 503-520. doi:https://doi.org/10.1080/01411920902989227

Hoffman, R. R., & McNeese, M. D. (2009). A history for macrocognition. *Journal of Cognitive Engineering and Decision Making, 3*(2), 97-110. doi:https://doi.org/10.1518/155534309X441835

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

International Information Systems Security Certification Consortium (ISC) (2018). *Cybersecurity Workforce Study.* Retrieved from https://www.isc2.org: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

Jabbour, K. (2009). The science and technology of cyber operations. *Air Force Space Command Journal High Frontier, 5*(3), 11-15. Retrieved from https://www.afspc.af.mil/Portals/3/documents/HF/AFD-090519-102.pdf

Jabbour, K. (2010). Cyber Vision and Cyber Force Development. *Strategic Studies Quarterly, 4*(1), 63-73. Retrieved from http://www.jstor.org/stable/26269779

Jaramillo, J. M., Rendón, M. I., Muñoz, L., Weis, M., & Trommsdorff, G. (2017). Children's Self-Regulation in Cultural Contexts: The Role of Parental Socialization Theories, Goals, and Practices. *Frontiers in Psychology, 8*(923). doi:https://doi.org/10.3389/fpsyg.2017.00923

Joint Chiefs of Staff (2018). *Joint Publication 3-12 - Cyberspace operations.* Washington DC: United States Defence Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Jøsok, Ø., Hedberg, M., Knox, B. J., Helkala, K., Sütterlin, S., & Lugo, R. G. (2018). Development and Application of the Hybrid Space App for Measuring Cognitive Focus in Hybrid Contexts. In D. D. Schmorrow & C. M. Fidopiastis (Eds.), *Lecture Notes in Computer Science. Augmented Cognition: Intelligent Technologies* (Vol. 10915, pp. 369-382). doi:https://doi.org/10.1007/978-3-319-91470-1_30

Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R., Sutterlin, S., & Ward, P. (2016). Exploring the Hybrid Space Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations. In S. D. & F. C. (Eds.), *Lecture Notes in Computer Science. Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience* (Vol. 9744, pp. 178-188). doi:https://doi.org/10.1007/978-3-319-39952-2_18

Jøsok, Ø., Knox, B. J., Wilson, K., Helkala, K., Lugo, R. G., Sutterlin, S., & Ødegaard, T. (2017). Macrocognition applied to The Hybrid Space: Team environment, functions and processes in cyber operations. In S. D. & F. C. (Eds.), *Lecture Notes in Computer Science. Augmented Cognition. Enhancing Cognition and Behavior in Complex Human Environments* (Vol. 10285, pp. 486-500). doi:https://doi.org/10.1007/978-3-319-58625-0_35

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., & Helkala, K. (2019). Self-Regulation and Cognitive Agility in Cyber Operations. *Frontiers in Psychology, 10*(875). doi:https://doi.org/10.3389/fpsyg.2019.00875

Journal of Cybersecurity. (2020). *About the Journal.* Retrieved from https://academic.oup.com/cybersecurity/pages/About

Kalyuga, S., & Singh, A.-M. (2016). Rethinking the Boundaries of Cognitive Load Theory in Complex Learning. *Educational Psychology Review, 28*(4), 831-852. doi:https://doi.org/10.1007/s10648-015-9352-0

Kampenes, I. (2018). *The Military Cyber Domain.* Power Point presentation: Norwegian Armed Forces Cyber Defence Intranet

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security, 38*(2), 7-40. doi:https://doi.org/10.1162/ISEC_a_00138

Khooshabeh, P., & Lucas, G. (2018). Virtual Human Role Players for Studying Social Factors in Organizational Decision Making. *Frontiers in Psychology, 9*(194). doi:https://doi.org/10.3389/fpsyg.2018.00194

Klein, G. (2007). Flexecution, part 2: Understanding and supporting flexible execution. *IEEE intelligent systems, 22*(6), 108-112. doi:https://doi.org/10.1109/MIS.2007.107

Klein, G., & Klinger, D. (1991). Naturalistic decision making. *Human Systems IAC Gateway, 2*(1), 16-19. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.191.833&rep=rep1&type=pdf

Klein, G., Ross, K. G., Moon, B. M., Klein, D. E., Hoffman, R. R., & Hollnagel, E. (2003). Macrocognition. I*EEE intelligent systems, 18*(3), 81-85. doi:https://doi.org/10.1109/MIS.2003.1200735

Klein, G., & Wright, C. (2016). Macrocognition: From Theory to Toolbox. *Frontiers in Psychology, 7*(54). doi:https://doi.org/10.3389/fpsyg.2016.00054

Klein, J. T., & Newell, W. H. (1996). Advancing Interdisciplinary Studies. In J. G. Gaff & J. L. Ratcliff (Eds.), *Handbook of the Undergraduate Curriculum. A Comprehensive Guide to Purposes, Structures, Practices, and Change* (pp. 393-415). San Francisco, CA: Jossey- Bass.

Knott, B. A., Mancuso, V. F., Bennett, K., Finomore, V., McNeese, M., McKneely, J. A., & Beecher, M. (2013). Human factors in cyber warfare: Alternative perspectives. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*(1), 399-403. doi:https://doi.org/10.1177/1541931213571086

Knox, B. J. (2018). The Effect of Cyberpower on Institutional Development in Norway. *Frontiers in Psychology, 9*(717). doi:https://doi.org/10.3389/fpsyg.2018.00717

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

Knutsen, P. (2016). Gjensyn med spørsmålet om metode [Revisiting the question of methods]. In *Å forstå historie. Vitenskapsteori og forskningspraksis.* Kristiansand: Porta Forlag.

Kott, A., Ludwig, J., & Lange, M. (2017). Assessing Mission Impact of Cyberattacks: Toward a Model-Driven Paradigm. *IEEE Security & Privacy, 15*(5), 65-74. doi:https://doi.org/10.1109/MSP.2017.3681068

Krawczyk, D., Bartlett, J., Kantarcioglu, M., Hamlen, K., & Thuraisingham, B. (2013). Measuring expertise and bias in cyber security using cognitive and neuroscience approaches. *2013 IEEE International Conference on Intelligence and Security Informatics,* 364-367. doi:https://doi.org/10.1109/ISI.2013.6578859

Kuehl, D. T. (2009). From Cyberspace to Cyberpower - Defining the Problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24-42): University of Nebraska Press.

Lathrop, S. D., Trent, S., & Hoffman, R. (2016). Applying Human Factors Research Towards Cyberspace Operations: A Practitioner's Perspective. In D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity: *Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity,* July 27-31, 2016, Walt Disney World®, Florida, USA (pp. 281-293). doi:https://doi.org/10.1007/978-3-319-41932-9_23

Lecy, J. D., & Beatty, K. E. (2012). Representative literature reviews using constrained snowball sampling and citation network analysis. *Available at SSRN 1992601*. doi:http://dx.doi.org/10.2139/ssrn.1992601

Lee, J. D., Kirlik, A., & Dainoff, M. J. (2013). *The Oxford handbook of cognitive engineering.* Oxford, New York: Oxford University Press.

Leech, N. L., Dellinger, A. B., Brannagan, K. B., & Tanaka, H. (2010). Evaluating Mixed Research Studies: A Mixed Methods Approach. *Journal of Mixed Methods Research, 4*(1), 17-31. doi:https://doi.org/10.1177/1558689809345262

Lerner, R. M., Lerner, J. V., Bowers, E. P., Lewin-Bizan, S., Gestsdottir, S., & Urban, J. B. (2011). Self-regulation processes and thriving in childhood and adolescence: A view of the issues. *New directions for child and adolescent development, 2011(133)*, 1-9. doi:https://doi.org/10.1002/cd.300

Libicki, M. C. (2016). *Cyberspace in peace and war.* Annapolis, Maryland: Naval Institute Press.

Limnéll, J., & Salonius-Pasternak, C. (2016). *Challenge for NATO: Cyber Article 5.* Retrieved from www.fhs.se/cats

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365-404. doi:https://doi.org/10.1080/09636412.2013.816122

Lockheed Martin (2019). *The Cyber Kill Chain.* Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lugo, R. G., Sütterlin, S., Knox, B. J., Jøsok, Ø., Helkala, K., & Lande, N. M. (2016). The moderating influence of self-efficacy on interoceptive ability and counterintuitive decision making in officer cadets. *Journal of Military Studies, 7*(1), 44-52. doi:https://doi.org/10.1515/jms-2016-0005

Lysne, O. (2016). *Digitalt Grenseforsvar [Digital Border Defence].* Oslo: Ministry of Defence Retrieved from www.regjeringen.no

MacDonnell, U. (2014). Cyber Threat! How to manage the growing risk of cyber attacks. New Jersey: Whiley.

MacroCognition. (2016). *Macrocognition Functions and processes,* Illustration. Retrieved from http://www.macrocognition.com

Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014). Human factors in cyber warfare II emerging perspectives. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 415-418. doi:https://doi.org/10.1177/1541931214581085

Maness, R. C., & Valeriano, B. (2015). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society, 42*(2), 301-323. doi:https://doi.org/10.1177/0095327X15572997

McClain, J., Silva, A., Aviña, G. E., & Forsythe, C. (2015). *Measuring Human Performance within Computer Security Incident Response Teams.* Sandia National Laboratories. CA. Retrieved from: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2015/159030.pdf

McNeese, M., Cooke, N. J., D'Amico, A., Endsley, M. R., Gonzalez, C., Roth, E., & Salas, E. (2012). Perspectives on the Role of Cognition in Cyber Security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 56*(1), 268-271. doi:https://doi.org/10.1177/1071181312561063

Mihai-Ştefan, D. (2017). The 5th operational domain and the evolution of NATO's cyber defence concept. Annals: *Series on Military Sciences, 9*(2), 69-77.

Ministry of Local Government and Modernisation (2016). *Digital agenda for Norge — IKT for en enklere hverdag og økt produktivitet [Digital Agenda Norway] (Mld. St. 27 (2015-2016)).* Oslo: Statsministerens kontor Retrieved from https://www.regjeringen.no/

Ministry of Justice and Public Security (2017). *Cyber Security - A Joint Responibility (Meld. St. 38 (2016–2017))*. Oslo: Norwegian Government Security and Service Organisation Retrieved from https://www.regjeringen.no

Ministry of Finance (2017). *Perspektivmeldingen 2017 [Perspectives 2017] (Meld. St. 29 (2016-2017)).* Oslo Retrieved from https://www.regjeringen.no

Moilanen, K. L. (2007). The Adolescent Self-Regulatory Inventory: The Development and Validation of a Questionnaire of Short-Term and Long-Term Self-Regulation. *Journal of Youth and Adolescence, 36*(6), 835-848. doi:https://doi.org/10.1007/s10964-006-9107-9

Morrow, D. G., & Fischer, U. M. (2013). Communication in Socio-Technical systems. In J.D. Lee & A. Kirlik (Eds.), *The Oxford handbook of cognitive engineering,* 178-199. New York, NY: Oxford University Press.

Mukaka, M. M. (2012). A guide to appropriate use of Correlation coefficient in medical research. Malawi Medical Journal : *The Journal of Medical Association of Malawi, 24*(3), 69-71. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3576830/

Naím, M. (2013). *The end of power.* New York: Basic Books.

Nevo, B. (1985). Face Validity Revisited. *Journal of Educational Measurement, 22*(4), 287-293. doi: https://doi.org/10.1111/j.1745-3984.1985.tb01065.x

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National initiative for cybersecurity education (NICE) cybersecurity workforce framework.* NIST Special Publication, 800, 181. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-181/final

Nitsch, R., Fredebohm, A., Bruder, R., Kelava, A., Naccarella, D., Leuders, T., & Wirtz, M. (2015). Student's competencies in working with functions in secondary mathematics education - empirical examinations of competence structure model. *International Journal of Science and Mathematics Education, 13*(3), 657-682. doi: https://doi.org/10.1007/s10763-013-9496-7

Nordic Instititute for Studies in Innovation, Research and Education (NIFU) (2017). *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud [ICT-Security Competence in*

Norway - Demand and Supply]. Retrieved from https://nifu.brage.unit.no/nifu-xmlui/handle/11250/2490041

Norman, K. L. (2017). *Cyberpsychology An Introduction to Human-Computer Interaction* (Second ed.). New York: Cambridge University Press.

North Atlantic Treaty Organization (NATO) (2016a). *Cyber Defence Pledge.* Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en

North Atlantic Treaty Organization (NATO) (2016b). *Warsaw Summit Communiqué.* Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

North Atlantic Treaty Organization (NATO) (Draft). *Allied Joint Doctrine for Cyber Operations (AJP 3-20).* Allied Information System (AIS): Allied Command Transformation

Norwegian Police Security Service (2018). *PST innstiller etterforskingen av datainnbruddet i Helse Sør-Øst RHF og Sykehuspartner HF [The Police Security Service close the investigation of the cyber attack against The South-Eastern Norway Regional Health Authority]* [Press release]. Retrieved from https://www.pst.no/alle-artikler/pressemeldinger/pst-innstiller-etterforskningen-av-datainnbruddet-i-helse-sor-ost-rhf-og-sykehuspartner-hf/

Norwegian Ministers (2019). *National Cyber Strategy for Norway.* Norwegian Government Security and Service Organisation Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

NRK (2019, 14th of April 2019). *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre [Norwegian Hydro ICT-executive on the cyberattack:- You think the crisis is big, and then it gets worse].* Retrieved from https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043

Nye, J. (2010). *Cyber Power*. Belfer Center for Science and International Relations. Retrieved from https://www.belfercenter.org/publication/cyber-power

Nye, J. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists, 69*(5), 8-14. doi:https://doi.org/10.1177/0096340213501338

Nye, J. (2014). The regime complex for managing global cyber activities. *Global Commission on Internet Governance Paper Series, 1*. Retrieved from http://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. doi:https://doi.org/10.1016/j.cose.2011.12.010

Poirier, W. J., & Lotspeich, J. (2013). Air Force cyber warfare: now and the future.(Space Focus: Feature). *Air & Space Power Journal, 27*(5), 73. Retrieved from https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-27_Issue-5/F-Poirier_Lotspeich.pdf

Postman, N. (1993). *Technopoly - The Surrender of Cuture to Technology.* New York: Vintage books.

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon, 9*(5), 1-6. doi:https://doi.org/10.1108/10748120110424816

Punch, S. (2002). Research with Children: The Same or Different from Research with Adults? Childhood: *A Global Journal of Child Research, 9*(3), 321-341. doi:https://doi.org/10.1177/0907568202009003005

Rantapelkonen, J., & Salminen, M. (Eds.). (2013). *The fog of cyber defence.* Helsinki: National Defence University.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics, 22*(3), 283-300. doi:https://doi.org/10.1080/13569775.2016.1201316

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security, 49*, 70-94. doi:https://doi.org/10.1016/j.cose.2014.11.007

Røislien, H. E. (2015). When the generation gap collides with military structure: The case of the Norwegian cyber officers. *Journal of Military and Strategic Studies, 16*(3). Retrieved from: https://jmss.org/article/view/58130

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2 ed.). Cambridge: Cambridge University Press.

Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2014). Factors impacting performance in competitive cyber exercises. Paper presented at the *Proceedings of the Interservice/Interagency Training, Simulation and Education Conference*, Orlando FL. Retrieved from: https://www.osti.gov/servlets/purl/1315132

Silverman, D. (2014). *Interpreting qualitative data* (5th ed.). London: SAGE.

Siroli, G. P. (2018). Considerations on the Cyber Domain as the New Worldwide Battlefield. *The International Spectator, 53*(2), 111-123. doi:https://doi.org/10.1080/03932729.2018.1453583

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber education: a multi-level, multi-discipline approach. *Proceedings of the 16th Annual Conference on Information Technology Education,* 109-114. doi:https://doi.org/10.1145/2656450.2656478

Ståhl, T. (2017). How ICT savvy are Digital Natives actually? *Nordic Journal of Digital Literacy, 12*(03), 89-108. doi:https://doi.org/10.18261/issn.1891-943x-2017-03-04

Stevens-Adams, S., Carbajal, A., Silva, A., Nauer, K., Anderson, B., Reed, T., & Forsythe, C. (2013). Enhanced training for cyber situational awareness. In S. D.D. & F. C.M. (Eds.), *Foundations of Augmented Cognition. AC 2013. Lecture Notes in Computer Science* (Vol. 8027, pp. 90-99). doi:https://doi.org/10.1007/978-3-642-39454-6_10

Tadda, G. P., & Salerno, J. S. (2010). Overview of cyber situation awareness. In J. S., L. P., S. V., & W. C. (Eds.), Cyber Situational Awareness. *Advances in Information Security* (Vol. 46, pp. 15-35). doi:https://doi.org/10.1007/978-1-4419-0140-8_2

Tan, M. (2016). The multi-domain battle. Defense News Weekly. Retrieved from http://www.defensenews.com/articles/the-multi-domain-battle

Tapscott, D. (2014). *The digital economy: Rethinking Promise and Peril in the Age of Networked Intelligence* (Vol. 2). McGraw-Hill New York.

The Ministry of Defence (2014). *FDs Cyberretningslinjer [Cybersecurity Guidelines].* regjeringen.no: The Ministry of Defence Retrieved from https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

The Norwegian Intelligence Service (2018). *Focus.* Retrieved from https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_engelsk_Enkeltsider_Godkjent_med.pdf

The Norwegian Intelligence Service (2019). *Focus.* Retrieved from https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf

The Norwegian National Security Authority (2019). *Risko [Risk].* nsm.stat.no Retrieved from https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

The Norwegian Police Security Service (2019). *Threat Assessment.* Retrieved from https://www.pst.no/globalassets/artikler/trusselvurderinger/annual-threat-assesment-2019-single-pages.pdf

Tikk-Ringas, E., Kerttunen, M., & Christopher, S. (2014). Cyber Security as a Field of Military Education and Study. *Joint Force Quarterly, 75*. Retrieved from http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577562/jfq-75-cyber-security-as-a-field-of-military-education-and-study/

Trent, L. T. C. S., Hoffman, R., Leota, T., Frost, C. P. T. R., & Gonzalez, M. A. J. D. (2016). Cyberspace Operations and the People Who Perform Them. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60*(1), 216-217. doi:https://doi.org/10.1177/1541931213601048

UK Ministry of Defence (2015). *Future Trends Programme - Future Operating Environment 2035.* United Kingdom Retrieved from https://www.gov.uk/government/publications/future-operating-environment-2035

US Army (2010). *Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe,VA: US Army Retrieved from https://www.tradoc.army.mil

Veksler, V., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology, 9*(691). doi:https://doi.org/10.3389/fpsyg.2018.00691

Wang, P. L. (1990). Assessment of Cognitive Competency. *The Neuropsychology of Everyday Life: Assessment and Basic Competencies,* 219-228. doi:https://doi.org/10.1007/978-1-4613-1503-2_9

Ward, P., Hoffman, R. R., Conway, G. E., Schraagen, J. M., Peebles, D., Hutton, R. J. B., & Petushek, E. J. (2017). Editorial: Macrocognition: The Science and Engineering of Sociotechnical Work Systems. *Frontiers in Psychology, 8*(515). doi:https://doi.org/10.3389/fpsyg.2017.00515

Waterhouse, T. A. (2013). *Hindre for digital verdiskapning [Challenges to Digital Prosperity] (NOU 2013:2).* Retrieved from https://www.regjeringen.no/contentassets/e2f0d5676e144305967f21011b715c16/no/pdfs/nou201320130002000dddpdfs.pdf

Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace Operations. *Joint Force Quarterly, 73*(2nd quarter). Retrieved from https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-73/Article/577499/the-joint-force-commanders-guide-to-cyberspace-operations/

World Economic Forum (2016). *The Global Information Technology Report 2016.* Retrieved from http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf

Yamada-Rice, D. (2017). Using visual and digital research methods with young people. In P. Christensen & A. James (Eds.), *Research With Children - Perspectives and Practices* (Third ed.). New York: Routledge.

Zimmerman, B. J., & Labuhn, A. S. (2012). Self-regulation of learning: Process approaches to personal development. In K. R. Harris, S. Graham, T. Urdan, C. B. McCormick, G. M. Sinatra, & J. Sweller (Eds.), *APA educational psychology handbook, Vol 1: Theories, constructs, and critical issues.* (Vol. 1, pp. 399-425). doi:http://dx.doi.org/10.1037/13273-014

1

Article 1: **Jøsok, Ø.**, Knox, B. J., Helkala, K., Lugo, R., Sutterlin, S., & Ward, P. (2016). *Exploring the Hybrid Space Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations*. In S. D. & F. C. (Eds.), Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience Lecture Notes in Computer Science (Vol. 9744, pp. 178-188): Springer, Cham. doi:https://doi.org/10.1007/978-3-319-39952-2_18

Exploring the Hybrid Space

Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations

Øyvind Jøsok[1](✉), Benjamin J. Knox[1], Kirsi Helkala[1], Ricardo G. Lugo[2], Stefan Sütterlin[2], and Paul Ward[3]

[1] Norwegian Defence, Cyber Academy, Lillehammer, Norway
ojosok@cyfor.mil.no, {f-bknox,khelkala}@mil.no
[2] Department of Psychology, Lillehammer University College, Lillehammer, Norway
{Ricardo.Lugo,Stefan.Sutterlin}@hil.no
[3] The Applied Cognition & Cognitive Engineering (AC2E) Research Group, University of Huddersfield, Manchester, UK
P.Ward@hud.ac.uk

Abstract. Operations in cyberspace are enabled by a digitized battlefield. The ability to control operations in cyberspace has become a central goal for defence forces. As a result, terms like cyber power, cyberspace operations and cyber deterrence have begun to emerge in military literature in an effort to describe and highlight the importance of related activities. Future military personnel, in all branches, will encounter the raised complexity of joint military operations with cyber as the key enabler. The constant change and complexity raises the demands for the structure and content of education and training. This interdisciplinary contribution discusses the need for a better understanding of the relationships between cyberspace and the physical domain, the cognitive challenges this represents, and proposes a theoretical framework - the Hybrid Space - allowing for the application of psychological concepts in assessment, training and action.

Keywords: Cyberspace · Physical domain · Cyber-physical system · Cyber security · Socio-technical system · Hybrid space · Human factors

1 Introduction

"The future commander needs to be as focused on cyber as on other environmental factors" [1]. This statement summarizes the current dilemma of contradictory task profiles and cognitive demands for military personnel, which result in challenges that present themselves across the social, physical and cyber domains. The complexity of cognitive work associated with human-technological interaction with multiple interdependent, interconnected and networked environments is compounded [2], as these human and technological agents consequently bring their own assets and goals (e.g., informational, social, physical, cyber [3–5]) into the operating and decision making space. Moreover, activity in this space is further complicated or complexified as each agent needs to secure their own assets, in order to maintain freedom of movement [17].

D.D. Schmorrow and C.M. Fidopiastis (Eds.): AC 2016, Part II, LNAI 9744, pp. 178–188, 2016.
DOI: 10.1007/978-3-319-39952-2_18

Examining asset protection from a security perspective is important to ensure security is not compromised, all assets need to be protected from current and future threats, both internal and external to the system. Simultaneously, vulnerabilities inherent within the entire socio-technical system (STS) have to be managed [5]. According to Whitman and Mattord [3] an asset is a protected organizational resource. Therefore, prioritizing these resources is achieved by weighting assets based on values ranging from: criticality, profitability, replacement or protection expenses, and embarrassment or loss of liability factor if the asset is revealed [3]. Assets and their vulnerabilities are interconnected. If an asset is lost, this loss has an effect on other assets and their vulnerabilities.

Expanded digitization and global network coverage [6] will connect people and physical infrastructure to cyberspace and to other physical entities via cyberspace. In turn, this will reveal novel and unforeseen connected vulnerabilities that requires human cognition to self-regulate and transform[1]. Several authors have identified a lack of understanding regarding how the connectivity of agents has negative consequences for decision making and action, especially relating to third party infrastructure [8]. We argue that today's decision makers have to acknowledge and understand how to prioritize multiple assets based on known and unknown vulnerabilities and risks. Achieving this level of understanding within a contradictory and hybrid landscape requires cognitive flexibility to control the multiple situational dynamics that can occur simultaneously between assets in the physical domain, the social domain and cyberspace.

In a military context, these hybrid conditions create challenges for efficient decision making as final responsibility lies with ranking officers whose past experience and current practice, including key command and control activities such as sensemaking and decision making, are rooted in and influenced by factors in the physical domain [7, 8]. Despite their affinity for the physical over cyber media, increasingly, officer understanding and decision making is being guided by information perceived, interpreted, evaluated and communicated to them by lower ranking, and often younger, officers who operate comfortably in this domain [10]. Agents equipped with the necessary capabilities to translate phenomena originating in cyberspace into the physical domain can potentially provide the crucial knowledge bridge required to influence far reaching military and political decision making.

The conjunction of age, rank and experience reveals a didactic shift in command responsibility and decision making. This can be addressed through better understanding of competencies or better definitions of competencies. The arrival of 'cyber' has revealed evidence that suggests more understanding of skill-sets and agile leadership [12] can contribute to defining human competencies as requisites for performance in contemporary military operations.

Huge investments have been made to develop and implement state-of-the-art technologies across sectors to improve human efficiency. Digitization has increased

[1] Kegan and Lahey [2] define the self-transforming mind as: "able to step back and reflect on the limits of our own ideology or personal authority; see that any one system or self-organization is in some way partial or incomplete; be friendlier toward contradiction and opposites; seek to hold on to multiple systems rather than projecting all but one onto the other" [2, p. 17].

information flow and interdependability of technological systems [13]. Efforts to leverage human performance have been answered by new technologies [15], yet the results seem only to increase cognitive demand [14, 16]. The cognitive workload placed on humans in this context exceed those in most common contexts [14]. Making the right decisions in Computer Network Operations (CNO) has added value given the potential for unknown or unintended consequences [17].

Several authors argued that there is a current lack of understanding of the human factors necessary to operate effectively, safely and securely in this complex space [9, 11, 18, 19]. This is revealed through the inability to adequately integrate CNO into contemporary military operations [17, 20], a pressing need for cyber related study materials at all command levels [8, 21], and insufficient career structures for cyber personnel [22]. The Hybrid Space approach acknowledges these factors as points of departure for continuing research that integrates situational dynamics in cyberspace and the physical domain, with individual cognitive skill-sets, psychological determinants of action and communicative aspects, within a merging socio-technical and cyber-physical system.

2 The Hybrid Space Framework

The Hybrid Space (Fig. 1) frames the interconnection between cyberspace and the physical domain, whilst simultaneously demonstrating the tension between tactical and strategic goals in decision making and action (compression of command-levels) in a future operating environment context. Individual domain specific competencies, experience and rank determine performance levels and behaviours in a organisational and institutional landscape that necessitate the integration, or at least complementary juxtaposition, of cyber and physical domains (henceforth, hybrid). Understanding the processes and actions required to enhance and accelerate these capabilities may hold the key to releasing the tension between command levels when attempting to project military power.

This framework acknowledges the Cyber-Physical System (CPS) and the effects of automation through cyber-based technological operations on the physical world. CPS research has been predominantly focused on the left side (Fig. 2a) of the horizontal axis and has been defined as "…the close interaction of computing systems and physical objects…" [24, p. 3]. With some exceptions (e.g., [37]), research in the area of STS - defined as; "…taking both social factors and technological factors into consideration" [25, p. 720] - resides primarily on the right of our horizontal axis (Fig. 2b). Going forward, we view the field of STS research exploring how people will cope and perform in a digitizing society.

In a pre-cyber landscape, the vertical axis has divided doctrine into three levels; tactical, operational and strategic [23]. The intent of the vertical axis in the Hybrid Space framework is to transfer conventional knowledge of military command levels and situate this doctrine into a present day context. This novel approach is representative of today's digitized context; where cyber pervades all aspects of military planning and leadership [23]. Cyber is shaping how traditional command levels are responding. It has resulted in the compression of command levels [10] as a means of adaptation for coping and

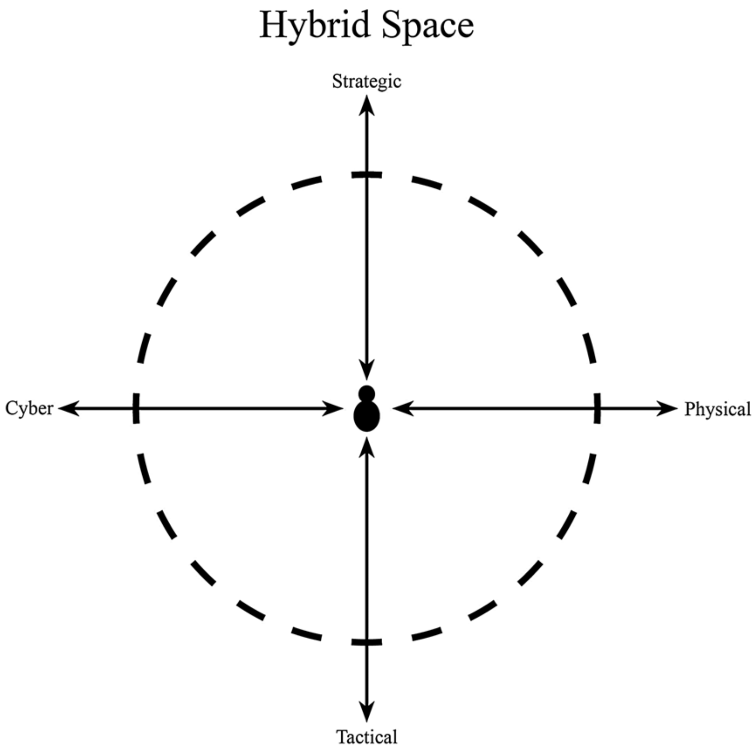


Fig. 1. The hybrid space framework

performance. In turn, bisecting the vertical axis with the horizontal axis reveals a convergence of complexity. The purpose of the Hybrid Space is to open the space for exploration in competencies, human behavior and cognitive processes [19] that occur, or need to occur, in and around this point of convergence.

Viewing this complex terrain through the lense of the Hybrid Space - where human and macrocognitive factors play a significant role [19] - can serve to bridge the expertise gap between cyberspace and the physical domain. Cyberspace operations merge in-depth tactical knowledge with strategic appreciation, which can create tension at different command levels as it challenges traditional military doctrine, education models and cultures [8, 16]. Inconsistencies in tactical and strategic operations across organizations result in difficulties in collaborative sensemaking with respect to core aspects of defining cyber and, as such, present significant barriers for CPS and STS interoperability [8]. Establishing clarity in this Hybrid Space is needed, not only to ensure effective intra and inter-organisational communication, cooperation and coordination, but to ensure national and international asset security.

2.1 Horizontal Axis

As indicated, the horizontal axis shown in Fig. 2 of the Hybrid Space framework acknowledges earlier research in CPS and STS. CPS research acknowledges the

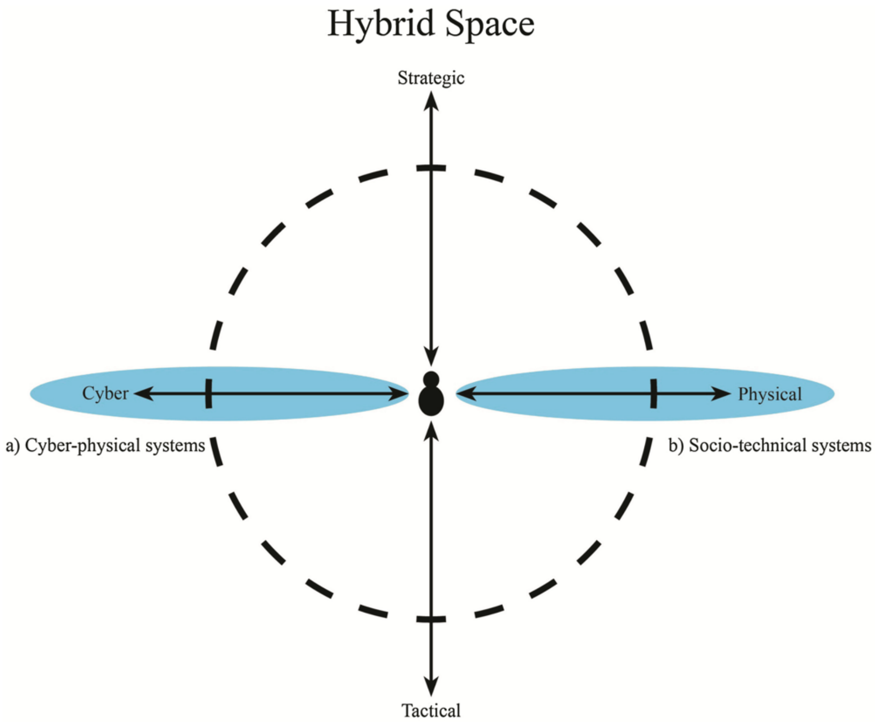


Fig. 2. The hybrid space framework in relation to CPS: "…the close interaction of computing systems and physical objects…" [24, p. 3] and STS: "…taking both social factors and technological factors into consideration" [25, p. 720].

integration of the cyber domain with the physical world [26, 27], but current frameworks describing CPS and cyber attack categorization are mostly technology-centric and tend to neglect the human factor [9, 19]. On the other hand, STS situates a human in the center and is composed of social, management and technical subsystems [28], but in most research conducted to date, STS has not fully embraced the role of cyberspace, as the technical subsystem only provides the necessary functions to meet the roles of the human [28]. We argue that including all environmental factors solely in an additive manner does not satisfy the level of complexity facing individuals and teams operating within these overlapping fields.

In the Hybrid Space framework, we extend the notion of STS to include cyber operations as well as the coordinating operations that result from its integration. As a result, the cognitive work in which humans engage, and the systems themselves, are increasingly complex [14]. Work is highly interactive and comprised of humans, agents and artifacts. Information may be novel, deceptive, and/or limited, and is typically distributed across space and time; Tactical goals (i.e., how to deal with a specific new threat) are frequently ill-defined, and there is often a need for conflict resolution between strategic goals (e.g., protect against a known state threat actor) and lower-order goals that are both dynamic and emergent. Much of this requires significant preparation, planning and replanning, as well as a considerable degree of domain-specific skill (such as situation assessment, sensemaking, and decision making skills within STS and CPS). A key feature is the requirement for proficiency at handling novelty, so that humans can adapt on the fly to changing demands. To complicate matters further, the stakes are almost always high, and uncertainty, time-constraints and stress are seldom absent. Moreover, tactics and strategy that dictate how work should unfold are typically constrained by broader professional, organizational, and institutional practice and policy [29]. The macrocognitive demand characteristics placed on young personnel when operating in the Hybrid Space exceeds those in most common contexts. Making the right decisions in the Hybrid Space has added value given the potential for unknown or unintended consequences [30].

The horizontal axis in the Hybrid Space model acknowledges the simultaneous presence and incongruent needs of cyberspace and the physical domain. Attacks in cyberspace do not differ from conventional attacks insofar as they generate effects beyond the intended domain of interest [9, 17]. However, they do differ in the way that consequences might be unintended or hidden, revealed in unconventional timeframes or affect third party interests. This incongruency necessitates a range of skill sets including highly developed technical skills (e.g., coding, programming, analysis, etc.), considerable macrocognitive skills (perception, interpretation, evaluation) and effective interpersonal and psychological skills (perspective taking, communicative skills, for instance to convey mission impact information to a commander). This axis highlights the need for a new category of personnel with a wide variety of social and technical expertise [1, 8, 11, 17, 20].

2.2 Vertical Axis

The vertical trajectory of the Hybrid Space framework visualizes the compression of command levels whilst simultaneously recognizing the institutional need to maintain such structures. The compression of command levels has been widely recognized in contemporary military doctrines and goes by the acronym of the Strategic Corporal [10]. Tactical decisions made by military personnel must take into account the strategic realities that used to be purview of the higher levels in the chain of command [10], as the distinction between tactical and strategic impact is becoming increasingly blurry [10]. In a CNO context, these decisions and actions performed by an operator, can have geopolitical consequences.

Lemay and colleagues [10] give a variety of plausible situations where a cyber operator is forced to decide and act on Advanced Persistent Threat (APT) incidents that may affect the strategic scope of the organization. Cyber operations are marked by unconventional timeframes (ranging from years to seconds in a both a future and historical timeline) that result in cognitive complexity and pressure when attempting to avoid negative consequences. Thus, a high level commander can easily miss out on decisions affecting the strategic goal due to his/her relatively distant placement on the Hybrid Space's horizontal axis. Consequently, strategic sensemaking and decision-making can suffer. When this is combined with concerns relating to adversary intent and attribution [10] young personnel need to understand the strategic picture in order to communicate events and respond accurately to uncertainty. This requires a model of leadership that is mature, agile and appropriate to context [8]. Lamay et al. [10] conclude that in this new context, the strict division between tactical and strategic personnel cannot hold as it potentially constrains and prevents leadership of cyber operators. They elaborate that it is unlikely that a manager with an IT background will keep up with technology development, and technical personnel spending all their time updating themselves, might lose track of the bigger picture. Having one supervisor for every cyber operator is not an answer, and given the time constraint and time available to make decisions [10] it narrows down the possible pathways ahead. As Lemay et al. [10] argue; enhanced training, understanding the commander's intent and decentralized decision making have been brought forward as possible solutions. However, this process will require instruction and training methods followed by evaluation to determine whether or not decentralized decision-making generally works.

So for now, incident handlers are strategic agents, often without being aware of it [10], and often without their operational and strategic levels of command being aware of it. If the current gap of technological skills and knowledge between managers/commanders and technical personnel [10] is viewed upon in the Hybrid Space framework, the implications for leadership training that can leverage mastery of the 'understand function' [1] through cognitive-technical and cognitive-psychological competencies becomes evident.

To the best of our knowledge, the Hybrid Space conceptualization is the first to fully acknowledge that investing in new technologies - to leverage human performance [31, 32] - has not accounted for what people view as important and given them strategies for organizing that information. The Hybrid Space acknowledges specific features that appear through a shift in contemporary military leadership. As knowledge agents (human and technical) are required to 'lead' commanders and senior military planners who experience heightened anxiety as their perceived self-efficacy and control beliefs are threatened due to the ambiguity and asynchronous nature of the digital battlefield [8].

The Hybrid Space framework simultaneously stresses how human agents are required to move between tactical and strategic considerations to master the understand function [1] and operate effectively within the complexity of merging CPS and STS landscapes. The Hybrid Space explains a novel state of being and opens up space for critical research that can guide practices capable of facilitating the necessary learning pathways for human performance in digitization.

3 Metacognition and Navigation Within the Hybrid Space

As command levels compress and systems converge, operating within the Hybrid Space requires agents take conscious control of assets and responsibility for improving their cognitive flexibility to move freely. This cognitive process builds on the Generation Y learning paradigm of perception, emotional involvement, intuitive and experience based practice [11, 33]; whilst also complimenting current pedagogical trends where learners are encouraged to develop their cognitive and metacognitive skills, as pathways to better performance and self-insight [35]. For military personnel, this learning process facilitates mastery of the future operating environment whilst also implying the need for systematic and autonomous application of adaptive reflection [36] to build self-regulatory processes and self-efficacy. Agents who are capable of mirroring the dynamism [34] of the complex developing Hybrid Space landscape, will demonstrate leadership qualities founded upon the power of knowledge-based abstractions, rather than being constrained by institutional norms of military command experience or rank. This cyber leadership 'art' chances that current military norms and solutions relating to command, control and understanding of leadership models, only present barriers and limit expectations [8].

Human factors focuses on the "fit" between the user, system, and the situational demands in a hybrid space between cyber and physical domain. The Hybrid Space model defines military personnel as located at the interface between CPS and STS and that both systems incorporate the human "in the loop". Events in the cyberspace, as perceived by the human agent, have not only direct effects on decisions made in the physical domain, but also influence human decision-making via indirect psychological effects. In a similar vein, circumstances in the physical domain can affect the interaction with and thus events within the cyberspace. Reacting adequately to constantly changing environmental needs requires efficient navigation within the Hybrid Space, i.e., between cyber- and physical domain (horizontal axis) as well as monitoring one's relationship towards current tactical and strategic goals and demands (vertical axis).

Metacognition refers to 'thinking about thinking' and includes the components knowledge of one's abilities, situational awareness, and behavioral regulation strategies [38]. Individuals with high metacognitive skills have more accurate and confident judgment of their own performance in relation to the demands and are better able to accurately describe their strengths, weaknesses, and their potential to improve. Thus, high metacognitive awareness of one's cognitive processes (planning, monitoring, evaluations) facilitates one's localisation within the Hybrid Space, a judgment on its appropriateness and initiation of change of cognition or action. As an example, individuals who recognize emotional impacts of events in one of the domains (e.g., a failure or sub-optimal performance in cyber) affecting their performance in the physical domain (e.g., distraction leading to impaired concentration and reduced physical or cognitive performance), can counter-regulate and apply emotion-regulation strategies.

An individual with a particular accurate judgment of his/her own performance level (high metacognitive awareness) will recognise a potential threat in cyberspace exceeding his/her technical abilities and consider to activate additional personal or technical resources in the physical domain. A person being aware that the outcomes of previous actions were taken under immense time pressure to serve short-term goals served primarily tactical purposes can readjust short-term goals earlier to put strategic goals back into the focus. The ability to be metacognitively aware of one's own performance without underestimation of own capacities or inappropriate over-confidence is considered a relatively stable personality trait that can be quantified and made subject to training and improvement. A crucial role for improvement of metacognitive skills is played by leaders, trainers, and all persons designing training and giving feedback.

As an example for the application of cognitive science in the Hybrid Space model serves the Recognition/Metacognition model [39] for tactical decision-making that involves the ability to recognize situations and supplement with processes of verification and optimal solution resolvement that is relevant to the Hybrid Space. The R/M approach identifies and outlines factors that can be trained to help deal with novel situations that may arise (see [39] for in-depth description). At the meta-recognition stage, agents will need to become aware of evidence-conclusion relationships, critically analyse the arguments that support a conclusion, correct any beliefs through external (collecting more data) and internal (attention shifting or regulating the recognitional process) actions, and quick testing the critical-analysis/correctional process. The meta-recognition component of the model provides information on the metacognitive factors so that it can monitor and evaluate the recognitional process to modify behavior efficiently. This process is dependent on expertise understanding of the Hybrid Space as well as an understanding of the physical demands and psychosocial processes needed (metacognitive skills) to function in it.

4 Future Research

Several authors suggest that cyber officers need a varied skill-set [10, 11]. We agree with these finding and see the Hybrid Space as a tool capable of framing the complex environment that both defines and reveals this skill-set. This is a framework that reflects the novel demands of the future operating environment.

The integration of cyber power into joint warfare presents a research gap that concerns more than just understanding CNO from a technological or human factors view. It requires us to understand the significance of these factors through their interdependency and the reciprocal processes that occur for functioning effectively in the Hybrid Space. At all operational levels agents can affect and are affected by abstraction levels of team and individual performance. Thus, by learning how to support performance in the Hybrid Space we hope to develop efficacy through multiple performance pathways. Research that embraces and leverages cross discipline collaboration is required to establish a pedagogic methodology concerning how to educate, train and accelerate the requisite skills that will enable responsible personnel to operate with superior cognition in the Hybrid Space.

This framework has the potential to reveal the cognitive and metacognitive processes required to conduct future military operations. By categorizing the relevant agents, prioritizing the critical assets and finding novel approaches to measuring adaptation can lead us to better understand the competencies, relationships and processes that occur in the Hybrid Space.

References

1. Ministry of Defence, United Kingdom: Future Trends Programme - Future Operating Environment 2035, 1st edn. First Published 14 December 2015. https://www.gov.uk/government/publications/future-operating-environment-2035
2. Kegan, R., Lahey, L.: Immunity to Change. Harvard Business School Publishing Corporation, Boston (2009)
3. Whitman, M., Mattord, H.: Principles of Information Security, 4th edn. Cengage Learning, Boston (2012)

4. NERC, Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets (2015) http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf
5. von Solms, R., van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
6. Andrews, J., Buzzi, S., Choi, W., Hanly, S.V., Lozano, A., Soong, A.C.K., Zhang, C.J.: What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 23–44 (2014)
7. Trujillo, C.: The Limits of Cyberspace Deterrence. JFQ 74, 3rd Quarter 2014 (2014)
8. Tikk-Ringas, E., Kerttunen, M., Spirito, C.: Cyber Security as a Field of Military Education and Study. JFQ 74, 3rd Quarter 2014 (2014)
9. Mancuso, V.F., Strang, A.J., Funke, G.J., Finomore, V.S.: Human factors of cyber attacks: a framework for human-centered research. In: Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting – 2014, pp. 437–441 (2014)
10. Lamay, A., Leblanc, S., De Jesus, T.: Lessons form the strategic corporal - implications of cyber incident response. In: SIGMIS-CPR 2015, 4–6 June 2015. ACM, Newport Beach (2015). ISBN 978-1-4503-3557-7/15/06
11. Røyslien, H.: When the generation gap collides with military structure: the case of norwegian cyber officers. J. Mil. Strateg. Stud. **16**(3), 1065–1082 (2015)
12. Joiner, B., Josephs, S.: Leadership Agility, Five Levels of Mastery for Anticipating and Initiating Change. Wiley, San Francisco (2007)
13. Zanenga, P: Knowledge eyes, nature and emergence in society, culture, and economy. IEEE (2014). 978-1-4799-4735-5/14
14. Paterson, D.M.: Work domain analysis for network management revisited: infrastructure, teams and situation awareness. In: IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). IEEE (2014). 978-1-4799-3564-2/14
15. Sawilla, R.E., Wiemer, D.J.: Automated computer network defence technology demonstration project (ARMOUR TDP). IEEE (2011). 978-1-4577-1376-7/11
16. Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., Garneau, C.: ARSCA: a computer tool for tracing the cognitive processes of cyber-attack analysis. In: IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA) (2015). 978-1-4799-8015-4/15
17. Williams, B.T.: The joint force commander's guide to cyberspace operations. JFQ 73, 2nd Quarter 2014. Major General Brett T. Williams, USAF, is the Director of Operations, J3, for U.S. Cyber Command (2014)
18. Proctor, R.W. Chen, J.: The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. Hum. Factors J. Hum. Factors Ergon. Soc. **57**(5), 721–727 (2015)
19. Gutzwiller, R.S., Fugate, S., Sawyer, B.D., Hancock, P.A.: The Human Factors of Cyber Network Defense. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. vol. 59, no. 1, pp. 322–326. SAGE Publications, September 2015
20. Bonner, L.E.: Cyber Power in 21st Joint Warfare. JFQ 74, 3rd Quarter 2014. Lieutenant Colonel E. Lincoln Bonner III, USAF, is Director of Operations at the Space Operations Squadron Aerospace Data Facility–Colorado (2014)
21. NATO MC 0616: NATO Cyber Defence Education and Training Plan. 6th Draft MC 0616. NATO UNCLASSIFIED (2015)
22. Arnold, T., et al.: Towards A Career Path in Cyberspace Operations for Army Officers. J. Art. Aug. **18**(10), 37am (2014)
23. Dombrowski, P., Demchak, C.C.: Cyber war, cybered conflict, and the maritime domain. Naval War Coll. Rev. **67**(2), 70 (2014)

24. Hu, F.: Cyber-Physical Systems: Integrated Computing and Engineering Design. CRC Press, Boca Raton (2013)
25. Coghlan, D., Brydon-Miller, M. (eds.): The SAGE Encyclopedia of Action Research. Sage, London (2014)
26. Ahmed, S.H., Kim, G., Kim, D.: Cyber physical system: architecture, applications and research challenges. In: Wireless Days, 2013 IFIP. IEEE (2013). doi:10.1109/WD.2013.6686528
27. Sanislav, T., Miclea, L.: Cyber-physical systems – concepts challenges and research areas. CEAI **14**(2), 28–33 (2012)
28. Troxler, P., Lauche, K.: Assessing Creating and Sustaining Knowledge Culture in Organisations (2014). http://www.academia.edu/1964062/Assessing_Creating_and_Sustaining_Knowledge_Culture_in_Organisations
29. Hoffman, R.R., Ward, P., Feltovich, P.J., DiBello, L., Fiore, S.M., Andrews, D.: Accelerated Expertise: Training for High Proficiency in a Complex World. Psychology Press, New York (2014). http://www.psypress.com/books/details/9781848726529
30. Farwell, J., Rohozinski, R.: The new reality of cyber war. Survival (00396338) **54**(4), 107–120 (2012). Academic Search Complete, EBSCOhost
31. Oltromani, A., Noam, B.-A., Cranor, L., Bauer, L., Christin, N.: General requirements of a hybrid-modeling framework for cyber security. In: Military Communications Conference (MILCOM). IEEE (2014)
32. Bennet, K.B.: Ecological interface design: military C2 and computer network defence. In: IEEE 2014 International Conference on Systems, Man, and Cybernetics, 5–8 October 2014, San Diego, CA, USA (2014)
33. Sookermany, AMcD: What is a skillful soldier? An epistemological foundation for understanding military skill acquisition in (post) modernized armed forces. Armed Forces Soc. **38**(4), 582–603 (2012)
34. Castells, M.: Information Technology, Globalization and Social Development. UNRISD Discussion Paper no. 114, Geneva, UNRI (1999)
35. Baas, D., Castelijns, J., Vermeulen, M., Martens, R., Segers, M.: The relation between assessment for learning and elementary students' cognitive and metacognitive strategy use. Br. J. Educ. Psychol. **85**(1), 33–46 (2015)
36. Hannah, S.T., Avolio, B.J.: Ready or not: how do we accelerate the developmental readiness of leaders? J. Organ. Behav. **31**(8), 1181–1187 (2010)
37. Woods, D.D., Hollnagel, E.: Joint Cognitive System: Patterns in Cognitive Systems Engineering. CRC Press, Boca Raton (2006)
38. Jacobs, J.E., Paris, S.G.: Children's metacognition about reading: Issues in definition, measurement, and instruction. Educ. Psychol. **22**, 255–278 (1978)
39. Cohen, M.S., Freeman, J.T., Thompson, B.: Critical thinking skills in tactical decision making: a model and a training strategy. In: Making Decisions Under Stress: Implications for Individual and Team Training, pp. 155–190 (1998)

2

Article 2: Knox, B. J., **Jøsok, Ø.**, Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R. G., & Sütterlin, S. (2018). *Socio-technical communication: The Hybrid Space and the OLB-Model for science-based cyber education.* Military Psychology 30(4), 350-359. doi: 10.1080/08995605.2018.1478546.

(This article has been removed from the digital thesis due to lack of permission from the publisher. It can be read in the journal named above or in the printed thesis)

3

Article 3: **Jøsok, Ø.**, Knox, B. J., Wilson, K., Helkala, K., Lugo, R. G., Sutterlin, S., & Ødegaard, T. (2017). *Macrocognition applied to The Hybrid Space: Team environment, functions and processes in cyber operations*. In S. D. & F. C. (Eds.), Augmented Cognition. Enhancing Cognition and Behavior in Complex Human Environments Lecture Notes in Computer Science (Vol. 10285, pp. 486-500): Springer, Cham. doi:https://doi.org/10.1007/978-3-319-58625-0_35

(This article has been removed from the digital thesis due to lack of permission from the publisher. It can be read in the book named above or in the printed thesis)

4

Article 4: **Jøsok, Ø.**, Hedberg, M., Knox, B. J., Helkala, K., Sütterlin, S., & Lugo, R. G. (2018). *Development and Application of the Hybrid Space App for Measuring Cognitive Focus in Hybrid Contexts.* In D. D. Schmorrow & C. M. Fidopiastis (Eds.), Augmented Cognition: Intelligent Technologies Lecture Notes in Computer Science (Vol. 10915, pp. 369-382). Cham: Springer. doi:https://doi.org/10.1007/978-3-319-91470-1_30

(This chapter has been removed from the digital thesis due to lack of permission from the publisher. It can be read in the book named above or in the printed thesis)

5

Article 5: **Jøsok, Ø.**, Lugo, R. G., Knox, B. J., Sütterlin, S., Helkala, K. (2019) *Self-regulation and cognitive agility in cyber operations.* Frontiers in Psychology 10(875). doi:10.3389/fpsyg.2019.00875.

frontiers in Psychology

ORIGINAL RESEARCH
published: 24 April 2019
doi: 10.3389/fpsyg.2019.00875

Self-Regulation and Cognitive Agility in Cyber Operations

Øyvind Jøsok[1,2*], *Ricardo Lugo*[3], *Benjamin James Knox*[1,4], *Stefan Sütterlin*[5,6] *and Kirsi Helkala*[1]

[1] Norwegian Defence Cyber Academy, Lillehammer, Norway, [2] Faculty of Social and Health Sciences, Inland University of Applied Sciences, Lillehammer, Norway, [3] Inland School of Business and Social Sciences, Inland University of Applied Sciences, Lillehammer, Norway, [4] Department of Information Security and Communications Technology, Norwegian University of Science and Technology, Trondheim, Norway, [5] Faculty for Health and Welfare Sciences, Østfold University College, Halden, Norway, [6] Division of Clinical Neuroscience, Oslo University Hospital, Oslo, Norway

Reliance upon data networks to conduct military operations presents new challenges to the competence profiles of military personnel. Specifically the increased demand for the new category of military cyber personnel is a direct consequence of the utility of the cyber domain in contemporary military operations, both to support leadership processes and as a domain of operations on its own. The conflation of the cyber and physical domains empowers cyber operators to influence events beyond their immediate physical environment. Proper education and training of such personnel requires new insight into the competencies that are beyond cyber specific technical skills, to govern the complexity of operating in a cyber-physical hybrid environment. This pilot research contributes to the debate on military cyber personnel competencies by investigating how cyber defense operator's level of self-regulation can contribute to their performance in operations. We hypothesize that higher levels of self-regulation predicts higher levels of cognitive agility as measured by cognitive movement in The Hybrid Space conceptual framework. Displays of cognitive agility within The Hybrid Space have previously been linked to performance in defensive cyber operations. A positive association was therefore expected between levels of self-regulation and displays of cognitive agility. $N = 23$ cyber cadets from the Norwegian Defence Cyber Academy (NDCA) completed self-regulation questionnaires (SRQs) and self-reported their cognitive location in The Hybrid Space during a 4-day cyber defense exercise. Data showed that higher levels of self-regulation were associated with displays of cognitive agility. According to the regression models in use, self-regulation could explain 43.1% of the total cognitive movements in The Hybrid Space. Understanding factors that contribute to cyber operator performance are needed to improve education and training programs for military cyber personnel. Validating self-regulation as a contributing factor to cognitive agility is important as this can be a pathway to empirically underpin individual cyber operator performance.

Keywords: self-regulation, cyber domain, cyber operations, defense, competence, cognitive agility

Edited by:
Aaron Williamon,
Royal College of Music,
United Kingdom

Reviewed by:
Varun Dutt,
Indian Institute of Technology Mandi,
India
Ion Juvina,
Wright State University, United States

****Correspondence:***
Øyvind Jøsok
ojosok@gmail.com

Specialty section:
This article was submitted to
Cognitive Science,
a section of the journal
Frontiers in Psychology

Received: *26 June 2018*
Accepted: *02 April 2019*
Published: *24 April 2019*

Citation:
Jøsok Ø, Lugo R, Knox BJ,
Sütterlin S and Helkala K (2019)
Self-Regulation and Cognitive Agility
in Cyber Operations.
Front. Psychol. 10:875.
doi: 10.3389/fpsyg.2019.00875

INTRODUCTION

The increased utility of, and reliance upon, the cyber domain in military operations has led to higher demand of technically qualified cyber personnel (Champion et al., 2014). This is demonstrated through investment in cyber defense units, cyber defense education (NATO, 2016a), and the recognition of cyberspace as a domain of operations (NATO, 2016b). However, cyber operator tasks, competence requirements, and performance are unsettled concepts that lack clear definition and guidelines to support selection, education, and training of this new category military personnel. While technical cyber competence is paramount to operate in the cyber domain, the soft skills and cognitive competencies have started to receive more attention. The high cognitive demands of cyber operators have been widely acknowledged (Tapscott, 2014; Røislien, 2015; D'Amico et al., 2016; Buchler et al., 2018); however, the soft skills[1] and cognitive competencies[2] contribution to cyber operator performance is yet to be empirically validated (Forsythe et al., 2013; Lathrop et al., 2016; Helkala et al., 2017; Knox B. et al., 2018).

The Hybrid Space conceptual framework describes the hybrid character of the work environment of a military cyber operator and defines the cognitive space available for agile maneuver (Jøsok et al., 2016). The Hybrid Space framework theorizes that technical skills alone are not enough to perform in an age of network enabled operations (Buchler et al., 2016; Jøsok et al., 2016). The Hybrid Space framework acknowledges that the work environment of military cyber operators is influenced by factors like, e.g., team-work, leadership, hierarchy, communication, etc., but is also influenced by the intangible character of the digital context and information domain – consequently "shifting demands from physical fitness toward cognitive performance" (Knox B.J. et al., 2018, p. 351). It also allows the cyber operator to engage in strategic thinking while performing cyber operator tasks on a tactical level (Jøsok et al., 2016).

Some recent research contributions are addressing the cognitive competencies of cyber operators. Lathrop et al. (2016) propose that cyber operators are reliant on competencies like sensemaking, creative thinking, mental projection, and other high-level cognitive functions to perform. Further, cyber operators' ability to collaborate, organize, and analyze problems has been described as: "... just as important as their technical acumen on the keyboard" (Buchler et al., 2018). However, it is unclear how these competencies relate to cyber operator performance. Knox B.J. et al. (2018) use The Hybrid Space framework to describe that individuals need to use different cognitive competencies to maneuver in The Hybrid Space. Examples include social-cognitive perspective-taking, spatial cognition, cognitive flexibility, macrocognition, metacognition, and self-regulation (Knox B.J. et al., 2018). The Hybrid Space framework has also previously been used to assess cyber operator cognitive agility during a cyber defense exercise. By utilizing the Hybrid Space framework, Knox et al. (2017) proposed cognitive agility as one important cognitive competency that could support cyber operator performance. They defined cognitive agility as "cognitive focus movements" in The Hybrid Space and later they associate displays of cognitive agility in The Hybrid Space with metacognition and performance of cyber operators (Knox et al., 2017). Metacognition is defined as "cognition of cognition" and is usually conceived as "an individual and conscious process that serves the regulation of cognition" (Efklides, 2008, p. 277). Self-regulation, a related concept, is defined as the regulation of cognition, emotions, behavior, and environment and includes metacognition in the process (Efklides, 2008). Self-regulation is a well-researched concept that has been shown to contribute to performance in other domains such as sport (Toering et al., 2009) and academic achievement (Zimmerman, 1990), but is yet to be researched in the military cyber operator context. In this article, we contribute to cyber operator competence profiles by investigating if cyber operators' self-regulation is associated with performance in cyber operations. The authors hypothesize that higher levels of self-regulation predict cognitive agility as measured by cognitive movement in The Hybrid Space conceptual framework.

CYBER OPERATOR COGNITIVE DEMANDS AND PERFORMANCE

The tasks in which cyber operators engage have been described as varied, often non-routine, and involve perception and comprehending large amounts of information (Erbacher et al., 2010). Cyber operator tasks include both human and technical aspects and: "...is heavily reliant upon the decision-making capabilities and skill-sets of defenders to overcome attackers" (Buchler et al., 2018). Ben-Asher and Gonzalez (2015) propose that cyber operators need updated theoretical knowledge, practical experience and training in how to: "...quickly learn and adapt to novel and dynamic environments" (p. 60). In addition, they address the need for this knowledge to be situated in the current operational environment, as tasks and priorities might vary in relation to operational demands (Ben-Asher and Gonzalez, 2015). In the military context, merging operational demands with the technical aspects of cyber operations results in a need to distinguish cybersecurity from cyber operations (Lathrop et al., 2016). Cybersecurity is concerned with defending own assets; defined as a protected organizational resource (Whitman and Mattord, 2012). In military cyber operations, the focus is: "...*defending* cyber- and cyber-physical systems from known or unknown adversaries and, when authorized, conducting *offensive* cyberspace operations to achieve military objectives" (Lathrop et al., 2016, p 283). Military cyber operators therefore distinguish themselves from civilian cybersecurity operators by using the cyber domain as a utility to create military effects. In addition, they defend and protect own critical assets in order to sustain the ability to deliver military kinetic effects. We argue that cyber operators are not limited to working in the

[1] According to Collins dictionary (2018), soft skills are defined as: "...interpersonal skills such as the ability to communicate well with other people and to work in a team."

[2] Wang (1990) describes cognitive competency as: "a psychological construct that cannot be directly observed but can be inferred from an individual's behaviour or performance on content-relevant tasks" (p. 219).

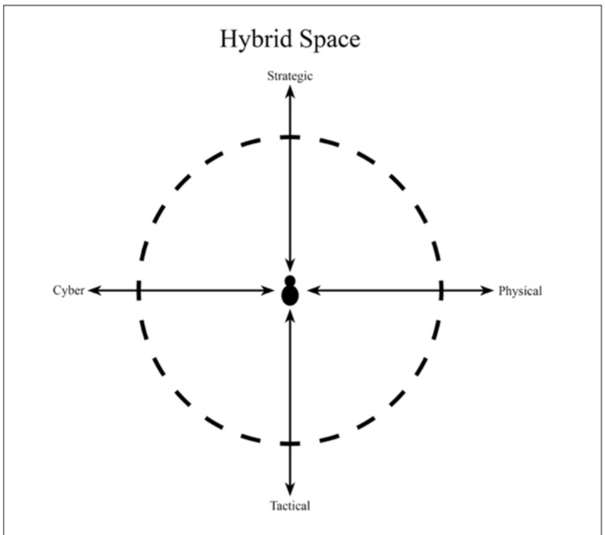


FIGURE 1 | The Hybrid Space conceptual framework (Jøsok et al., 2016).

cyber domain, but work in a hybrid environment where cyber, physical aspects, and cognitive effects are interconnected and intertwined. This argument implies that military cyber operators need to be aware of and understand the sociotechnical system, defined as: "...taking both social factors and technological factors into consideration" (Coghlan and Brydon-Miller, 2014, p.720), they are a part of. These task demands alongside high information load, result in cyber operator work to be described as safety-critical (Buchler et al., 2018; Knox B. et al., 2018), cognitively demanding (D'Amico et al., 2016), and require cognitive agility to traverse and maneuver across cyber-physical and tactical-strategic dimensions in order to make sense of their work environment (Jøsok et al., 2016).

A recent theoretical proposal (see **Figure 1**) describes the cognitive work environment of military cyber operators and defined it as *"The Hybrid Space"* conceptual framework (Jøsok et al., 2016).

The framework represents a cyber operator's range of cognition when conducting cyber operations, taking cyber, cyber-physical, and sociotechnical systems into account. The Hybrid Space framework can be used to measure cyber operator's cognitive agility. Cognitive agility requires exercise of cognitive focus, which can be understood as an aspect of attention that involves bringing selected information into conscious awareness (MacKay-Brandt, 2011). Individual cyber operator cognitive focus, in this research, is represented by a location in The Hybrid Space, e.g., a cyber operator immersed in coding would be cognitively located in the quadrant facing down to the left (see **Figure 1**). During the course of a cyber operation, the operator would report different cognitive focus depending on the task. The operator would also be obliged to move cognitively inside, and in-between quadrants depending on the operational requirements. For example, the task of contributing to joint operational planning would require the cyber operator to move to the operational level and traverse into physical domain considerations.

Cognitive agility is defined as a construct made up of three components:

- Cognitive flexibility – ability to cognitively control and shift mental sets and overcome automatic or dominant responses.
- Cognitive openness – being receptive to new ideas, experience, and perspectives.
- Focused attention – ability to attend to relevant stimuli and ignore distracting ones (Good and Yeganeh, 2012).

In line with the above definition, cyber operator capability of cognitive movement by the use of flexible attention and self-regulatory strategies is previously described as displaying cognitive agility (Jøsok et al., 2018; Knox B. et al., 2018) and operationalized as movements (total distance traveled, *x*- and *y*-movement, and quadrant changes) in The Hybrid Space (Knox et al., 2017). Cognitive agility has previously been associated with performance in cyber operations, with higher values of cognitive agility associated with higher level of performance (Knox B. et al., 2018).

Performing deliberate cognitive movements in The Hybrid Space requires observation of and control of own thoughts and actions. Self-regulation refers to the self's ability to control its own thoughts, emotions, and actions (Baumeister et al., 1994). Self-regulation has previously been linked to individual performance across multiple domains, working through the sustained effort of self-observing behavior, self-directed actions, and performing self-reactive influence (Jaramillo et al., 2017). A large body of studies have linked the ability to self-regulate to positive outcomes in academic achievement and learning in children (Bohlmann and Downer, 2016; Montroy et al., 2016), adolescents (Duckworth and Seligman, 2005; Lerner et al., 2011; Cetin, 2015), and adults (Lerner et al., 2011). Ability to self-regulate has also been linked to development of multiple literacies (Bohlmann and Downer, 2016). Self-regulation is thought to be a relatively stable trait (Shoda et al., 1990), but can be developed through external influence (e.g., modeling and/or mentoring) and own effort (Bandura, 1986). Self-regulation is a well-established and powerful concept that (a) offers the possibility to be measured reliably, (b) can be made subject to training or selection, and (c) is also relevant as it – if shown relevant – might open the opportunity to be used in training of cyber personnel to make better use of their self-regulatory resources. Self-regulation should therefore be explored in relation to displays of cognitive agility and performance in cyber operations. A challenge that remains is establishing consensus of how to assess operator performance in cyber operations (Forsythe et al., 2013). Previous research points to agility and flexible cognitive strategies as pathways to performance in cyber operations (Knox B. et al., 2018). However, how cyber operators maneuver cognitively to make sense of the hybrid environment is unknown. This article explores the relationship between self-regulation, cognitive agility, and performance.

Examining cyber operators in a naturalistic environment, such as during cyber defense exercises, is essential to understanding how they think and work together to conduct successful cyber operations. Few studies have addressed the cognitive competencies of cyber operators, and how these contribute to performance. Our approach seeks to identify individual cognitive competencies that support performance in cyber operators across the hybrid space they are expected to manage. Identification of cognitive competencies that support performance in cyber operators can help develop cyber operator education and training, and pave the way for more focused research in cyber specific competency requirements. As well as advancing the development of reliable performance measures in cyber operations.

MATERIALS AND METHODS

Description of Participants

The participants in this study were cadets attending the Norwegian Defence Cyber Academy (NDCA). This is a military academy organized under the Norwegian Defence University College. The education offered by the NDCA is a 3.5-year study program, where approximately 40 students are recruited every year. Upon successful completion of the program, students are awarded a bachelor's degree in computer engineering and military studies. Students accepted for this education undergo an officer candidate selection process similar to other military academies in Norway, but with additional demands in science, technology, engineering, and mathematics (STEM) subjects. During selection, cyber-domain specific abilities, motivation, and interest are subject to assessment, as well as health and physical performance. This specific process of selection results in considerable homogeneity in the student group on numerous measures. The subsequent computer and information systems (CIS) and cyber focused education results in knowledge of cyber domain characteristics and understanding of multi-domain military operations. In addition, a mandatory leadership development program is included in the education. The students can therefore be expected to have knowledge and competence in basic psychological and leadership theories (see Knox B. et al., 2018 for a description of the curriculum and pedagogy). In their final year, they are required to take part in a military exercise, named Cyber Defence Exercise (CDX). The CDX marks the completion of the education, and serves as the experimental environment for this study. Participants in the study comprised of 25 cyber cadets (two were removed in the data analysis due to incomplete data sets making the total number of participants $N = 23$), $M_{\text{age}} = 22.7$ years, $SD = 0.71$. Students were invited to participate in the research during the preparation week leading up to the CDX. At this time, they were provided all necessary information regarding The Hybrid Space conceptual framework and assessment of own cognitive location in relation to this (Jøsok et al., 2018).

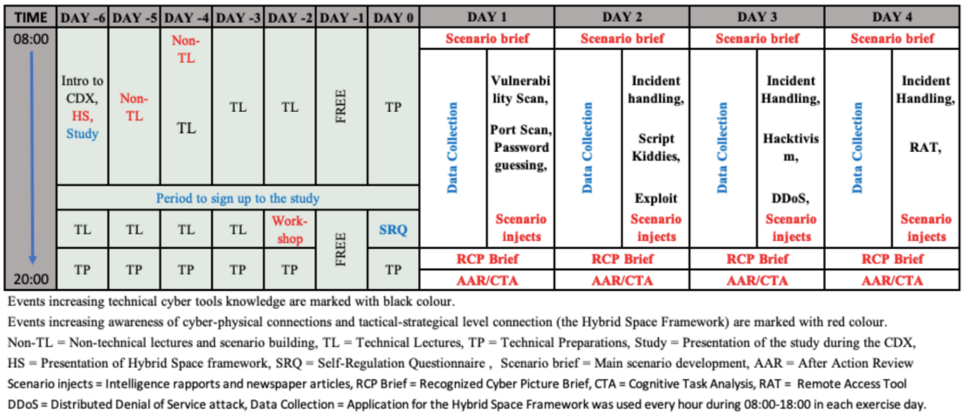
Experimental Conditions

This study took place in the CDX of November 2017. The purpose of the CDX it to produce a naturalistic environment in which participants have to exercise a variety of competencies in cyber, physical, and social domains in order to excel in proficiency and understanding of interactions occurring in cyber operations. The design of the exercise simulates a real-world scenario, and includes an attacker team, mentors, and an exercise control (EXCON) that manages the cyber-physical training infrastructure. The exercise is driven by an interconnected cyber-physical scenario with the aim of mirroring the complexity of real-life military cyber operations. Using a scenario-based approach allowed students the opportunity to understand the complexity, uncertainty, and interconnectivity associated with a geopolitical multi-domain conflict. Having a real-world scenario with dynamic attacking strategies was expected to create a learning environment in which students lift their head out of their computer and think critically concerning their actions in a broader context. Scenario injects were delivered to participating teams via an EXCON using various means (e-mail, news articles, webpages, etc.) and guided by a comprehensive scenario handbook.

The outline of the components of the study is shown in **Figure 2**. Students were introduced to the CDX, The Hybrid Space, and the study on the first day (day 6). The following days leading up to the start (6 to 2) were dedicated to technical lectures (TL), non-technical lectures (non-TLs), and technical preparations (TPs). Mentors facilitated a non-technical workshop where students considered different attack scenarios: what could be targeted, who could be behind, the scale and impact for own operations, and how to handle the situation. Students signed up to the study during these days. Self-regulation questionnaires (SRQs) were administered to the participants at day 0. Cognitive agility data were collected from day 1 to day 4 while the students defended their network from the different attacks shown in **Figure 2**.

The attacker team included three cyber security professionals. The role of attacker team was to attack targets in the infrastructure of the defender team. The attacker team attempted to gain access to data and services, such as websites and e-mails, on the defender team's networks without being detected. Attack types such as port-scanning, distributed denial of service (DDoS), and remote access tool (RAT) attacks were used. The attacks were synchronized with the existing and ongoing developments in the physical scenario simulation. The scale and sophistication of the attacks progressively increased throughout the exercise.

During the CDX, students were divided into four teams of approximately 10 students and operated as independent security operation centers (SOCs) with the task of defending a network. The role of defender team was to detect and defend against the attacker team attacks while maintaining their normal network services. The groups in the defender team were expected to be pro-active and monitor their network based on their overall situation awareness. The groups were allowed to make decisions themselves relating to the organizational structure (i.e., organizing the responsibilities within the group, such as picking a team leader), the physical structure (i.e., workstation arrangements, display of different maps, and graphical representations), and planning and discussion activities (i.e., providing status updates in team meetings).



TIME	DAY -6	DAY -5	DAY -4	DAY -3	DAY -2	DAY -1	DAY 0	DAY 1		DAY 2		DAY 3		DAY 4	
08:00	Intro to CDX, HS, Study	Non-TL	Non-TL TL	TL	TL	FREE	TP	Scenario brief		Scenario brief		Scenario brief		Scenario brief	
								Data Collection	Vulnerability Scan, Port Scan, Password guessing, Scenario injects	Data Collection	Incident handling, Script Kiddies, Exploit Scenario injects	Data Collection	Incident Handling, Hacktivism, DDoS, Scenario injects	Data Collection	Incident Handling, RAT, Scenario injects
	Period to sign up to the study														
	TL	TL	TL	TL	Work-shop	FREE	SRQ								
20:00	TP	TP	TP	TP	TP		TP	RCP Brief		RCP Brief		RCP Brief		RCP Brief	
								AAR/CTA		AAR/CTA		AAR/CTA		AAR/CTA	

Events increasing technical cyber tools knowledge are marked with black colour.

Events increasing awareness of cyber-physical connections and tactical-strategical level connection (the Hybrid Space Framework) are marked with red colour.

Non-TL = Non-technical lectures and scenario building, TL = Technical Lectures, TP = Technical Preparations, Study = Presentation of the study during the CDX,

HS = Presentation of Hybrid Space framework, SRQ = Self-Regulation Questionnaire , Scenario brief = Main scenario development, AAR = After Action Review

Scenario injects = Intelligence rapports and newspaper articles, RCP Brief = Recognized Cyber Picture Brief, CTA = Cognitive Task Analysis, RAT = Remote Access Tool

DDoS = Distributed Denial of Service attack, Data Collection = Application for the Hybrid Space Framework was used every hour during 08:00-18:00 in each exercise day.

FIGURE 2 | Outline of the different components of the study.

The CDX was led by an EXCON team that included external mentors, commander in chief, and subject matter experts (SMEs). The role of the EXCON team was to manage the exercise, play the scenario, host the network infrastructure, coordinate and provide the defender team with necessary inputs to ensure the exercise was executed as intended, and record all network traffic. The external mentors were computer network defense (CND) professionals who were responsible for observing and providing guidance to the SOCs. The mentors were not allowed to directly influence the actions of SOCs, but were allowed to clarify various uncertainties about what to do, and ensure that the SOCs received useful and constructive feedback. The commander in chief was a professional officer. His role was in the physical domain. He acted as the senior ranking officer whose decisions making (e.g., deploying troops on the ground) was dependent upon on situational awareness presented by the SOCs. SMEs were responsible for scenario and story line development and the logic behind them. During the exercise, they made adjustments to the scenario in an effort to ensure that students obtain maximal benefits from such experiences.

Experimental Infrastructure

A cyber-range was set up with physical hardware and a virtual environment consisting of virtual computers and network equipment. All SOCs had the same/similar hardware, similar physical working conditions, followed the same time-table, and were exposed to the same demands (i.e., ordered to brief the commander in chief, called in to status meetings and delivering the same products based on their current understanding of the situation).

Data Collection

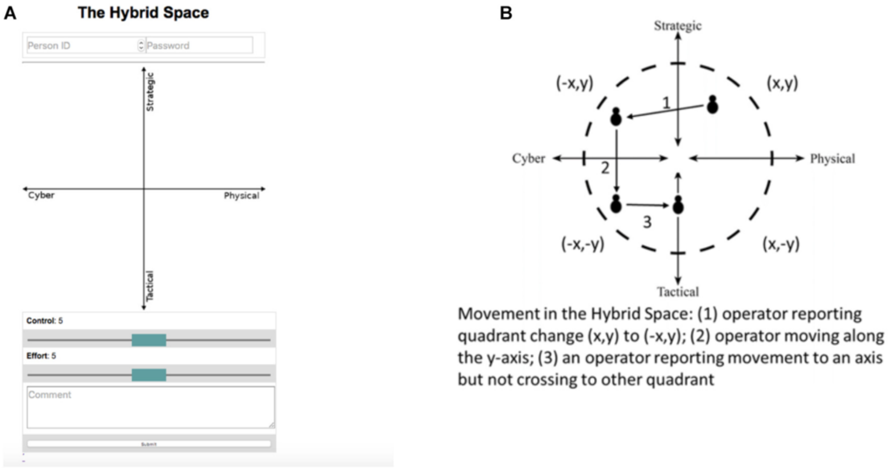
The SRQ was used to evaluate self-regulatory ability through self-report (Brown et al., 1999). The seven-step model of self-regulation was initially developed to study addictive behavior. However, the self-regulatory processes described in the model are considered to reflect general principles of behavioral self-regulation, the reliability appears to be excellent, and the total SRQ score has been validated to reflect self-regulatory functioning (Miller and Brown, 1991; Brown, 1998). In the SRQ model, behavioral self-regulation is seen as a process and therefore may fault as a result of failure in completing any of these seven steps (Brown et al., 1999):

1. Receiving relevant information
2. Evaluating the information and comparing it to norms
3. Triggering change
4. Searching for options
5. Formulating a plan
6. Implementing the plan
7. Assessing the plan's effectiveness (which recycles to steps 1 and 2).

A sample item includes "I have personal standards, and try to live up to them" and "When I'm trying to change something, I pay a lot of attention to how I'm doing." The form has previously demonstrated high internal consistency and reliability (Cronbach's $\alpha = 0.91$) and showed acceptable reliability score for this study (Cronbach's $\alpha = 0.75$). The SRQ consists of 63 items, and each point is scored through a five-point Likert scale (1 – strongly disagree, 2 – disagree, 3 – uncertain or unsure, 4 – agree, 5 – strongly agree) (Brown et al., 1999). Participants filled out the SRQ prior to the CDX exercise. The items comprise a total score and a score for each subscale.

Application of the Hybrid Space Framework

Cognitive agility data were collected by use of a web-based application where 0 is the center, X- and Y-axis range from -100 to $+100$ (see **Figure 3A**). The application was specifically designed and developed to collect data during the CDX (see Jøsok et al., 2018 for details on the development and application of the data collection app). Students participating in the research were instructed to mark their cognitive location every hour



Movement in the Hybrid Space: (1) operator reporting quadrant change (x,y) to (-x,y); (2) operator moving along the y-axis; (3) an operator reporting movement to an axis but not crossing to other quadrant

FIGURE 3 | (A) Screenshot of The Hybrid Space app. **(B)** Visualization of computed variables.

(0800–1800) for 4 consecutive days while participating in the CDX. Students first entered their location in The Hybrid Space (e.g., when conducting malware analysis, one would typically mark a lower left position, and when collaborating in their team making sense of the malware one would typically mark a position lower and to the right based on their human-to-human interaction). When sense making on operational/strategic impact of their findings, one would consider information that required cognitive positioning toward the higher dimensions of The Hybrid Space). Students then entered their perceived level of control and their perceived level of cognitive effort at the moment by adjusting the sliders to a nine-point Likert scale with distinct points ranging from 1 till 9, where 1 represents the lowest subjective assessed momentary effort or control and 9 is the highest level of momentary control or effort. Comments were made voluntary in order to minimize intervention time; however, if they chose to use the comment field, they were instructed to disclose the current task they were engaged in.

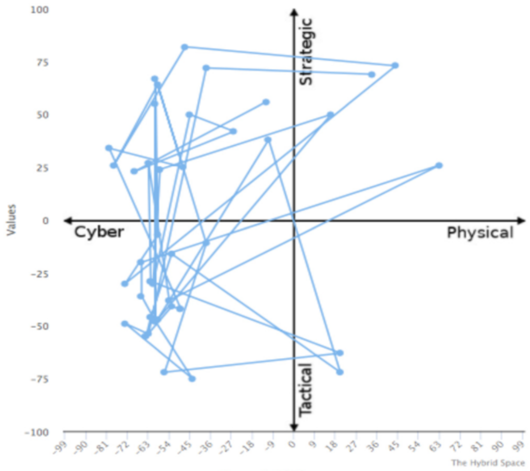
For the purpose of analysis, and based on the possible operator reported movements shown in **Figure 3B**, totals for the following dependent variables were computed; HSDT: total distance traveled in the Cartesian plane measured by Euclidean distance; HSQC: number of quadrant changes; HSxM: movement along the cyber-physical domain (*x*-axis); HSyM: movement along the strategic-tactical domain (*y*-axis). The dependent variables were first developed and reported in Knox et al. (2017). An example of raw data collected from one individual is shown in **Figure 4**.

Data Reduction and Analysis

All variables were checked for distribution and normalized if needed. Statistical analysis was then performed with all variables. Correlations and regression analysis were then performed with self-regulation entered as the independent variable and Hybrid Space movements (HSDT, HSQC, HSxM, HSyM) entered as dependent variables. The alpha levels for testing the hypothesis were set at the 0.05 level. All analyses are performed using SPSS v24. Although Cohen's convention is often used to interpret effect size in psychology (Cohen, 2003), due to a moderate sample size in this pilot study, we have applied a more restrictive wording in accordance with Mukaka (2012) to interpret the effect size of the correlation coefficient. The applied wording is shown in **Table 1**.

Ethics Statement

Prior to the start of the exercise, all participants were informed about the overall scope of the study and how to use the Hybrid



X travel: **1973**
Y travel: **1466**
Total travel: **2766**
Quadrant changes: **24**

FIGURE 4 | Visualized data from The Hybrid Space App.

TABLE 1 | Interpretation size of correlation coefficient (Mukaka, 2012).

Size of correlation	Interpretation
0.90 to 1.00 (−0.90 to −1.00)	Very high positive (negative) correlation
0.70 to 0.90 (−0.70 to −0.90)	High positive (negative) correlation
0.50 to 0.70 (−0.50 to −0.70)	Moderate positive (negative) correlation
0.30 to 0.50 (−0.30 to −0.50)	Low positive (negative) correlation
0.00 to 0.30 (−0.00 to −0.30)	Negligible correlation

TABLE 2 | Descriptive statistics (*N* = 23).

	Mean	Std. deviation	Minimum	Maximum
Cognitive agility HSDT	2225.09	93.71	723	4161
HSQC	17.39	6.92	6	30
HSxM	1539.17	740.41	456	3145
HSyM	1271.96	550.90	446	2595
SRQ SR_Receiving	30.53	4.32	23	38
SR_Evaluating	29.33	4.14	21	41
SR_Triggering	30.41	2.65	26	35
SR_Searching	32.28	3.01	25	36
SR_Planning	31.39	3.99	24	36
SR_Implementing	31.00	4.43	24	38
SR_Assessing	31.00	2.48	26	34
SR_Total	214.33	12.6	199	236

HSDT: distance traveled in the Cartesian plane measured by Euclidian distance; HSQC: number of quadrant changes; HSxM: movement along the cyber-physical domain (x-axis); HSyM: movement along the strategic-tactical domain (y-axis); SRQ: self-regulation questionnaire.

Space application. Participants signed informed consent prior to the intervention, and were informed of the unquestioned opportunity to withdraw at any time. The project is registered with the Norwegian Social Science Data Services (NSD) project number 55446.

RESULTS

The comment field (see **Figure 3A**) was rarely used by the participants, and hence it was excluded in further analysis. Participants also reported their perceived momentary level of effort and control at the same time as entering their cognitive location in The Hybrid Space. However, during analysis, it was decided to exclude the data from this paper in order focus on cognitive agility and self-regulation. Henceforth, the remaining data presented are SRQ data and cognitive agility data. Descriptive statistics are presented in **Table 2**.

The relationship between cognitive agility (as measured by The Hybrid Space application) and self-regulation (as measured by the SRQ) was investigated using Pearson product-moment correlation coefficient (see **Table 3**). Preliminary analyses were performed to ensure no violation of the assumptions of normality, linearity and homoscedasticity. Using Mukaka's (2012) standards for interpreting correlations, all measures of cognitive agility were low to moderately positive correlated to total self-regulation score (SR_total) (see **Table 3**).

Linear regression was used to assess the ability of self-regulation to predict cognitive agility (see **Table 4**). Computed cognitive agility indicators were set at as dependent variables, and self-regulation total scores were set as independent variable. All self-regulation variables moderately predicted HS movements (see **Table 4** and **Figure 5**). Using this model, self-regulation explained 43.1% of cognitive agility in The Hybrid Space. Looking at the subcomponent of the total movement, self-regulation explained 41.6% of the *x*-axis movement, and 29.9% of the *y*-axis movement; 24.4% of the quadrant changes is explained by self-regulation.

Scatterplots of the results visualize a moderate positive relationship between higher levels of self-regulation and increased cognitive agility by all variables. Curved lines show confidence intervals to the mean at the 0.05 level.

In summary, display of cognitive agility in The Hybrid Space appears to be predicted by self-regulation when performing defensive cyber operations during this CDX.

DISCUSSION

This study tested if self-regulation could predict performance of cyber operators during a CDX. The results show that higher levels of self-regulation in cyber cadets are associated with displays of cognitive agility as measured by movement in The Hybrid Space, thus supporting the hypothesis. The environment that this CDX is replicating is earlier described as hybrid (Jøsok et al., 2016), and characterized by novel task demands (McClain et al., 2015), cognitive intense work (D'Amico et al., 2016), challenging situational awareness (D'Amico et al., 2005), team collaboration and coordination perspectives (Champion et al., 2012; Jøsok et al., 2017), communication challenges (Knox B.J. et al., 2018), and challenges in assessing performance (Ben-Asher and Gonzalez, 2015). A cyber operations environment is argued to crave constant adaptation to complexity by cyber operators (Lathrop et al., 2016). This involves displays of higher order cognitive skills (Knox B. et al., 2018) associated with displays of cognitive agility (Knox et al., 2017), here represented by ability to flexibly adjust attention, exercise cognitive control, shift cognitive focus, and regulate responses in The Hybrid Space. Self-regulation has shown similar results in previous studies, suggesting that self-regulation is associated with displays of cognitive agility and performance of cyber operators (Knox et al., 2017; Knox B. et al., 2018). The subcomponents of self-regulation in relation to cognitive agility are discussed below.

Higher levels of self-regulation were associated with more active search for information in The Hybrid Space, meaning that the individual operator traversed cyber and physical domains cognitively, as well as strategic and tactical considerations when seeking out relevant information. As self-observation is a prerequisite for self-regulation (Bandura, 1986), contextual overview of the environment is necessary to situate oneself and one's actions in The Hybrid Space. Hence, a presupposition for self-regulation action would be to locate oneself and identify human or digital artifacts in the Hybrid Space. Therefore, a behavior that displays high levels of cognitive agility when

TABLE 3 | Pearson's correlations (*N* = 23).

	2	3	4	5	6	7	8	9	10	11	12
1.HSDT	**0.858****	**0.946****	**0.874****	**0.778****	**0.491***	**−0.661****	−0.043	0.403	0.260	0.459	**0.685****
r (Clmax-Clmin)	0.938–0.69	0.977–0.875	0.945–0.722	0.901–0.539	0.751–0.099	−0.342–0.843	0.375–0.447	0.699–0.011	0.607–0.17	0.732–0.058	0.855–0.381
2.HSQC		**0.766****	**0.809****	**0.617****	**0.427***	**−0.502***	−0.173	**0.448***	0.347	0.107	**0.543***
r (Clmax-Clmin)		0.851–0.366	0.915–0.596	0.82–0.275	0.713–0.018	−0.114–0.757	0.257–0.546	0.726–0.044	0.664–0.076	0.497–0.319	0.78–0.169
3. HSxM			**0.676****	**0.812****	**0.436***	**−0.660****	−0.009	0.362	0.240	0.488	**0.675****
r (Clmax-Clmin)			0.851–0.366	0.917–0.601	0.718–0.036	−0.341–0.214	0.404–0.419	0.673–0.059	0.593–0.191	0.749–0.095	0.85–0.365
4. HSyM				**0.603****	**0.461***	**−0.526***	−0.053	0.399	0.273	0.328	**0.588****
r (Clmax-Clmin)				0.813–0.254	0.733–0.061	−0.146–0.771	0.367–0.45	0.696–0.015	0.615–0.156	0.652–0.097	0.805–0.233
5. SR_Receiving					**0.433***	**−0.470***	−0.183	0.286	0.220	0.474	**0.740****
r (Clmax-Clmin)					0.717–0.026	−0.072–0.739	0.247–0.553	0.624–0.143	0.579–0.211	0.741–0.077	0.882–0.472
6. SR_Evaluating						−0.196	−0.334	0.020	−0.083	0.178	0.385
r (Clmax-Clmin)						0.235–0.562	0.09–0.655	0.428–0.395	0.34–0.478	0.549–0.252	0.688–0.032
7. SR_Triggering							0.037	−0.190	−0.344	0.158	−0.223
r (Clmax-Clmin)							0.442–0.381	0.241–0.558	0.079–0.662	0.535–0.271	0.208–0.581
8. SR_Searching								−0.014	0.225	0.244	0.181
r (Clmax-Clmin)								0.4–0.423	0.583–0.206	0.596–0.187	0.552–0.249
9. SR_Planning									**0.449***	0.344	**0.608****
r (Clmax-Clmin)									0.726–0.046	0.662–0.079	0.815–0.262
10. SR_Implement										0.094	**0.529***
r (Clmax-Clmin)										0.487–0.331	0.772–0.15
11. SR_Assessing											**0.703****
r (Clmax-Clmin)											0.864–0.41
12. SR_Total											1.000
r (Clmax-Clmin)											1–0.998

***Correlation is significant at the 0.01 level (one-tailed). *Correlation is significant at the 0.05 level (one-tailed). Upper confidence and lower confidence intervals r(Clmax-Clmin) are shown at the 0.05 level. Bold values are both significant at the 0.01 and 0.05 level.*

TABLE 4 | Regressions for self-regulation and cognitive agility indicators.

Model	*R*	R^2	Adj R^2	*F*	*p*	β	*t*
HSDT	0.685	0.469	0.431	12.372	0.003	0.685	3.517
HSQC	0.543	0.294	0.244	5.843	0.030	0.543	2.417
HSxM	0.675	0.455	0.416	11.692	0.004	0.675	3.419
HSyM	0.588	0.345	0.299	7.384	0.017	0.588	2.717

HSDT: hybrid space distance traveled; HSQC: hybrid space quadrant changes; HSxM: hybrid space x-axis movement; HSyM: hybrid space y-axis movement.

searching for information in order to make sense of the evolving situation could be considered a performance strategy in cyber operations as this would facilitate better cyber situational awareness (D'Amico et al., 2005). This is supported by the findings that self-regulation receiving behavior was moderately associated with all cognitive agility measurements.

Evaluating the accuracy and importance of the obtained information from one Hybrid Space dimension might require additional revisiting of other locations in The Hybrid Space. This can be the result of a rapid changing situation or that the task challenges limitations in working memory capacity, and requires additional refreshing or confirmation of information. Other explanations can be that operating in change and novelty shifts the demands from problem solving to problem identifying, resulting in needs to continually shift in between searching and evaluating information, at least until an abnormality, challenge, or problem is identified. Prior research confirms that ambiguous shifting conditions require competencies at identifying problems (Lathrop et al., 2016), and that flexible cognitive strategies need to be applied to construct higher levels of understanding of the problem-solving at hand (Ward et al., 2013). Spending effort in this phase makes sense also in a cyber defense setting where a lot of the time nothing happens. A resulting effect may be sustained attention toward understanding the state of affairs as they are, leading to effort that might build proficiency in detecting and evaluating anomalies as they occur. The association between cognitive agility and the self-regulation evaluating subscale is therefore quite possibly interlinked, as searching and evaluating information in cyber operations is a twofold process.

The self-regulation triggering subscale is negatively associated with cognitive agility, and could be interpreted as reduction in distance covered in The Hybrid Space. This might be a natural consequence of the two prior subfunctions, searching and evaluating, as a stop/temporary pause in Hybrid Space probably can be triggered by identifying information that requires closer scrutiny. For example, if a piece of code or a specific internet protocol (IP) address requires attention, this would temporarily limit the need for searching.

Self-regulation in planning, implementation, and evaluating shows low positive association with cognitive agility. However, the variations between planning and implementing are interesting. While planning shows low to moderate association, implementing shows in general low association. Planning might require the cyber operator to zoom out of the current focus in The Hybrid Space and engage in conversations with the team in order to share understanding and come up with ideas to tackle the problem identified. In this vain, a cyber operator might traverse the cyber, physical, and social domains in an operational planning process, producing high levels of cognitive

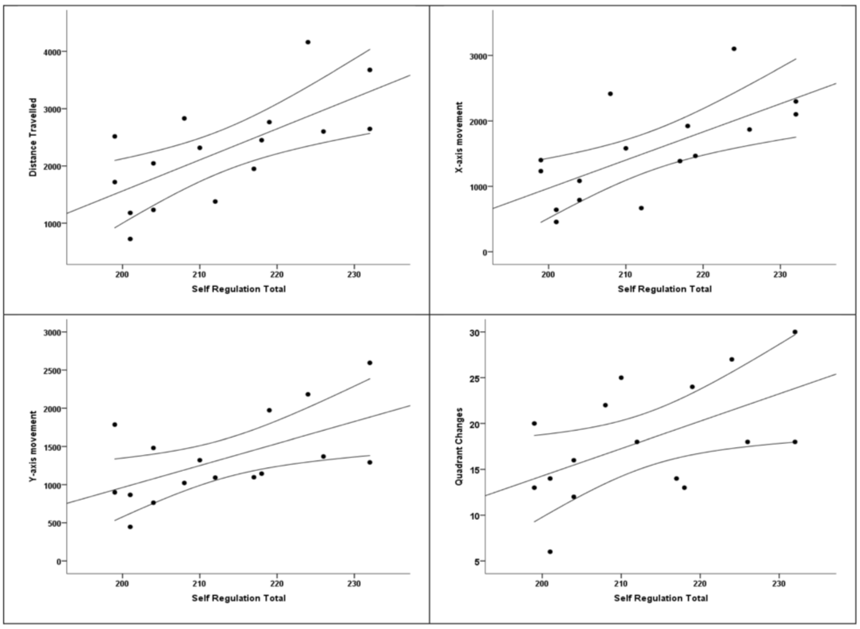


FIGURE 5 | Scatterplots.

agility. Further, when a solution (or in the absence of a solution) is present, implementing would not necessarily require high levels of cognitive agility as the solution might be limited to implementation in one part of quadrant of The Hybrid Space. Lastly, assessing the impact of the implementation shows low to moderate correlation with cognitive agility. This might be explained by the process of self-regulation which at this stage will return to stage one and two (searching and evaluating) (Brown et al., 1999).

According to the regression models, a total of 43.1% of the cognitive agility in The Hybrid Space can be explained by the self-reported trait of self-regulation. In an applied setting, a lot of contributing factors are at play. Team dynamics are previously shown to influence operator behavior (Champion et al., 2012) and team performance (Buchler et al., 2018), and could both boost or limit individual movement in The Hybrid Space, depending upon high or low team cohesion. Expert mentors triggering movement by asking questions or observing operator performance can also explain movement in the Hybrid Space. The research itself can produce a Hawthorne effect by introduction of The Hybrid Space conceptual framework and instructing participants to mark their cognitive location, constantly nudging operators to reflect over their current cognitive location. Despite the uncertainties addressed, we consider this as relatively strong results when accounting for the naturalistic setting of the CDX, the applied research approach and the novelty of The Hybrid Space approach. As self-regulation had moderate to high positive association with all Hybrid Space movements, the results state that The Hybrid Space can be used to assess levels of self-regulation and the display of cognitive agility among cyber operators.

With the self-regulation construct being linked to performance in a variety of domains, and especially important for learning, it is likely that cognitive agility in The Hybrid Space can be closely linked to performance. High levels of self-regulation have been associated with sticking to behaviors consistent with long-term goals (Brown et al., 1999), and in the context of military cyber operator tasks this implies ability to make decisions regarding in the moment activity that is consistent with reaching overall operational goals. This means that the cyber operator has to have understanding of the overall operational goals as well as own tactical goals and how actions in the cyber domain might influence both. Cognitive agility in The Hybrid Space could support the individual cyber operator to perform better by taking actions in line with the overall context by enabling better contextual knowledge and understanding. However, there is to date no consensus about the operationalization, the assessment, and the quantification of cyber operator performance (Mancuso et al., 2014; Lathrop et al., 2016). There are though attempts to understand performance by comparing the use of software tools between novices and experts (McClain et al., 2015). With the current difficulties in assessing performance in cyber operations, and the absence of performance indicators in cyber operations, the proposed causality between displays of cognitive agility and performance can serve as a pathway to further research and insight into human performance in cyber operations. Building on previous research results proposed in Jøsok et al. (2016) and Knox et al. (2017), we see this as a step further in validating The Hybrid Space as a not only a conceptual model, but also as a tool for assessing individual performance in cyber operations.

This research was approached as a naturalistic and descriptive study in an applied setting, and as such correlational in nature. Further systematic research is needed in which causal pathways are identified, and the complex concepts of self-regulation and cognitive agility investigated in more detail, including intervention studies on enhancement of these skills in cyber operator education. In order to confirm the findings in this study, larger samples are required, as well as developed performance measures to assess levels of cyber operator performance.

CONCLUSION

The results support the hypothesis by showing that self-regulation predicts cognitive agility in cyber operators, as measured by cognitive focus movements in The Hybrid Space conceptual framework, when performing defensive cyber operations during a CDX. Theories of cyber operator competencies highlight that cyber operators need a varied skill-set and competencies beyond technical proficiency to perform well; previous research has associated cognitive agility to performance in cyber operations. Our results are in line with theories of cyber operator competencies, and we contribute to cyber operator competence profiles by confirming that cyber operators' self-regulation is associated with performance in cyber operations, in a training environment. This work highlights the need to focus on developing cyber operators soft skills as pathways to better performance. Future work should include investigating cognitive agility in relation to reliable performance measures in cyber operations to evaluate the association between cognitive agility and performance in cyber operations.

ETHICS STATEMENT

The project is approved by Norwegian Centre for Research Data with project number: 55446 and project title: Grow up digital – Developing cognitive agility and decision-making competence to maneuver in domains of complexity. The following information sheet was distributed, read, and signed by each participant prior to the data collection.

AUTHOR CONTRIBUTIONS

ØJ contributed to the ideas, design, preparation, and execution of the study as well as the analyses of results, drafting, necessary theory research, and write up of all parts of the manuscript. RL contributed to data preparation, data analyses, writing of results, as well as writing the manuscript. BK contributed to designing, planning, and execution of the CDX as well as execution of the study, interpreting results, and improving the manuscript. KH contributed to improving the manuscript. SS contributed to framing the manuscript, interpreting the results, and improving the manuscript.

FUNDING

This work was supported by the Norwegian Defence Cyber Academy.

ACKNOWLEDGMENTS

A special thanks is given to the students of Wing 69 at the NDCA for their contributions that made this research possible.

REFERENCES

Bandura, A. (1986). *Social Foundations of Thought & Action - a Social Cogntive Theory*. Upper Saddle River, NJ: Prentice Hall.

Baumeister, R. F., Heatherton, T. F., and Tice, D. M. (1994). *Losing Control: How And Why People Fail at Self-Regulation*. San Diego, CA: Academic Press.

Ben-Asher, N., and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Comput. Human Behav.* 48, 51–61. doi: 10.1016/j.chb.2015.01.039

Bohlmann, N. L., and Downer, J. T. (2016). Self-regulation and task engagement as predictors of emergent language and literacy skills. *Early Educ. Dev.* 27, 18–37. doi: 10.1080/10409289.2015.1046784

Brown, J. M. (1998). "Self-regulation and the addictive behaviors," in *Applied Clinical Psychology. Treating Addictive Behaviors*, eds W. R. Miller and N. Heather (New York, NY: Plenum Press), 61–73. doi: 10.1007/978-1-4899-1934-2_5

Brown, J. M., Miller, W. R., and Lawendowski, L. A. (1999). "The self-regulation questionnaire," in *Innovations in Clinical Practice: A Source Book*, Vol. 17, eds L. Vandecreek and T. L. Jackson (Sarasota, FL: Professional Resource Press), 281–292.

Buchler, N., Fitzhugh, S. M., Marusich, L. R., Ungvarsky, D. M., Lebiere, C., and Gonzalez, C. (2016). Mission command in the age of network-enabled operations: social network analysis of information sharing and situation awareness. *Front. Psychol.* 7:937. doi: 10.3389/fpsyg.2016.00937

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., and Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Front. Psychol.* 9:2133. doi: 10.3389/fpsyg.2018.02133

Cetin, B. (2015). Academic motivation and self-regulated learning in predicting academic achievement in college. *J. Int. Educ. Res.* 11, 95–106. doi: 10.19030/jier.v11i2.9190

Champion, M., Jariwala, S., Ward, P., and Cooke, N. J. (2014). Using cognitive task analysis to investigate the contribution of informal education to developing cyber security expertise. *Proc. Human Fact. Ergon. Soc. Annu. Meet.* 58, 310–314. doi: 10.1177/1541931214581064

Champion, M. A., Rajivan, P., Cooke, N. J., and Jariwala, S. (2012). "Team-based cyber defense analysis," in *Proceedings of the 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, (New Orleans, LA: IEEE), doi: 10.1109/CogSIMA.2012.6188386

Coghlan, D., and Brydon-Miller, M. (2014). *The SAGE Encyclopedia of Action Research*. London: Sage Publications, Ltd. doi: 10.4135/9781446294406

Cohen, J. (2003). "A power primer," in *Methodological Issues & Strategies in Clinical Research*, ed. A. E. Kazdin (Washington, DC: American Psychological Association), 427–436.

D'Amico, A., Buchanan, L., Kirkpatrick, D., and Walczak, P. (2016). "Cyber operator perspectives on security visualization," in *Advances in Human Factors in Cybersecurity*, (Cham: Springer International Publishing), 69–81. doi: 10.1007/978-3-319-41932-9_7

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., and Roth, E. (2005). "Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, (Los Angeles, CA: SAGE Publications), doi: 10.1177/154193120504900304

Duckworth, A. L., and Seligman, M. E. P. (2005). Self-discipline outdoes IQ in predicting academic performance of adolescents. *Psychol. Sci.* 16, 939–944. doi: 10.1111/j.1467-9280.2005.01641.x

Efklides, A. (2008). Metacognition: defining its facets and levels of functioning in relation to self-regulation and co-regulation. *Eur. Psychol.* 13, 277–287. doi: 10.1027/1016-9040.13.4.277

Toering, T. T., Elferink-Gemser, M. T., Jordet, G., and Visscher, C. (2009). Self-regulation and performance level of elite and non-elite youth soccer players. *J. Sports Sci.* 27, 1509–1517. doi: 10.1080/02640410903369919

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., and Fink, G. (2010). A multi-phase network situational awareness cognitive task analysis. *Inform. Vis.* 9, 204–219. doi: 10.1057/ivs.2010.5

Forsythe, C., Silva, A., Stevens-Adams, S., and Bradshaw, J. (2013). "Human dimension in cyber operations research and development priorities," in *Proceedings of the International Conference on Augmented Cognition*, (Berlin: Springer), 418–422. doi: 10.1007/978-3-642-39454-6_44

Good, D., and Yeganeh, B. (2012). Cognitive agility: adapting to real-time decision making at work. *OD Pract.* 44, 13–17.

Helkala, K., Knox, B., Jøsok, Ø, Lugo, R., Sütterlin, S., Dyrkolbotn, G. O., et al. (2017). "Supporting the Human in Cyber Defence," in *Proceedings of the International Workshop on Computer Security: SECPRE 2017, CyberICPS 2017*, (Oslo: Springer), 147–162. doi: 10.1007/978-3-319-72817-9_10

Jaramillo, J. M., Rendón, M. I., Muñoz, L., Weis, M., and Trommsdorff, G. (2017). Children's self-regulation in cultural contexts: the role of parental socialization theories, goals, and practices. *Front. Psychol.* 8:923. doi: 10.3389/fpsyg.2017.00923

Jøsok, Ø, Hedberg, M., Knox, B., Helkala, K., Lugo, R., and Sutterlin, S. (2018). "Development and application of the hybrid space app for measuring cognitive focus in hybrid contexts," in *Proceedings of the International Conference on Augmented Cognition: Intelligent Technologies. AC 2018*, (Las Vegas, NV: Springer), doi: 10.1007/978-3-319-91470-1_30

Jøsok, Ø, Knox, B., Helkala, K., Lugo, R., Sutterlin, S., and Ward, P. (2016). "Exploring the hybrid space theoretical framework applying cognitive science in military cyberspace operations," in *Proceedings of the 10th International Conference on Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience. AC 2016*, (Toronto, ON: HCI International Canada), 178–188. doi: 10.1007/978-3-319-39952-2_18

Jøsok, Ø, Knox, B. J., Wilson, K., Helkala, K., Lugo, R. G., Sutterlin, S., et al. (2017). "Macrocognition applied to the hybrid space: team environment, functions and processes in cyber operations," in *Proceedings of the International Conference on Augmented Cognition. Enhancing Cognition and Behavior in Complex Human Environments. AC* 2017, (Cham: Springer), doi: 10.1007/978-3-319-58625-0_35

Knox, B., Lugo, R., Helkala, K., Sütterlin, S., and Jøsok, Ø (2018). "Education for cognitive agility: improved understanding and governance of cyberpower," in *Proceedings of the International European Conference on Cyber Warfare and Security*, (Oslo: ACPI).

Knox, B. J., Jøsok, Ø, Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R. G., et al. (2018). Socio-technical communication: the hybrid space and the OLB model for science-based cyber education. *Mil. Psychol.* 30, 350–359. doi: 10.1080/08995605.2018.1478546

Knox, B. J., Lugo, R. G., Jøsok, Ø, Helkala, K., and Sütterlin, S. (2017). "Towards a cognitive agility index: the role of metacognition in human computer interaction," in *Proceedings of the Conference on HCI International 2017*, (Cham: Springer International Publishing), 330–338. doi: 10.1007/978-3-319-58750-9_46

Lathrop, S. D., Trent, S., and Hoffman, R. (2016). "Applying human factors research towards cyberspace operations: a practitioner's perspective," in *Advances in Human Factors in Cybersecurity*, ed. D. Nicholson (Cham: Springer International Publishing), doi: 10.1007/978-3-319-41932-9_23

Lerner, R. M., Lerner, J. V., Bowers, E. P., Lewin-Bizan, S., Gestsdottir, S., and Urban, J. B. (2011). Self-regulation processes and thriving in childhood and adolescence: a view of the issues. *New Dir. Child Adolesc. Dev.* 2011, 1–9. doi: 10.1002/cd.300

MacKay-Brandt, A. (2011). "Focused attention," in *Encyclopedia of Clinical Neuropsychology*, eds J. S. Kreutzer, J. DeLuca, and B. Caplan (New York, NY: Springer), 1066–1067. doi: 10.1007/978-0-387-79948-3_1303

Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., and Knott, B. (2014). "Human factors in cyber warfare II emerging perspectives," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, (Thousand Oaks, CA: SAGE Publications), 415–418. doi: 10.1177/1541931214581085

McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., et al. (2015). Human performance factors in cyber security forensic analysis. *Procedia Manuf.* 3, 5301–5307. doi: 10.1016/j.promfg.2015.07.621

Miller, W. R., and Brown, J. (1991). "Self-regulation as a conceptual basis for the prevention and treatment of addictive behaviors," in *Self-Control and the Addictive Behaviours*, eds N. Heather, W. R. Miller, and J. Greeley (Sydney: Maxwell Macmillan), 3–79.

Montroy, J. J., Bowles, R. P., Skibbe, L. E., McClelland, M. M., and Morrison, F. J. (2016). The development of self-regulation across early childhood. *Dev. Psychol.* 52, 1744–1762. doi: 10.1037/dev0000159

Mukaka, M. M. (2012). A guide to appropriate use of correlation coefficient in medical research. *Malawi Med. J.* 24, 69–71.

NATO (2016a). *Cyber Defence Pledge*. Brussels: NATO.

NATO (2016b). *Warsaw Summit Communiqué*. Brussels: NATO.

Røislien, H. E. (2015). When the generation gap collides with military structure: the case of the Norwegian cyber officers. *J. Mil. Strateg. Stud.* 16, 23–44.

Shoda, Y., Mischel, W., and Peake, P. K. (1990). Predicting adolescent cognitive and self-regulatory competencies from preschool delay of gratification: identifying diagnostic conditions. *Dev. Psychol.* 26, 978–986. doi: 10.1037/0012-1649.26.6.978

Tapscott, D. (2014). *The Digital Economy: Rethinking Promise and Peril in the Age of Networked Intelligence*. New York, Ny: McGraw-Hill.

Ward, P., Fiore, S. M., Feltovich, P. J., Hoffman, R. R., DiBello, L., and Andrews, D. H. (2013). *Accelerated Expertise: Training for High Proficiency in a Complex World*. New York, NY: Psychology Press.

Wang, P. L. (1990). "Assessment of cognitive competency," in *The Neuropsychology of Everyday Life: Assessment and Basic Competencies*, eds D. E. Tupper and K. D. Cicerone (Boston, MA: Springer), 219–228. doi: 10.1007/978-1-4613-1503-2_9

Whitman, M. E., and Mattord, H. J. (2012). *Principles of Information Security*. Boston, MA: Cengage Learning.

Zimmerman, B. J. (1990). Self-regulated learning and academic achievement: an overview. *Educ. Psychol.* 25, 3–17. doi: 10.1207/s15326985ep2501_2

Conflict of Interest Statement: Three of the authors were employed at the NDCA at the time of data collection.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Inland Norway
University of
Applied Sciences

Cyber Operator Competencies: The Role of Cognitive Competencies in Cyber Operator Practice and Education

The theme of this thesis is the role of cognitive competencies in cyber operator practice and education. Cyber operator practice is a new field of research where the importance and attention is growing rapidly. Research has accumulated a solid amount of knowledge about the technical skills required by a cyber operator. However, less is known about the cognitive competencies that support cyber operator proficiency. In order to gain insight into the cognitive demands of cyber operators, the cognitions of young cyber officers attending the Norwegian Defence Cyber Academy have been studied. Findings contributes to the development of theory and evidence-based knowledge needed to develop educational guidelines for the cyber operator workforce.

Findings indicate that knowledge and understanding of cyberspace as a domain of operations and the cognitive competencies supporting cyber operator proficiency are limited. Cognitive agility is proposed as a cognitive competency and is associated with higher levels of self-regulation. These findings suggest that cognitive competencies can indeed support cyber operator performance. This thesis therefore contributes to cyber operator practice and education by suggesting that education and training would benefit from including the development of cognitive competencies alongside the technical education and training needed to become a cyber operator. In this way, this thesis adds new insight and perspective into the novel area of cyber operator practice. The results provide the first indications that cyber operator performance can be supported by the development of cognitive competencies during education.