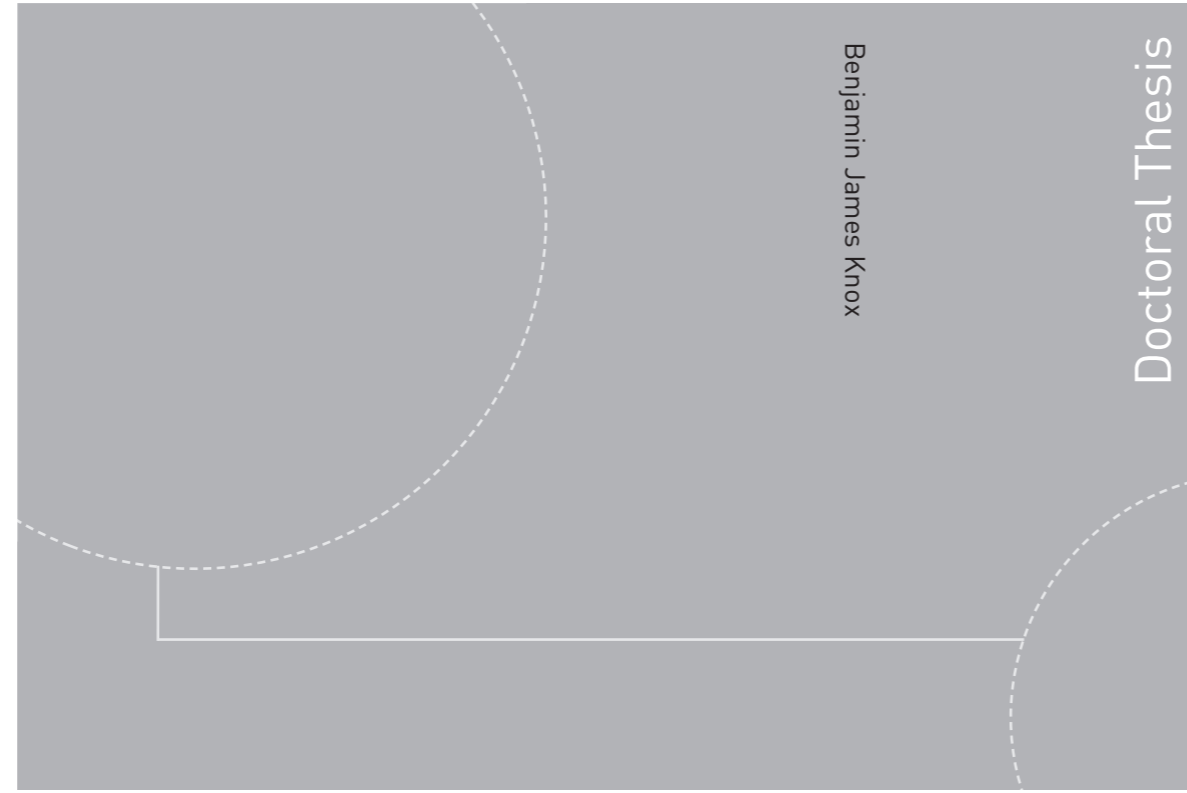


ISBN 978-82-326-4654-8 (printed version)
ISBN 978-82-326-4655-5 (electronic version)
ISSN 1503-8181



Doctoral theses at NTNU, 2020:153

Benjamin James Knox

Cyberpower Praxis: A Study of Ways to Improve Understanding and Governance in the Cyber Domain

Doctoral theses at NTNU, 2020:153

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

 **NTNU**
Norwegian University of
Science and Technology

 NTNU

 **NTNU**
Norwegian University of
Science and Technology

Benjamin James Knox

Cyberpower Praxis: A Study of Ways to Improve Understanding and Governance in the Cyber Domain

Thesis for the degree of Philosophiae Doctor

Gjøvik, January 2020

Norwegian University of Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security and Communication
Technology



Norwegian University of
Science and Technology

NTNU

Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology
and Electrical Engineering
Department of Information Security and Communication
Technology

© Benjamin James Knox

ISBN 978-82-326-4654-8 (printed version)
ISBN 978-82-326-4655-5 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2020:153



Printed by Skipnes Kommunikasjon as

Declaration of authorship

I, Benjamin James Knox, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

(Benjamin James Knox)

Date: 20 April 2020

Summary

Powerful effects arriving through cyberspace present real-world shared problems that cannot be foreseen. This thesis acknowledges the modern-day Faustian Bargain of *staying digitally dependent, staying vulnerable* presented by relentless digitalisation and the internetification of our 'Lived' and 'Official' realities. This digital dependency vs. vulnerability paradox presses for approaches to education and training that develop and support the application of the theory, lessons and skills required to effectively conduct operations in cyberspace i.e. cyberpower praxis. As we experience the effects of cyberpower through rapid, and often unchecked digitalisation, we learn that human understanding and approaches to self-governance are lacking. This makes for an uneasy arena where complexity, contestation and emerging challenges frame the institutional landscape leading to immediate reactive practices over long-term strategies.

This thesis presents a route to better cyberpower praxis by encouraging a more open, holistic and flexible way of thinking about competence development for learners in the cyber domain. Attempting to combine capacities and skills on multiple plains via alternative forms of education can help build understanding around a common goal of harnessing or defeating cyberpower effects. As well as preparing for its emerging effects. To answer the question of *identifying approaches to support performance among novice cyber operators*, this research constitutes a quantitative and qualitative design with participants from across sectors as well as cadets from the Norwegian Defence Cyber Academy. The method encourages a holistic academic and applied approach to develop activities and attitudes founded upon skills such as unstructured problem solving, critical thinking, learning, reasoning and mentoring.

Dealing with the capacity cyberpower has to influence tangible and intangible assets through digital means, requires modes of human self-governance and understanding capable of mitigating maladaptive or time-dysfunctional praxis in the face of digital uncertainty. Building cognitive capacities by drawing attention to modes of education that focus on nonroutine thinking and high order cognitive skills can be judged as a step towards performance development in the cyber domain.

This evolving art requires new and experienced domain experts, leaders, operators and educators from across disciplines to combine their skills and capacities in order to remain current with evolving technologies and adversarial actions. Whilst simultaneously being able to maintain and encourage mindsets that seek to influence into the future, rather than settling for a passive reactive posture that is susceptible to rigidity.

The presented thesis aims to provide insights and knowledge to contribute to improved proficiency levels as workplace demands increase due to complex socio-technical systems. The cognitive and collaborative nature of military cyberspace operations requires high levels of knowledge, reasoning skills and critical thinking skills. This cognitive readiness needs to be anchored in adaptive, resilient and robust capabilities.

Acknowledgements

This doctoral thesis is the outcome of an unexpected journey into academia. Although unexpected, this project has felt like one of the most natural and logical choices of my life. The purpose of this project always made sense to me due to how incredibly fortunate I was to be surrounded by amazing people, who shared the same passion and energy for this project. To those amazing people:

Stefan and Ric: you made this surreal experience real. You are two of the kindest, smartest, most humble, funny and gifted men I have ever had the pleasure of knowing. There would be no thesis without you. This is not the end....

Øyvind and Kirsi: you made me believe this was possible. The two people who believed in me, trusted me, and backed me in some dark times when no one else dared to understand or was willing to listen. You pushed me and challenged me to stick to my beliefs.

Thank you **Sokratis** for agreeing to be my main supervisor. The trust you placed in me to get this done has been a major motivator. I cannot thank you enough for making me feel worthy.

I would like to thank the Norwegian Cyber Defence and the Norwegian Defence Cyber Academy for supporting me whilst I pursued this project. You trusted me and made it possible for me to collect data, do analysis, apply and disseminate the research inside and outside the classroom, nationally and internationally. Thank you, past and present cadets, at the Cyber Academy. For twelve years you have inspired, challenged, frustrated and taught me so much. This thesis is because of you.

Then to those closest to me to whom I owe so much:

To my parents: Thank you for your patience and unwavering support. This thesis is a token of gratitude for the investment you made in my early education and the support you have given me through the years. I am extremely grateful for everything you have done for me.

To Silje: Thank you for making this possible and for always being there and believing in me. This is about 'us', not just me. We learn and journey together.

To Frøya and Finlay: Thank you for being a constant reminder that the Ph.D was not the most important thing in my life. Observing and being inspired by your drive for school and sporting endeavors was a constant source of energy for me. You fuel my engine. I hope I have instilled in you the belief that anything is possible.

Content

Part 1

1	Introduction	1
1.1	The Broader context	2
1.2	The Specific context	3
1.3	The Research problem	6
1.4	Synopsis of research studies	7
1.5	Results	10
1.6	Implications	12
1.7	Structure of thesis	13
2	Background	14
2.1	Cyberpower	14
2.2	Cyberspace domain	16
2.3	The Norwegian Defence Cyber Academy	16
2.4	Leadership	18
2.5	Governance	19
2.6	Metacognition	20
2.7	Slow Education	21
2.8	Mentoring	23
2.9	Cognitive Agility	24
3	Design and Methods	25
3.1	Philosophical approach	25
3.2	Validity in qualitative research	27
3.3	Quantitative approaches	31
3.4	Validity in Quantitative Research	31
3.5	Challenges and Benefits of Mixed Methods & Triangulation	32
3.6	Cyber Defence Exercise (CDX)	33
3.7	Research Ethics	34
4	Summary of Work (Overarching research question)	36
4.1	To what extent is cyberpower affecting institutional development in Norway?	38
4.2	Can cognitive engineering be applied to communication activities in the cyber domain to improve performance?	39
4.3	Is it possible to measure cognitive agility in cyber defence scenarios with The Hybrid Space framework?	41
4.4	To turn the Hybrid Space cognitive framework into an applied tool for measuring cognitive agility.	42
4.5	Can slow education and training interventions designed to improve metacognitive skills improve performance in cyber cadets?	44
4.6	What are the protective and risk factors of the Norwegian Defence Cyber Academy in female cyber cadet retention?	46
4.7	To present an approach to cyber defence training that supports understanding for better governance of cyberpower effects	47
4.8	Limitations	48
5	Conclusion	49
5.1	Contributions	49
5.2	Future Research	52
6	References	54

Part 2

I. The Effect of Cyberpower on Institutional Development in Norway65

II. Socio-technical Communication: The Hybrid Space and the OLB Model for Science-based Cyber Eeducation.....88

III. Towards a Cognitive Agility Index: The Role of Metacognition in Human Computer Interaction103

IV. Development and Application of the Hybrid Space App for Measuring Cognitive Focus in Hybrid Contexts112

V. Slow Education and Cognitive Agility: Improving Military Cyber Cadet Cognitive Performance for Better Governance of Cyberpower125

VI. Cognitive Profiles and Education of Female Cyber Defence Operators147

VII. Cognisance as a Human Factor in Military Cyber Defence Education155

List of Figures

Figure 1.1 The Hybrid Space4

Figure 4.1 The OLB model as a procedure to communicate across The Hybrid Space40

Figure 4.2 Pedagogic path for OLB – a practice to reduce the cognitive cost of communication in The Hybrid Space40

Figure 4.3 Example of data collected with The Hybrid Space app43

List of Tables

Table 1.1 Research flow8

Table 4.1 Overview of articles and outlets38

Appendices

Appendix 1 Questionnaire utilized for Paper I85

PART 1

Chapter 1

Introduction

Cyberspace is an artificially constructed ever expanding computerised environment (NATO, 2020). Deterring threats and reducing an adversary's attack surface in this interconnected global infrastructure is complex and requires multiple levels of control. One such level is the human cyber operator. From a military perspective any performance advantage cyber operators can gain should be exploited (Gutzwiller et al., 2019; Thomson, 2019). At the cyber operator level, and in the context of this thesis, the term 'understand' relates to the ability to discover causal and associative relationships and the ability to explain these processes and situations. The term governance¹ refers to the way cyber operators attempt to impose a general framework of order and steer powerful effects through cyberspace by piloting their own cognitive processes.

Kuehl et al. (2009) see cyberpower as the capacity to use cyberspace to create advantage and influence events. In line with this definition, this doctoral thesis defines cyberpower as the capacity to influence tangible and intangible assets through digital means [see Paper I, p. 65]. The way this capacity is applied by cyber operators is understood as praxis; the use of a theory in a practical way (Hornby, 2010). Consequently, the art of *cyberpower praxis* is the way an individual accurately applies the theory, lessons and skills required to effectively conduct operations in cyberspace. To do this requires developing the cognitive competencies that support better understanding and self-governance. Formal education is one way to facilitate this. So too is regular practice and exposure to the relevant information as well as problem-oriented interaction with peers, leaders and cross domain experts.

To master the art of cyberpower praxis requires high levels of domain-specific knowledge, technical skills, and social intelligence (Thomson, 2019). It can be viewed as having the cognitive and practical skills to reflect on and act in a way that can

¹ The term governance in this thesis refers primarily to individual self-governance, i.e., as the ancient Greek philosopher Plato posited; to be one's own master. Or similarly how the political philosopher John Locke saw it; to exercise all necessary functions of cognitive self-discipline (Casson, 2011). This places less emphasis on governance structures, process and documentation and instead the focus is on factors that can support effective regulatory behaviours for performance. Section 2.5 (p. 19) in this thesis expands on the concept of governance and how it applies to this study.

transform thinking and action (Freire, 1996). This ability to change is underscored by cognitive flexibility (Feltovich et al., 1997; Spiro, 1988). At cyber operator level, the ability to steer own and adversarial actions - be they tangible, intangible or a combination of both - can be understood as self-governance occurring at lower levels in military hierarchies.

Cyber operations are part of modern warfare. The cyber domain is challenging military conventions relating to such things as leadership models, deterrence, information sharing and ultimately it may be changing the concept of war (Schroefl, 2020). Achieving good cyberpower praxis at cyber operator level is reliant upon education and training to further understanding and allow governance to develop as an individual skill for achieving better performance.

1.1 The broader context

In 2010, the political scientist Joseph Nye wrote that the “cyber universe is complex and well beyond anyone’s understanding” (p. 17). The Cisco Visual Networking Index (VNI) projected annual global IP traffic to nearly triple from 1.5 ZB per year in 2017, to reach 4.8 ZB per year by 2022 (Cisco, 2018). This presents an unfathomably vast surface area for activity. As much as this activity drives economic growth in areas such as social media, machine learning, AI, Big Data analytics, IoT, e-commerce, mobile payments, cloud computing, and e-health. It also presents increased risk for users and businesses in the form of cyber-attacks. It is unsurprising then that cybercriminal activity is assessed to be one of humanity's biggest challenges in the decades to come (Morgan, 2019).

Having grown up in an IT and media-rich environment it is generally agreed that the digital natives of ‘Generation Y’ (Kennedy et al., 2006), also known as the ‘net generation’ (Tapscott, 1998) born between 1980 and 1994, have developed a different set of attitudes and aptitudes (Wessels & Steenkamp, 2009). Generation Y and subsequently ‘Generation Z’ (born between 1997 and 2012) process information and think differently to their predecessors (Prensky, 2001). For this reason, when customisable and flexible learning paradigms that involve perspectives, real-world activities, emotional involvement, peer learning, interactive hands-on assignments, and experiential learning based practice (Wessels & Steenkamp, 2009) are combined with contemporary pedagogies focusing on developing cognitive and metacognitive skills, there is the potential to reveal pathways to improved cognitive flexibility, for performance and self-insight (see Papers III and IV in this thesis).

From a military perspective, this process is essential if personnel are to master the future operating environment that sees the constant spawning of new technologies and with-it greater expectations on operator and leader roles, tactics, techniques and procedures (see paper VII in this thesis). Increased interconnectedness, interdependency, and the need for coordination among actors add complexities, resulting in adaptations and workarounds (Koopman & Hoffman, 2003). It also requires that they engage systematically with reflection, build self-regulatory processes, self-efficacy and avoid reductive tendencies (Feltovich et al., 2004). Personnel who can mirror the dynamism of the complex developing hybrid landscape, will demonstrate qualities not constrained by institutional norms of military command, experience or rank. Instead their cognitive work will center on obtaining, applying, and communicating knowledge in the pursuit of shared goals under changing circumstances. These ideas are explored further in papers I, II, V & VII in this thesis.

1.2 The specific context

Technological developments to improve efficiency and effectiveness come at the cost of finding ways to strengthen the human-in-the-loop. The research articles in this thesis are a necessary step in furthering the study of how we approach building understanding and supporting ways to improve human performance in the cyber domain. This is necessary in order to better control the power phenomena that emerge and emanate from it. In previous work, the author and colleagues developed a theoretical framework for cognitive science in military cyberspace operations (Jøsok & Knox et al., 2016). This interdisciplinary contribution formed the foundation for this thesis. The article discusses the human as the interface between cyberspace and the physical domain, and the cognitive challenges this represents. The Hybrid Space conceptual framework (see Figure 1.1) is a visualisation of two orthogonal dimensions on which a person's cognitive focus can be located at a given time point. Cyber-physical and strategic-tactical factors - represented as dimensions on a Cartesian Plane - are constant variables for fast and slow decision-making in military cyberspace operations. This theoretical article highlights the demand for improved structure and content in modes of education and training for cyber-military personnel. The argument is grounded in the need for both enhanced and augmented understanding concerning the relationships between actions and consequence in cyberspace and the physical world. The perceived outcome is better understanding of the cognitive challenges facing those people charged with operating in, and leading military

cyberspace operations. The Hybrid Space frames a thinking and action space that requires cyber operators and cyber leaders to use a wide range of cognitive and metacognitive skills for improved performance in complex operations and operating environments that involve cyber as a component.

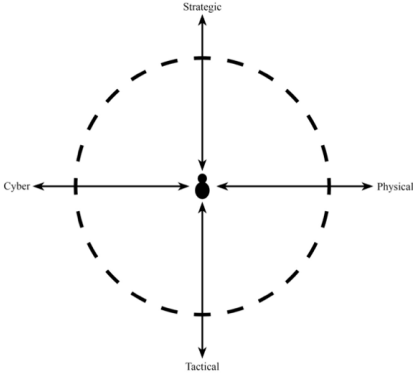


Figure 1.1: The Hybrid Space (Jøsok & Knox et al., 2016)

Cyberspace is a new military domain that is inherently part of all other military domains. As such it creates transformatory challenges as it pervades all aspects of military planning, operations and leadership (Dombrowski & Demchak, 2014). This creates tension for doctrine, education and training, as well as culture. The sensitive nature of conducting operations in cyberspace requires in-depth tactical savvy with an understanding of the strategic level factors that frame the operation (Jøsok & Knox et al., 2016). The role of a cyber operator is to not be constrained by these factors, nor by the technology. Accordingly, the cyber operator possesses high technical aptitude, is a creative problem solver, has a hacker mindset, enjoys manipulating complex systems and pushing technology in unintended ways (Conti & Raymond, 2011). Not all these are necessarily aligned with traditional military attitudes. However, a cyber operator may be expected to work in a highly collaborative way across domains, with operators from other disciplines, across nationalities and outside traditional hierarchies. This illustrates the vertical axis (tactical–strategic) in the Hybrid Space (Figure 1.1) and the shift to a more fluid, adaptive approach to command structures. Challenges to power-relations and organisational norms call for adaptive approaches (McChrystal, 2016). Problem solving and relation building based on cognitive agility rather than rigidity. A risk to this is the high cognitive load placed upon cyber operators resulting from the

information intensive work, leading to reduced communication impacting team performance (Champion et al., 2012).

Seeing cyberspace operations in the wider context is a responsibility of the cyber operator. They are required to appreciate physical world impacts and the consequence of actions, in-actions or incorrect attribution. The communication, information technology and other electronic systems, networks and their data, including those that are separated or independent, which process, store or transmit data have become weapons. Cyber cadets are trained to establish, operate through and defend in these systems. They are expected to do this in a demanding operating environment (FHS, 2020). The cyber operator should therefore be a resilient soldier with a good understanding of the tactical situation and the overall operational context outside of cyberspace. Thinking, deciding, and acting in highly complex technical operations with potentially strategic and global implications is standard procedure (Boleng et al., 2008). This translates to an appreciation for the diminishing distinction between the cyber domain and the physical domain (the horizontal axis of the Hybrid Space in Figure 1.1) regarding understanding how operations in cyberspace fit into military operations. An example of cyber operators applying cognitive agility in this context is the need to figure out how malware works. They will analyse the code. They may attempt to make sense of it individually and then come together as a collaborative team. They may share ideas and liaise across agencies. Critically, they may begin to look for indicators beyond the code. Here they focus attention on the geopolitical context in which the attack was taking place. Attempting to identify factors or indicators from the physical world may help scaffold understanding. This sensemaking and merging of clues to obtain situational awareness concerning the purpose and intent of the actor behind the malware requires cognitive agility. The operator implements an alternative mode of thinking revealing her ability/capacity to recognise the need to change in the context of the current linear thinking. When this occurs as a planned activity for problem-solving it demonstrates cognitive agility. That is, the ability to change the focus of attention between wide and narrow perspective for deep analysis whilst also not missing new information (Hutton & Turner, 2019).

Reflecting on the above roles and responsibilities a cyber operator has to know her own strengths and weakness (self-awareness), and be able to answer the question; “am I achieving the objective of the activity?” (self-regulation). These, as well as awareness and understanding of other key decision-makers are metacognitive skills. Metacognitive skills are what cognitive agility is reliant upon: the ability to orientate thinking effectively and appropriately to meet objectives with situational constraints

(Hutton et al., 2020). The cyber operator task profile requires self-governance and focus attention in both the vertical and horizontal dimensions of the Hybrid Space.

1.3 The research problem

This thesis aims to address the research problem of:

Identifying approaches to support performance among novice cyber operators.

Attempting to develop thinking skills that result in better actions among novice level military cyber cadets attending the Norwegian Defence Cyber Academy (NDCA) organized under the Norwegian Defence University College was the motivation. The cadets undergo a three and a half year programme combining a Bachelor of Engineering degree in telematics and practical military training. This explicit combination of required capabilities places high demands on cadets to focus on cyber as much as on other environmental factors (U.K. Ministry of Defence, 2015). With multiple competing task profiles comes increased cognitive demands. Demands such as these are further compounded when complex events in cyberspace are revealed and have complex physical world impacts. In this context, greater understanding and the ability to manage multiple simultaneous and often competing interactions is key to performance. These interactions may occur in cyberspace or in the physical world. They may involve friendly or enemy actors. They may be taking place in a tactical setting however the consequences could have strategic implications. This thesis aims to reveal ways to advance cognitive strategies and release the performance potential relating to self-governance. The role and responsibilities of cyber operators means their behaviours should be characterised by a clear understanding of the operation and the operating environment (the strategic goal and tactical frames); the ability to deploy the appropriate skills; knowledge, experience and judgement; unafraid to think independently; willing to question assumptions and established views; and be part of a supportive decision-making environment. The importance of self-governance can be illustrated in the example of a hierarchical convergence when a junior - but more domain knowledgeable - cyber operator may have to give a direct order to a senior decision maker as a consequence of his/her low cyber domain cognisance (see Paper II & Paper VII in this thesis). For this reason, to develop the necessary governance behaviours, cadets need to develop and apply context adaptive and flexible cognitive strategies founded on regulatory processes and situational self-efficacy (Hepler & Feltz, 2012; Judge et al., 2007; Stajkovic & Luthans, 1998).

Previous research conducted with colleagues at the NDCA regarding what the 'cyber soldiers need to know' (Lund et al., 2014), 'factors to affect improvement in cyber officer performance' and 'how coping strategies influence cyber task performance' (Helkala, et al., 2016a & b), as well as extended consultations with applied cognitive scientists are the key drivers behind this thesis.

1.4 Synopsis of research studies


This thesis details the effects of cyberpower and reveals novel concepts and approaches that can be applied to cyber cadet education and training to support better performance.

Paper I investigated ways in which the growing phenomenon of cyberpower impacts on institutional development in Norway. Specifically, it attempted to identify cross domain shared challenges. The type of institutional level cyber challenges that cyber operators will have to contribute to resolve. The research identified points of convergence and divergence across societal sectors and came with a series of recommendations capable of responding to existing and emerging cyber domain challenges. This study identified the need for investment in building the human factor skills and capacities necessary for managing the effects of cyberpower. Paper II followed on from this finding and took a cognitive engineering process and applied it to communication activities conducted by military personnel operating in the cyberspace domain. The Orientating, Locating and Bridging (OLB) model (Figure 4.2, p. 40) aims to prevent communication failures arising from individual differences driven by factors such as hierarchy, bias or effort. The model is based on The Hybrid Space framework (Figure 1.1, p. 4) and allows for the introduction of applied cognitive science into cyberspace domain education. The role of metacognition has been shown to be an important factor in performance. It was also identified as a key cognitive skill in Paper II. Consequently, Paper III aimed to investigate metacognition as a potential index of evaluating individual cognitive performance in cyberspace operations. This was achieved by measuring metacognitive abilities, understood as a cyber operators' subjective movements in The Hybrid Space. Data collection in Paper III involved rudimentary methods involving pen and paper. In order to make data entry less intrusive and feel more like an operational requirement, such as entering information into a battle log, a digital application was developed. Paper IV presents the development and application of a Hybrid Space App to measure cognitive focus. The app was able to help capture, visualize and analyse the cognitive focus of individuals and teams. This supported the function of mentors and leaders in their capacity to help

develop performance among novice cyber operators. The differing pedagogic approaches military instructors, civilian teachers and mentors take when educating cadets at NDCA has a decisive impact on how they perform. For this reason, Paper V introduces a Slow pedagogic approach that is adaptive and available to all educators with minimal impact on existing techniques. Central to Slow Education interventions is metacognitive skill enhancement. The study showed how combining Slow methods with psychological techniques has the potential to support cognitive performance among military cyber cadets. The uniqueness of the educational setting at the NDCA and how it impacts female cyber cadets was the focus of Paper VI. Anxiety, low self-efficacy, and maladaptive emotion regulation styles are all risk factors in academic underperformance. However, for a number of reasons these factors do not appear to contribute to females dropping out of education at the NDCA. Instead, as Paper VI shows, there are several factors and approaches that support and contribute to female retention and performance. Building on this, Paper VII presents an approach to cyber defence training that the author considers a priori to supporting a cyber operator’s ability to manage the effects of cyberpower. By applying a rigorous expert mentor model that is built into the design and architecture of a capstone Cyber Defence Exercise (CDX) the NDCA can preserve complexity during protracted periods of training for novice level cyber operators. The critical outcome is developing cadets understand function, their self-governance behaviours, as well as their wider domain cognisance.

Together the research studies in this thesis provide a theoretical and empirical grounding, as well as an inspiration for future research that aims to strengthen the pathway to mastering the art of cyberpower praxis.

Table 1.1 presents the flow of research in this thesis.

Title of thesis	Cyberpower praxis: A study of ways to Improve Understanding and Governance in the Cyber Domain
Research Focus	<i>Identifying approaches to support performance among novice cyber operators.</i>
	
Paper I Research question	<i>To what extent is cyberpower affecting institutional development in Norway?</i>
Key Findings	The research showed a pressing need for approaches that build collaboration capacities capable of facilitating better cooperation over time. Building human capacities through modes of education that focus on non-routine, higher order cognitive skills can support better performance.

The study established levels of understanding, concerns and demands placed on institutions relating to cyberpower. Paper I identified the shared need for behaviours and attitudes founded upon skills such as unstructured problem solving, critical thinking, learning and reasoning. To develop these skills in cyber operators requires approaches to education and training that develop psychological factors such as metacognitive skills and perspective-taking. Ensuring that these factors of self-governance behaviour contribute to safe and efficient communication lead to the subsequent study. Paper II aimed to prevent communication failures arising from individual differences driven by factors such as hierarchy, bias or effort.



Paper II Research question	<i>Can cognitive engineering be applied to communication activities in the cyber domain to improve performance?</i>
-----------------------------------	---

Key Findings	When co-constructing a shared mental model, communication partners should apply techniques to enhance situational awareness, information-processing resources such as working memory, cognitive flexibility, metacognitive awareness, and perspective-taking. The Hybrid Space framework (Figure 1.1) allows for the introduction of applied cognitive science as an approach to cyberspace domain education. With a tailored pedagogic approach that builds cognitive capacities (such as metacognitive awareness, perspective taking and adaptability), it is possible to take a cognitive engineering process and apply it to communication activities in cyber cadet education.
---------------------	---

In other domains, metacognitive awareness and regulation have been shown to be important factors in performance. Research on these human factors in the cyberspace domain is scarce. Paper III attempted to address this by investigating metacognition as a potential index of evaluating individual cognitive performance in cyberspace operations during a CDX.



Paper III Research question	<i>Is it possible to measure cognitive agility in cyber defence scenarios with The Hybrid Space framework?</i>
------------------------------------	--

Key Findings	Metacognitive strategies could explain Hybrid Space performance outcomes and support the development of a <i>Cognitive Agility Index</i> for cyber operators.
---------------------	---

After a review of the methodology used in Paper III and spurred on by the initial findings, a second round of data was collected. This time with a less intrusive method of collecting cognitive focus data. Paper IV introduces the Hybrid Space App as tool to capture, visualize and help analyse the cognitive focus of individuals and teams conducting a CDX.



Paper IV Research question	<i>To turn the Hybrid Space cognitive framework into an applied tool for measuring cognitive agility.</i>
-----------------------------------	---

Key Findings	Using the app gives researchers, mentors and leaders access to individual cadet cognitive focus, levels of control and effort. Combined with other data sources this information can shed light on how participants cognitively manoeuvre and focus to make sense of (understand) information emerging from cyber and physical domains.
---------------------	---

The next step was to see if the data collected via the app could be seen in relation to the intended outcomes of specific pedagogical educational interventions introduced to the educational platform at the NDCA. Constructivist pedagogic approaches and retrospective reports combined to support performance outcomes.



Paper V Research question	<i>Can Slow Education and training interventions designed to improve metacognitive skills support performance in cyber cadets.</i>
----------------------------------	--



Key Findings	Combining and applying novel, adaptive non-standards based pedagogic methods with psychological techniques suggests reflective pondering, self-regulation and metacognition as being associated with cognitive agility.
As the goal of Slow pedagogies is to improve high order thinking skills, such as reflective cognitions, then these findings and this approach can be seen as positive outcomes for supporting cyber operator performance. Education and training approaches that bolster personality, cognitions, and behaviour governance strategies can make a difference to well-being and consequently to retention during formal education. Paper VI looked at factors that may lead to academic underperformance in females at the NDCA and viewed results in the light of specific institutional practices and approaches.	
	
Paper VI Research question	<i>What are the protective and risk factors of the Norwegian Defence Cyber Academy in female cyber cadet retention?</i>
Key Findings	Some findings showed that female cyber cadets could be at risk of dropping out of the NDCA. Factors such as anxiety and maladaptive emotion regulation strategies as well as significantly less self-efficacy than all other groups tested.
Anxiety, low self-efficacy, and maladaptive emotion regulation styles are all risk factors in academic underperformance. However, these factors do not seem to contribute to females dropping out at the NDCA. This may be due to certain key institutional factors and approaches that promote stronger self-governance: mentoring, peer support, role-models, a positive culture of high performing female cadets. Paper VII ties together the learning and approaches described in the earlier research to support cyber cadet performance through increasing their levels of self-governance and domain understanding.	
	
Paper VII Research question	<i>To present an approach to cyber defence training that supports better cyber power praxis.</i>
Key Findings	An approach that applies a rigorous expert mentor model built into the design and architecture of a capstone CDX at the NDCA can lead to more efficient collaboration and communication. This occurs as it facilitates educational benefits based on insight, accurate self-perception, motivation and decreased team workloads. Approaches known to accelerate learning, scaffold performance and build domain cognisance through cognitive and metacognitive development can be applied to education and training techniques in the cyber domain. Although yet to be validated, this study provides the groundwork for future application and validation to support novice cyber operator performance.

Table 1.1 Research flow.

1.5 Results

The initial results of Paper I reflect an uncertain institutional landscape as a digital dependency vs. digital vulnerability paradox shapes values, rules and norms across instruments of power in Norway. There is a need to move understanding forward from the current state where cyberpower has relevance, but conflicting interests and value conflicts mean it is not yet a well categorized concept. The results showed that

cyberpower influences organisations differently depending upon their domain of interest. Critically though, the research showed a pressing need for new approaches that build collaboration capacities capable of facilitating better co-operation over time. Failure to do so is an opportunity lost. The OLB pedagogic approach (Figure 4.2) presented in Paper II is one vector to address the concerns raised in Paper I. Paper II revealed the potential to reduce the cognitive load and ease communication challenges in complex and critical cyberspace operations. Changes within educational institutions responsible for preparing future cyber operators, such as the NDCA, have the potential to improve how cyber operators conduct cyberpower praxis. As Paper II identified, education approaches that aim to develop metacognitive skills can support performance improvement among learners. The results of Paper III lead to an understanding that metacognition strategies could explain Hybrid Space performance outcomes and support the development of a *Cognitive Agility Index* for cyber operators. For example, an individual self-reported Total Distance Travelled in The Hybrid Space (HSDT) during one day of a CDX was predicted by metacognitive debugging strategies, defined as a regulation of cognition used to correct comprehension and performance errors, and self-regulation.

To build on this study and improve how Hybrid Space data can be collected the Hybrid Space app was developed in Paper IV. The app demonstrated ease of use for real-time analysis opportunities, as well as a reliable data collection, computation and visualization tool. In the context of education and training, the app gave insight into so far unexplored cognitive dynamics on individual and group level performance. Using the app in a later CDX meant more data became available. The results of Paper V show how combining and applying a novel, adaptive non-standards based pedagogic method with psychological techniques suggests reflective pondering, self-regulation and metacognition as being associated with cognitive agility. Reflective pondering and self-regulation were significant variables that influenced Hybrid Space movements for Distance Travelled and X-axis movements and almost significant for Y-axis movements. Self-regulation was the only significant predictor for distance travelled, X-axis and Y-axis movements.

The results of Paper VI lead to the discussion that several psychological factors could be putting female cyber cadets at the NDCA at risk of dropping out. The female cadets reported higher anxiety and maladaptive emotion regulation strategies than both fellow male cyber cadets as well as when compared to age and gender matched controls. They also reported significantly less self-efficacy compared to male counterparts and age and gender matched controls. Factors such as these can be mitigated through embedding critical processes such as metacognition, self-

regulation, coping strategies, communication, mentoring, and shared mental modelling into educational practice. The results of Paper VII lead to the conclusion that Slow Education methods and a rigorous approach to mentoring are fundamental to enabling the advancement of domain cognisance among cyber cadets. Together they open space for insight, accurate self-perception, motivation and decreased team workload.

1.6 Implications

There are a number of key implications resulting from this research. The thesis proposes approaches and suggests methods that are suitable to support cyber operator performance. The studies add valuable content to the development of career structures, guidelines for recruiting and selection, education and training. In the cyber domain, these are all areas that lack the maturity levels of other military domains (Dawson & Thomson, 2018; Sobiesk et al., 2015).

Military and civilian activities are becoming more intertwined and dependent upon each other due to the emergence of the cyber domain. Complex value chains, cloud services, deterring and defending against shared threats from state and non-state actors are just some examples of dependencies. In Norway, the Armed Forces alone is unable to protect society from cyber-attacks (Kampenæs & Røislien, 2019). For this reason, approaches that support how cyber operators are educated to govern the effects of cyberpower need not be limited to the Defence sector. The conclusions offered in this thesis are equally applicable to civilian institutions. They too are attempting to define approaches to performance improvement for cyber operators. Protecting critical infrastructure, personal privacy protection and sharing science-based educational approaches to support performance and decision-making in cyberspace is a shared responsibility. The small-state context of Norway means multiple agencies and institutions attempting to access talent from the same pool. Much of the engineering and computer science education at the NDCA is mirrored and taught in conjunction with civilian education institutions. Academically equivalent students attending civilian universities end up working in the field of cyber within either the civilian or military sectors. It is therefore prudent and viable to extrapolate the findings from this thesis and apply them to a wider population. The outcome would be a societal cyber workforce that is able to recognise in each other factors such as experience, knowledge, mental models of how the world works, self-awareness, techniques of disciplined thinking, creative thinking, collaborative engagement, proactivity and responsiveness (Hutton & Turner, 2019).

Significantly this research highlights the role metacognition has in improving domain understanding and governance competence. This thesis makes a case for metacognition being taught and measured as an approach to support better cyberpower praxis. Metacognitive skill development can enable individuals to be aware of their cognitive processes and appropriateness and their ability to redirect/re-adjust them. The outcome is thinking and behaviour can change if necessary. The implication then is the importance of cognitive agility as a requisite for self-governance if personnel are to manage the demands of cyberpower. This reasoning is based upon the psychological characteristics of cognitive agility being openness to alternatives, flexibility to respond with alternative solutions, ability to adapt attentional focus between wide and narrow perspectives (Hutton & Turner, 2019).

1.7 Structure of Thesis

The thesis is structured in two parts. Part 1 contains five chapters. Chapter 1 is the introduction. This includes the broader and specific context, the research problem, a synopsis of the research, the results and implications. Chapter 2 presents the necessary theory to understand the contributions to this thesis. This includes: cyberpower, cyberspace domain, the NDCA, the cyber operator, leadership, governance, metacognition, Slow education, mentoring and cognitive agility. Chapter 3 presents the research design and methods. This includes the philosophical approach, methods and validity, the research ethics relating to this project and a description of the cyber defence exercise central in this project. Chapter 4 presents a summary of the work completed for this thesis, including an analysis and synthesis i.e., showing the relationship and bridge between the seven research articles, as well as a final section concerning limitations. Chapter 5 covers the conclusion and includes the contributions of this research and future work. In Part 2 of the thesis the seven research papers, constituting the main body of the thesis are found.

Background

This research takes a national level issue, that of finding ways to improve understanding and governance in the cyberspace domain; and attempts to identify and recommend solutions from a military perspective that can occur at a lower level of praxis. Building cognitive capacities and drawing attention to modes of education that focus on nonroutine thinking and high order cognitive skills can lead to military cyber personnel with developed aptitude and mental agility. This advances necessary technical and domain competencies, as well as the application of metacognitive skills to avoid the natural inclination towards for example cognitive rigidity (Feltovich, Spierer & Coulson, 1997) or invoking a 'knowledge shield' to preserve simplistic understanding (Feltovich et al., 2001). Instead cognitive flexibility is promoted (Klein & Baxter, 2006 & 2009; and see Spiro & Feltovich et al. 2019 for a summary of work conducted on Cognitive Flexibility Theory). Thus, making people responsible for managing own cyberpower effects better, and more resilient to effects that intend to obfuscate knowledge or exert reflexive control (Thomas, 2011).

This human centered approach highlights the increased importance of psychological factors such as metacognitive skills and perspective-taking. When managing or making tactical cyberspace judgements or decisions that can have strategic implications inside and outside the cyberspace domain, these factors can help attempts to communicate, mitigate risks and avoid judgement errors. Depending on the actor's motivation and goal, cyberpower and how it integrates with other instruments of power (Kuehl, 2009) to create impacts, can pose novel challenges for military forces and their decision makers (Libicki, 2016).

The remainder of this chapter concentrates on aspects which are of special importance to this study. Furnishing an overview of the key theories and central concepts.

2.1 As indicated above, **cyberpower** effects are domain agnostic, meaning they cannot be considered as known only to one specific or unique cyberspace domain. Cyberspace enables the delivery of cyberpower effects to wherever an actor, whether it is a State, institution or individual, has needs and goals. The author defines cyberpower as *the capability to influence tangible and intangible assets through digital means* (Paper I). For example, a state may utilise cyberspace to deliver cyberpower effects

with the goal of projecting its political will over another state, or in an attempt to gain advantage through espionage (Libicki, 2017; Ikeda, 2019; Inkster, 2016; Krekel et al., 2014). A state may also, overtly or covertly, apply cyberpower over its own population to exert forms of control and censorship (Greitens, 2013; Ognyanova, 2019).

At an institutional level, cyberpower can be understood as the outcome of the application of advanced software to remain competitive in for example global financial markets. However, the risk of being part of a global banking cyber-commons, where all transactions occur in cyberspace, can lead to disasters such as the Bangladesh Bank cyber heist in 2016 that saw hackers infiltrate the system and transfer almost \$1 Billion through the established global banking networks almost undetected (Mallet & Chilkoti, 2016). A second example is the digitalization of the healthcare sector. This process is unleashing enormous potential in terms of cost-effectiveness, decentralization and the availability of specialist services and expertise in the form of eHealth, mHealth, teleHealth, telemedicine. Applied cyberpower effects can leverage these services for universal health coverage (WHO, 2016). Conversely, in the hands of an adversarial actor, cyberpower effects can exploit critical vulnerabilities leading to debilitating impacts on physical and economic security or public health or safety (Department of Homeland Security, 2019).

From a military perspective cyberpower effects can enable a military force to set the conditions for or determine the outcome of a conflict. The operational application of cyberpower can impose limitations on an opponent (Siedler, 2016) as a stabilizing effect, or it can provide the decisive blow through a cyberspace operation (Kallberg & Thuraisingham, 2013; Lewis, 2015). Military cyberspace operations may be conducted in a conventional or non-conventional way. They may be conducted as a stand-alone operation or in coordination with kinetic operations as part of a cyber-enabled battlefield (Martelle, 2019). The tactical and operational choices will be dependent upon the nature of the conflict, the intended target, and not least legal and ethical factors (Barrett, 2013; Schmitt, 2011, 2017). Lastly, an actor will assess the cost of using a sophisticated cyber weapon given the one-shot-nature of specially developed, highly bespoke malware and the risk of it being available 'in the wild'. In the wild, can mean in adversarial hands wreaking havoc (Cobb & Lee, 2014; Doffman, 2019).

Responding to the growing influence of cyberpower effects involves developing techniques and methods to counter the threats, as well as address and mitigate known and unknown vulnerabilities. Successful defence measures should be based upon proactive cross-sector and multi-domain shared mental models framed by hybrid approaches to education and training. Defence against cyberpower should not

be passive, as it requires a wide range of defensive actions transformed into a proactive attitude (Neag, 2018).

2.2 In July 2016 NATO Allied Heads of State and Government agreed to declare cyberspace a domain of operations. Just as NATO defends itself in the air, on land and at sea, the cyberspace domain must also be effectively defended in order to improve NATO's ability to protect and conduct its missions and operations (NATO, 2016a). The **cyberspace domain** is reshaping modern conflict particularly as the laws of cyberspace exist only in the Tallinn Manual; a non-binding guideline (Schmitt, 2017). The cyberspace domain is in a state of constant expansion and is therefore subject to more rapid change than other military domains (Nye, 2010). No longer is warfare limited by geography. Digitization and the expansion of cyberspace means conflict can take place anywhere, anytime, by any actor with a motivation, at greater speed, as well as covertly with populations as the non-kinetic target. Meaning national defence no longer rests with the government and state military apparatus. Consequently, the cyberspace domain presents profound challenges for how militaries prepare and counter threats that cross geo-legal boundaries and require cross-sectoral collaboration (Ministry of Justice and Public Security, 2017; Waterhouse, 2013). This situation is described in Paper I of this thesis when presenting a Norwegian institutional landscape that is ill-prepared for systematic and targeted cyber-attacks by an adversary. The implication is that, although considered an advanced democratic nation with strong institutions, the institutional framework is already destabilized enough that a sustained strategic cyber-attack against it could lead to a decisive outcome for the attacker. This is somewhat contra to the strategic cyberwar theory presented by Kallberg (2016) which posits that the "theory's predictive power is strongest when applied to targeting theocracies, authoritarian regimes, and dysfunctional experimental democracies, and their common tenet of weak institutions" (p. 114).

The NATO declaration of cyberspace as a warfighting domain was followed by NATO Cyber Defence Pledge (2016b). This committed Allies to enhancing cyber defence as a matter of priority. The Allies agreed to honour their responsibility to improve resilience and their ability to respond quickly and effectively to cyber-attacks. Points four and five in the pledge specify education as part of national defence efforts.

2.3 At the **NDCA** the educational platform for the Bachelor of Engineering degree is built on a hybrid conflation of quasi military training and an approved variant of the national framework for engineering education (Regjeringen, 2016). The NDCA

graduates officer cadets and specialists to all services within the Norwegian Armed Forces. The academy offers a holistic learning environment where civilian academics and military teachers work in collaboration. This collective approach allows for cadet exposure to stimulating overlapping and diverse perspectives. Graduates from the NDCA acquire similar basic technical competencies as their civilian equivalents graduating from universities. Both educational paths are designed to prepare graduates to operate with technical tools that are developing faster than business leaders, policy makers and planners can keep up with. The NDCA education encourages a proactive mindset. Standing still means falling behind as the techniques, skills and tools required for operations in cyberspace rapidly evolve. Further, from a defensive perspective, the adversary has an alternate ethical play book and a set of objectives and capabilities that may be invisible in cyberspace until they are manifest in the physical world.

With the right cognitive competencies, cyber cadets can adapt rapidly after graduation to their chosen operating environment and perform. However, some receiving units must invest heavily in additional external courses as well as internal training programmes to bring their new employees up to the required operating standard. This has an effect on operational capability as it drains human and fiscal resources. There is also the added risk to retention as the novice cyber operator earns competencies and qualification that are also in high demand and well rewarded in the private sector. This situation is not unique to the Norwegian Defence (see Hardinsen et al., 2019; Lynch, 2018).

What is the right curriculum/education model for cyber military personnel is debatable and well published (e.g., Dawson & Thomson, 2018; Fulp, 2003; Sobiesk et al., 2015; Spidalieri & McArdle, 2016). What is indisputable is the impossible individual task of remaining up-to-speed with the knowledge, skills and abilities required for proficiency in this new domain. The readiness problem, how to move from novice to proficient operator in a shorter period of time, has been the subject of research and success in other domains such as sport (e.g. Williams et al., 2002), law enforcement (e.g. Ward et al., 2011) and nursing (e.g. Whyte et al., 2009). Methods that are founded in cognitive engineering and techniques known to accelerate learning inspired this thesis (e.g. Hoffman et al., 2009; Klein, 1998; Ward et al., 2013). Significantly they encouraged the applied interventions attempting to develop adaptive skills within the framework of the existing curriculum at the NDCA. This meant introducing mentoring processes and re-thinking teaching methods to scaffold cyber *hard skills* and the critical human *people skills* at individual and team level. Developing cognitive focus and greater overall domain cognisance is understood as a

contributing factor to intrinsic motivation to work on hard problems and building mental toughness. The latter has been described as a defining feature of what it takes for an individual to achieve the highest levels of proficiency (Ward et al., 2013).

2.4 Future battlefields and hybrid warfare requires new skill sets characterized by new and better cognitive competencies (Hutton & Turner, 2019; Schroefl, 2020; U.K. MOD, 2015). Untapped cognitive potential could be unlocked through **leadership** processes focusing on judgement and improved understanding across hierarchies. Traditional military leadership norms relating to command, control and obedience can restrict performance potential as they micromanage, over-specify and create knowledge barriers. This is not an effective way to show trust and give purpose to subordinates (Lopez, 2017). This thesis argues for approaches to develop future cyber operators and cyber leaders with the skills and vision to achieve objectives in spite of future demands from an increasingly Volatile, Uncertain, Complex, Ambiguous (VUCA) operating environment (Mackey, 1992).

As an expansion on this perspective, one can observe the predominance of hierarchical and 'heroic' ideals of desirable leadership qualities within most military contexts. Although taught that leadership principles and behaviours such as; leading by example; know yourself and seek self-improvement; encourage confidence in the team; set the example; and strive for team goals, are the criteria of being a good leader (Sandhurst, 2015; West Point, 2019). Exercising these actions and allowing subordinates to thrive under these conditions is often lacking. It has been argued that hierarchical systems and engrained cultures can hinder performance (Greer et al., 2018). In the case of leadership in the domain of cyberspace this may also be true due to the nature of the work, as well as the characteristics of those doing the job (Conti & Raymond, 2011). Cyber operators and specialists can feel disenfranchised by the cultural dominance of this heroic view of leadership and may suffer from low self-efficacy and confidence issues. How these people cope and react can transpire in different ways (in this thesis, Papers II, V and VI explore this in more detail). Some may not take opportunities because they feel unworthy of being there even though they should, while others may overcompensate and 'front-up' (Pedler, 2011). Fronting-up can be a good thing and demonstrates determination and courage. However, there is a risk that those who choose to take this option may have a poor judgement of their own abilities (Kruger & Dunning, 1999). A little knowledge can be dangerous. Whereas a high level of accuracy in one's self-judgment is related to better performance in a given task (Bandura, 1986 & 1997). Those who have more knowledge may choose to remain out of the light - meaning they are more aware of

what they don't know - and be reluctant to front-up. When considering team workload demands that may influence cyber operator and team performance, the context above is likely to have negative effects. A recent study found that team workload demands - in a novice cyber team - can be associated with, and in certain operationalisations predict movements in the aforementioned Hybrid Space (Lugo et al., 2017). Meaning either greater movements, or no movements in The Hybrid Space may represent cognitive strain among novice level operators in tactical cyber units. Thus, hindering team cognition and performance. Papers III, V and VI in this thesis expand on this.

2.5 Governance is a term that can be used to categorise how cyber operators steer powerful effects through cyberspace by piloting their own cognitive processes. Cognitive agility performance is supported by better understanding of their domain and the ability to govern own behaviours. The desired outcome is improved cyberpower praxis: a cyber operator's ability to manage the effects of cyberpower.

Usage of governance in this context can be seen in the example of why banks failed so spectacularly in 2008/9. It has been argued that the answer lies in individual and group behaviours; the effectiveness of governance systems (no matter how good structurally they were) was undermined by poor and unethical behaviours (Almond Tree, 2020; Szyszka, 2011). For cyber operators to avoid psychological traps that can lead to, for example communication errors, they should have well developed self-governance based upon educated and trained cognitive capacities that are known to support performance.

The cyberspace domain presents real-world shared problems. Cyberpower effects can influence technology as well as the human-in-the-loop. The effects are often ill-structured and difficult to predict. Therefore, gaining and accurately communicating experiences across related fields may encourage a more open, holistic and flexible way of building robust modes of managing novelty. This may also advance competence levels in hierarchies as cyber operators are better able to contribute to for example institutional process and policy development.

Dealing with novelty presents special cognitive challenges and may appear to be an impossible task, particularly in the mind of a novice. As Spiro et al. (2019) wrote: "How can we come to know what we do not already know?" (p. 956). Yet if novice cyber operators can improve their understanding of their psychological traits that influence their behaviours and decision making, i.e., if they engage in processes that teach them to monitor and control their learning (Zimmerman, 2001). Then they become more adaptable (Ward et al., 2018). They develop their cognitive repertoire

and readiness to process novelty with an adaptive worldview rather than a reductive one (Spiro et al., 2019). They become better at assessing task demands, evaluating their knowledge and skills, can plan approaches, monitor progress and make appropriate situational adjustments (Ambrose et al., 2010). Consequently, we see how metacognitive skills can improve the individuals' situational awareness and thus increase the chance of better performance; as improved situational sense-making leads to better situational leadership (Northouse, 2015). Meaning the ability to lead and direct themselves, based upon enhanced understanding and piloting of own behaviour as a result of better situational awareness.

Situational leadership is defined as leaders able to diagnose the demands of their situation (Schermermore, 1997). In this thesis, governance differs from this perspective due to its suitability to go beyond diagnosing, to actually making things happen in praxis. The chaos, complexity and hybridisation of modern warfare (Bousquet, 2009) means adaptive modes of governance praxis may be more legitimate than relying on traditional forms of leadership as who can govern, comes ahead of who can lead (Kallberg, 2016, p. 108 on Waldo, 1948). This perspective is relevant in today's context where cyberspace domain expertise often resides lower in the hierarchy.

Seeing governance of cyberpower effects this way recognizes a legitimate effort to make events in and through cyberspace happen in a productive direction. It allows for governance to be understood as a practice capable of occurring at lower levels in military hierarchies, as it meshes both the process and the [human] performance concepts of governance (Hyden, 2004). At this level, good governance is more representative of the techniques required to: "...impose a general framework of order on the disorder, to prescribe the general flow of action rather than to try to control each event" (FMFM1, 1989).

2.6 Metacognition is a central theory (metacognitive theory) and concept (the actual processes) in this thesis. Where cognition describes the act of thinking, metacognition describes the act of thinking about thinking. This research proceeds from the idea that personnel conducting operations in cyberspace need to consciously move their momentary cognition within The Hybrid Space for optimal performance. For an individual to localize themselves in The Hybrid Space requires high levels of metacognitive skills: knowledge of one's abilities, situational awareness, and behaviour regulation strategies (Flavell, 1979). As well as metacognitive awareness of one's cognitive processes: planning, monitoring and evaluations (Metcalfe & Shimamura, 1994). In sum, this can be described as having an accurate judgment of

one's own performance levels. At this level of consciousness, judgment and appropriate initiation of change of cognition or action/behaviour becomes optimal. An individual's ability to understand, control, and manipulate one's cognitive processes' (Meichenbaum, 1985) is the art of being aware of and exerting control over one's thinking to achieve present goals. Through planning, monitoring, and evaluating one's cognitions, emotions and behaviours, and actively adapting to the situational demands one can support encoding experiences for consolidation into long-term memory, as it integrates both cognitive and emotional processes.

Metacognitive knowledge is renewed through reflection when the situation has ended, which then has a top-down influence on future behaviours. On the other hand, metacognitive experiences are feelings and cognitions that arise during the situation and include judgements, emotion regulation strategies and self-efficacy. Self-efficacy is supported by metacognitive skills and can be thought of as beliefs about one's own capabilities to learn or perform (Bandura, 1986, 1993, 1997). Levels of belief influence an individual's self-evaluating process and their ability to exercise control in their current environment (Bandura, 1997) i.e. their ability to self-govern; foresee, appraise own capability and weigh up consequences based upon improved understanding and reflection. Metacognitive skills support personal agency, allowing for greater freedom to exercise options and adapt own behaviours (Bandura, 1986). As this thesis shows, metacognitive development is dependent on metacognitive instruction that incorporates three principles, all of which can be taught and mentored:

- Embedding metacognitive instruction in the content matter to allow for consolidation into long-term memory.
- Informing learners about the usefulness of metacognitive activities to make them exert the initial extra effort.
- Prolonged periods of training to guarantee the smooth and maintained application of metacognitive activity.

This strategic instruction approach has been associated with better metacognitive development and necessitates a transactional educational setting (Schraw & Gutierrez, 2015).

2.7 Slow Education is a transactional and adaptive non-standards-based approach to education. Categorized alongside Slow Movement philosophies and rooted in Student-centered education methodologies (see Weimer, 2002) where self-expression, interests and capacities are prioritised (Holt, 2002). This pedagogical method is intended to facilitate students gaining situational self-efficacy and empowerment as

they engage in reflective practice and critical thinking (Bandura, 1997). This approach can lead learners to: "...displaying richer intertextual connections [...] and meanings beyond prescribed lesson content..." (Jenson, 2016, p. 35).

A Slow pedagogy approach was chosen as it aligned with practices and values already being incorporated into faculty development at the NDCA. This meant that teachers and trainers were willing to use the Slow pedagogy as a frame to incorporate alternative approaches that inspired and motivated them. The choice of approach occurred in dialogue with teachers, rather than the researcher imposing an approach on them. Slow pedagogy was chosen ahead of other pedagogies for its adaptability. Pedagogies such as Dialogue pedagogy for acquiring knowledge through communicative interactions (see Freire, 1970; Wells, 1999), Cooperative Learning for positive interdependence and individual accountability (see Cooper, 1990), and Critical pedagogy for awakening of the critical consciousness (see Giroux, 1989) can all be incorporated within the Slow frame. Examples of teaching approaches that fall within these categories and used by teachers at the NDCA are Problem-Based Learning (see Boud & Feletti, 1998), Self-Directed Learning (see Knowles, 1975) and Flipped-classroom (see Gilboy et al., 2015). Importantly the Slow pedagogy also recognises that direct instruction to convey certain concepts may be the most effective way (Grenier in Wilby, 2019). The key cognitive factors that drove decision-making relating to the choice of pedagogy and teaching approach was where possible replace direct transmission of knowledge with collaborative and individual procedures promoting critical thinking and reflection (Shaw et al., 2013; Schon, 1987).

Slow techniques are suitable for creating and deepening knowledge into the context of the cyberspace domain and operations as they have the capability to aid orientation and learner understanding (Hannafin, 2010). This is possible as learners are engaged in a variety of processes to monitor and control their learning (Zimmerman, 2001). Being cognizant of exercising metacognitive skills builds authentic real-world knowledge through the process of assessment, evaluation, planning, application, monitoring, and reflection (Ambrose et al., 2010). This can be of particular use when dealing with geo-political factors, legal and ethical limitations/frames, strategic guidance, governance mechanisms, and risk analysis based on tactical, operational and strategic cyberpower effects.

By practicing newly acquired knowledge and skills in as close to authentic training environments, such as attack and defence cyber exercises, teachers can establish naturalistic professional contexts that allow for 'slow' learnt skills to manifest in the form of improved praxis (Klein, 1998; Ward et al., 2013). Slow pedagogical approaches, combined with traditional types of instruction methods for engineer and

military studies, can create a robust evidence-based approach to learning. This trajectory for educating cyber military personnel into the context of cyberpower and cyberspace operations has the potential to secure expanded domain understanding and self-governance. Currently though, this is a novel approach and lacks qualitative and quantitative research to validate its applicability in relation to task and learner demands in a cyberspace operations context.

Slow methods tend to be seen as messy, inefficient and are rejected in favor of mechanistic, one-size-fits-all time and resource friendly instructional methods (Wright, 2014). What the Slow approach offers however is an alternative to the standards and content-focused and institutionally-centered information delivery method. Evidence has shown that Constructivist pedagogical approaches are capable of accelerating learning and improving performance by building deeper knowledge grounded in metacognitive strategies such as reflective practice and self-regulation (Kember et al., 2000; Panadero, 2017; Piaget, 1964; Zimmerman, 2000). For this to be successful there is a need for learner scaffolding.

2.8 Education and training for conducting operations in cyberspace requires individual, collaborative and cooperative human input through cognitive processes that can for example scaffold learning for sensemaking and decision-making (Chi et al., 2001). This demands significant human effort from the learner and facilitator/teacher. Even though technology can be developed, taught and applied to support defensive cyberspace operations, until we reach a time when these technologies become an actual part of the human body, connected at a mental level (Gálik & Tolnaiová, 2019), there is still the pressing need to harden the human-in-the-loop through proficiency development. One approach that has proven highly successful is **mentoring** (Bloom, 1984; Hoffman et al., 2017; Ward et al., 2013). Mentoring can support learning processes as it stimulates reflection on behaviour, dealing with received feedback and how to apply learning strategies (Annink & van Mook, 2019). When a learner, supported by an expert mentor, monitors, debugs and evaluates what is learned, then metacognition develops (Nietfeld & Schraw, 2002). A key mentor function is to give precise feedback. Correctly receiving this feedback can facilitate metacognitive skill development as it allows the recipient to reflect upon how cognition affects behaviour. Besides facilitating metacognitive accuracy, mentoring and expert-mentors feedback also has the potential to increase motivation that consequently triggers the amount of effort an individual invests into a challenging (difficult and/or tiring) task (Ward et al., 2013). For example, the cognitive effort it takes to communicate and make-decisions in a complex socio-technical system (see

Paper II in this thesis). Evidence from pedagogical research indicates a clear association between expert mentoring and academic performance (Rhodes, 2008), self-regulatory skills (Wentzel, 2019), satisfaction levels, and lower stress and anxiety levels (Crisp & Cruz, 2009).

2.9 Cognitive Agility defines cognitive focus movements in a VUCA or hybrid environment. It can be understood as an individuals' metacognitive strategy proficiency to meet objectives with situational constraints (Hutton et al., 2020). Cognitive agility is reliant upon metacognitive skills. These skills need to be orientated to improve cybepower praxis in human computer interaction. Operations where the task characteristics require effective coordination between multiple agents and asset types (human, technical, tangible and intangible) to build understanding will likely benefit from self-governing individuals with openness, flexibility, and adaptability: the psychological characteristics of cognitive agility (Hutton & Turner, 2019).

Evaluating performance in cyber tasks requires more than 'capture-the-flag' type competitions/exercises (Bashir et al., 2017; Fink et al., 2013). Yet what is good performance in cyber tasks is still under discussion (Buchler et al., 2016; Forsythe et al., 2013; Thomson, 2019). Increasingly the importance of developing human abilities - ways of thinking adaptively - to grasp threat complexities, understand and minimize consequences, and reduce of communication failures in routine and nonroutine situations should be taken into consideration when attempting to evaluate and improve performance (Klein, 1998; Ward, 2018). The Hybrid Space framework was used as a tool to measure cognitive focus movements, aka. cognitive agility, with the aim of relating these movements to metacognitive strategies during training and educational programmes at the NDCA.

Design and Methods

The applied nature and real-world complexity of this field means this research is interdisciplinary. Research into understanding and learning what the effects of cyberpower are, and how to manage the role of the human in cyberspace operations is still in the early stages. From the outset, there were no existing theoretical frameworks in the literature encompassing these research questions, or answers to the applied nature of this research. Hypothetic deductions lead to discoveries that require a problem-solving approach. This meant reaching out across disciplines and applying well validated methods, in for example psychology, to this new field of applied research.

Through a mixed methods design including qualitative, quantitative and theoretical approaches, this thesis takes a broad societal perspective, an organizational perspective, a team and an individual perspective. The methodology has introduced and revealed models and modes of educational strategies suited to support cyberpower praxis. These modes have been applied, reasoned and assessed. In sum, this theoretical and applied research methodology has presented an approach for how to improve human factor prospects of achieving a holistic approach to managing negative cyberpower effects, whilst also taking advantage of the opportunities cyberpower presents.

3.1 Philosophical approach

A methodology provides a piece of research with its philosophy, the values and assumptions which drive the rationale for the investigation as well as the standards that will be utilised for interpreting findings (Almalki, 2016). Mixed approaches must complement each other in order that the information that is generated is pertinent to the subject of the study and follow in a logical progression. Due to the novelty and rapid developments of the cyberspace domain, this thesis uses a mixed methods approach. Mixed methods support the inclusion of different theoretical designs to give a holistic picture of the studied phenomena. This can include quantitative and qualitative approaches that are flexible and adaptable for research (Almalki, 2016). The benefits of using differing approaches come in the form of width for understanding a domain, as well as simultaneously giving an in-depth focus, as opposed to one approach alone. Mixed methods allow researchers to have insight that is provided by

both quantitative and qualitative collection methods. Greene et al., (1989, in Almalki 2016) describes five distinct reasons for integrating quantitative and qualitative data. This triangulation *converges* and *corroborates* the findings from each perspective, both subjective experiences (qualitative) and observational data (quantitative). This happens through *complementary* actions, such as elaborating and enhancing processes through subjective interpretations, and confirming these in more objective observations. This *developmental* iterative process helps develop new methods for data collection that enable coverage of all aspects of the research question. It also *initiates* the discoveries of contradictions or inconsistencies within the data sets which can result in hypothesis reformulation or opening new avenues of inquiry. For this thesis, nomothetic, phenomenological and observational approaches are used.

Nomothetic approaches define phenomena in terms of general principles (Porpora, 1983) and allow for model building but they can be incomplete. Nomothetic approaches allow for use of empirical data collection to support and disconfirm theoretical modelling. This is a staple principle of the research proposed by Popper (1963) in his term 'falsification'. The nomothetic approach allows for the building and testing of theories and conceptual frameworks such as those presented in this thesis and encourages replication. This requires the researcher to have an overview and in depth understanding of not only the domain in focus (in this case the cyberspace domain), but also of the domains that are related and integrated within the new domain (i.e., military structures, and human factors in performance). Building models based on previous research helps validate conceptual frameworks, especially since one model cannot capture all the facets. These missing and/or incorrect aspects will be addressed in future research. One of this thesis's main outcomes was to establish a theoretical foundation from which research can grow.

Theory building and modelling not only comes from previous research, it also has to arise from the experiences of people within the domain. Therefore, phenomenological approaches are also used. Phenomenological approaches provide descriptions and interpretation of cultural and social structure experiences at an individual level. This approach is qualitative in nature and requires the researcher to be reflective of their influence with the participants. Qualitative research is defined as "any kind of research that produces findings not arrived at by means of statistical procedures or other means of quantification" (Strauss & Corbin, 1990, p. 17) and can involve several approaches such as interviews, narrative reviews, and retrospective

reports among others. The focus of qualitative data is to gather an understanding of experiences of the people involved and exploration of phenomena.

This research used semi-structured interviews and cued retrospective reports for qualitative data. Semi-structured interviews help elicit information through predetermined questions and follow-up questions. Follow-up questions help explore responses so that the interview becomes a conversation where both interviewer and interviewee can explore the subjects they feel are important (Longhurst, 2003). Retrospective reports are when participants are instructed to report the thoughts they had while they were working on a task immediately after completing it and result in verbal protocols of cognitive processes that happen in short-term and long-term memory (Van Gog et al., 2005). Retrospective reports have been widely debated (see Miller et al., 1997 for review) but using cued retrospective reporting has been shown to generate better verbal reports (Van Gog et al., 2005). Cued retrospective reporting instructs participants to report retrospectively on the basis of a record of observations or intermediate products of their problem-solving process, which leads to less distortions of thoughts than plain retrospective reporting thus increasing the validity of the data (Van Gog et al., 2005). Alone, interviews and cued retrospective reports have problems with validity, but triangulation of methods helps mitigate this (Golafshani, 2003).

3.2 Validity in qualitative research

While traditional understanding of validity in research has been a focus in quantitative research, qualitative research has been behind in defining how validity pertains to qualitative methods (Flick, 2018). Flick identifies that validity has to encompass how the data was produced and presented. Validity in qualitative research has thus been expanded to include eight specific focuses (Tracy, 2010, p. 840): (1) worthy topic, (2) rich rigor, (3) sincerity, (4) credibility, (5) resonance, (6) significant contribution, (7) ethics, and (8) meaningful coherence. The following summarises each focus area with respect to studies in this thesis:

3.2.1 The topic of this thesis is **worthy** due to its relevance in creating safe behaviours that reflect and meet the rapid development of technologies in all facets of daily life. The Introduction and Background sections of this thesis defined and described the challenges advancing technologies brings to individuals and society. Cyber security should be an ingrained attitude and activity at individual, organisational and institutional level. Achieving this is a universal challenge. For this reason, this thesis

is relevant, timely, and significant as approaches for supporting better performance in cyberspace are in demand.

3.2.2 Rich rigor involves a rich complexity of information that arises from a “requisite variety” (Weick, 2007, p.16) of sources. The variety of studies in this thesis and requisite number of theoretical constructs, contexts, and samples helped develop adaptive tools. These were based upon discoveries initially made during qualitative analyses in Paper I. The qualitative research in this thesis was informed from expert accounts (Paper I). This led to the discovery of relevant factors that could be explored further (Paper II), operationalised for experimental testing (Paper III) and subsequently development into hypothetical constructs that were tested (Paper V).

3.2.3 Sincerity within qualitative studies is defined as “research is marked by honesty and transparency about the researcher’s biases, goals, and foibles as well as about how these played a role in the methods, joys, and mistakes of the research” (Weick, 2007, p. 842). This is shown through self-reflexivity of one’s own involvement in the research and its transparency. Throughout this project the researcher understood his role as part of the research, and the risk power relationships can play during the data collection process. Continuous dialogue with participants and fellow researchers helped ensure inevitable power imbalances did not negatively influence the validity of the findings. This was supported by education, training and guidance the researcher received (Patton, 2005). Regular reflection (asking “does my participation as a researcher increase demand characteristics?”) and introspection (asking “why am I doing this?”) helped the researcher understand his position and influence. To avoid any distortions in data analysis driven by for example either overestimation or underestimation of selective perceptions and bias (Patton, 2005), this research included iterative discussions with other researchers within the multidisciplinary teams. These discussions included the interpretations and meaning of the results, what Flick (2018) deems procedural validity (discussed below in section 3.2.7).

As this research was conducted in a multidisciplinary team (psychologists, applied practitioners, educators, stakeholders) this allowed for the reflection processes to be multifaceted. This is reflected in the theoretical Papers I & VII and lead to educational developments (Paper II, V & VII). The multidisciplinary approach helped inform the researcher. Regular calibrating, discussions and insight, lead to

understanding and knowledge development. This made the transparency of the research open for discussions and inclusive of differing views.

3.2.4 Guba and Lincoln (1994) state that good qualitative research must be dependable through providing reliable, replicable, consistent, and accurate descriptions (Golafshani, 2003). This is achieved through practices including thick description, triangulation or crystallization, multivocality and partiality. Thick description provides in-depth accounts that can explain, in detail, situational aspects (Weick, 2007). The interviews and retrospective reports are a triangulation approach within the qualitative approach. By using more than one method, systematic biases from data analysis are reduced, thus increasing the validity of the findings (crystallization). Alongside this qualitative triangulation, the addition of quantitative data further decreases the researcher's biases, but also increases the validity of the findings. Multivocality and member reflections, i.e. the inclusion of other viewpoints and experiences, helped the researcher and collaborators develop educational approaches. Importantly, for the purpose of **credibility**, the different approaches (qualitative and quantitative) included feedback from experts, participants and stakeholders (Lindlof & Taylor, 2017). Reliability can be increased through dialogue where the research findings and the understandings of the participants being studied are involved. Including the cyber operators in discussions and giving space to their reflections enhanced qualitative credibility. This method provided deeper and richer analyses based on everyone's experience. These reflections are not a research finding per se, but an opportunity for collaboration and reflexive elaboration which informed the approaches to support performance development in this thesis.

3.2.5 Resonance refers to the "research's ability to meaningfully reverberate and affect an audience" (Weick, 2007, p. 844). This is achieved through aesthetic merit, evocative writing, formal generalizations and transferability. The researcher has attempted to achieve aesthetic merit by using clear language that is understandable to the audience without unnecessary jargon or overly technical explanations. The findings, both from the quantitative and qualitative approaches are taken from naturalistic environments. This supports the generalizability and transferability to other populations and context (Pfaffenberger, 1992) domains which lead to improved practice (Stake & Trumbull, 1982).

3.2.6 Tracy (2010) states that qualitative research needs to provide a **significant contribution** to novel or developing domains on four levels: (1) theoretical, (2) heuristic, (3) practical, and (4) methodological significance (Tracy, 2010). Due to the

lack of human factors research within the cyber domain (Gutzwiller et al., 2015), this thesis develops theoretically significant contributions by developing new hypothetical constructs developed from theoretical perspectives in other domains. Heuristic significance is achieved by this research developing future inquiries. This thesis also demonstrates practical significance by supplying information that helps develop coping strategies (Tracy, 2010) and help to inform decision-making at various levels (i.e. individual, social, policymaker; Sadler & Zeidler, 2005). The varying works in this thesis also provide the development of novel hypothetical constructs making the study methodologically significant.

3.2.7 The **ethical** focus of qualitative research validity spans dilemmas faced by researchers concerning design, field relations when in contact with people, data handling, analysis and presentation. Additionally, the ethics of how the data may be fed back to the field all contribute to the ethical soundness of a project (Flick, 2007). Throughout this project cautions were taken to ensure ethical guidelines were followed. Informed consent and anonymity were constant priorities. Considering the current position, and potential future roles of participants, privacy and confidentiality was essential. This was ethically correct as well as respectful to participants. In the case of Paper IV, it was imperative to write in a respectful and sensitive manner. This was necessary to avoid participants' incorrect interpretation, as well the reader in the final product, of what 'at risk of dropping out due to individual cognitive styles' means.

Data accuracy and interpretation is a leading principle in qualitative research (Flick, 2007). This was key to Paper I to ensure the researcher interpreted the relationship correctly between sectors, at the top governance level, and how this translates to institutional development needs - particularly aggregating it to relate to the role cyber operators have in this context. The research plan was to avoid framing questions that would lead respondents to tell the investigator what they wanted from cyber operators.

Considering the researcher's position as an employee at the NDCA lead to reflections about how this could obscure a naïve position. This potential dilemma was reduced due to the researcher not having an engineering/cyber operations background, as well coming from a different cultural background than Norway.

The aspect of procedural ethics is integrated in each of the paper's literature reviews and discussions. Procedural ethics encompasses: (a) the relation of what is being observed and how it is related to societal levels, (b) the relation between the observer and participants, (c) the issue of perspective, (d) the role of the readers of the research, and (e) how the research is presented (Flick, 2018). The researcher reflected

around these aspects of procedural ethics through continual dialogue with all involved persons (i.e. research team, experts, participants), maintaining objectivity by founding the studies on validated theoretical approaches and the collected data, and presenting objective conclusions through the iterative process of communication with all people involved while interpreting theories and data.

3.2.8 Tracy (2010) summarizes **meaningful coherence** when research “(a) achieve their stated purpose; (b) accomplish what they espouse to be about; (c) use methods and representation practices that partner well with espoused theories and paradigms; and (d) attentively interconnect literature reviewed with research foci, methods, and findings” (p. 848) are part of the communicative validity of the research (Flick, 2018). These four points are discussed throughout the thesis and specifically addressed in the general discussion and conclusion.

3.3 Quantitative approaches

Quantitative research is regarded as a deductive approach with objective observations where data can be reduced to smaller, more manageable processes. This allows for hypothesis testing and replication. Allowing also for bigger theories to be tested through specific hypotheses where conclusions and generalizations can be made. This is done through observations and statistical analysis of the data. Quantitative data allows for a more objective understanding of phenomena. This research incorporated both correlational and comparative analyses. While correlational analysis cannot establish causation, it does give an indication of the relationship between variables where more rigorous methods can establish causality. Comparative analyses allow for the identification of specific factors within groups that may separate them from others.

3.4 Validity in quantitative research

Whereas validity and reliability in qualitative approaches are focused on researcher qualities, validity and reliability within quantitative data is focused on theoretical validity, measurement instrumentation, design and analysis. Behaviours are operationalized into hypothetical constructs in order to observe and measure them. For these operationalisations to be valid, instrumentation undergoes several checks for reliability and validity. All behaviour measurement instruments used for the quantitative approaches have previously undergone stringent validation procedures and have been used in several domains.

This research also incorporated naturalistic settings over laboratory settings due to the nature of the domain studied. Socio-technical domains incorporate human computer interactions while in social settings (i.e., teams). Experimental laboratory settings are applicable when one wishes to manipulate one or few variables and see their influence on an outcome variable. This approach may give high internal validity, where control over manipulated variables and control over extraneous variables is high, but it cannot be generalized to populations. Naturalistic design sees the participants in their settings and observes for outcomes. While this approach may have low internal validity, it is high in ecological validity, therefore the findings can be generalized to other populations. This is done through representative design (Brunswick, 1956; Dhami et al., 2004), where both the participants and the situations with which they are faced are representative of the populations to which researchers claim to generalize results.

All quantitative behaviour trait tools used in Paper III, IV, V, VI have been validated in previous studies and tested for reliability. Reliability indices have been reported in the published articles, where appropriate. Hypothetical constructs (as detailed in Paper III) that were developed for this research, were operationalised and validated through a series of experiments (see Lugo, 2018 for review).

Situational behaviour measurements for The Hybrid Space App used validated Hybrid Space constructs (Lugo, 2018). Additionally, the use of adapted visual analogue scales (sliders), validated in other domains (Price, McGrath, Rafii, & Buckingham, 1983), supported a reliable and less intrusive way of capturing situational data. Procedures in using The Hybrid Space app can be found in (Lugo et al., 2020).

3.5 Challenges and benefits of mixed methods and triangulation

The greatest challenge is for the researcher to have insight in both quantitative and qualitative approaches, as well as which method to use at each stage. However, using mixed methods allows the researcher to balance out weaknesses provided from each approach and allows a greater degree of understanding (Flick, 2018). This happens since both subjective experiences and objective observations are taken in the discussion (Almalki, 2016; Golafshani, 2003).

Where qualitative limitations involve limited sample observations, cultural aspects (temporal, social), and selection (Patton, 2005), quantitative data can help counter these limitations. But when quantitative data lacks in-depth understanding of experiences, and is mechanical in nature, then qualitative approaches help to enrich

more superficial data. Taken together, these two approaches reduce issues in validity that would be prominent in one approach alone (Almalki, 2016). While different forms of mixed methods can be used (i.e., embedded, explanatory, exploratory), this research uses the approach to form a more robust answer to the overarching research question via triangulation (Flick, 2018). This is opposed to individual papers using a mixed methods approach. The different methods complement each other with distinct data. This allows for efficient designs where the data can be integrated for analysis and interpretation.

Onwuegbuzie and Johnson (2006) have identified two problems with mixed methods: the problem of representation and the problem of integration. But these problems can be minimized by *legitimizing* the use of both approaches through different types of legitimation. These include sample integration, weakness minimization, conversion, and multiple validities (see Onwuegbuzie & Johnson, 2006 for descriptions). These legitimisations allow for meta-inferences that cannot be achieved by using one approach alone. Legitimation of mixed methods is a process that is "...analytical, social, aesthetic, emic, etic, political, and ethical..." (Onwuegbuzie & Johnson, 2006, p.60). Combining both approaches in a representative design, allows for some generalization of the findings (Dhami et al., 2004).

3.6 Cyber Defence Exercise (CDX)

Much of the applied research activity, observations, data gathering and validation for this thesis was conducted during an annual capstone CDX held at the NDCA. The CDX is designed to train cyber cadets with relatively low levels of proficiency in conducting military cyberspace operations. During the exercise the cadets operate in independent, but not opposing, cyber protection teams. The CDX contributes to developing the human and technical competencies necessary to govern the effects of own and adversaries' cyberpower capabilities.

This thesis is an outcome and representation of almost a decade spent by the author modifying and developing the pedagogic architecture of the NDCA CDX. The CDX is structured in such a way that cadets' task-specific cognitive status is in focus (Hoffman & Ward, 2015). Learning, understanding and communication techniques are scaffolded to ensure better praxis at team and individual level. A key tenet is not to oversimplify and instead preserve the complexity (Ward et al., 2018) and have the cadets learn at the *zone of proximal development* (Vygotsky, 1978). To achieve this the CDX has an adaptive tailor-made mentor model that aims to meet the cadet's current needs, be they domain-specific knowledge, technical skills or developing their social

intelligence. This is different to gamified CDX designs that see friendly cyber teams (blue teams) competing against an adversary (red team) for points, prestige and bragging rights. It is also different to capture-the-flag type exercises that are often more reliant upon one extremely talented individual or dependent upon socioeconomic status (Thomson, 2019). Neither of the above necessarily ensure task/case balancing, or the mechanisms for accelerating learning, aiding professional development, and supporting personal growth (Petushek et al., 2019; see also Paper VII in this thesis).

The NDCA CDX allows for a safe-to-fail environment. This is achieved by way of balanced incremental adversarial threat modelling, a bespoke virtualized cyber-range facility, mentor rigour, daily after-action-reviews, and cadet retrospective reporting. The exercise is unclassified allowing for easier access to participants and data collection. During the NDCA CDX there are four teams consisting of approximately 8-10 cadets per team. The duration of the exercise is five days with incidents running from 08:00 to 22:00 each day.

The week leading up to the exercise is an intense period of refresher training and competence building. The preparation week is cognitively demanding as cadets are expected to [re]-master already learnt skills, acquire and apply new skills and then learn how to integrate them with existing retained knowledge. As well as grasping the hybrid scenario that includes cyber- legal and ethical, forensic, and multi-domain elements; they must establish and rehearse team structures, allocate tasks and roles and settle routines. Achieving this is essential for their praxis as they are expected to be cognizant of strategic considerations, give operational guidance and take tactical level decisions from the moment the exercise starts. Challenging the cadets in this way by increasing the complexity of tasks and exercises is to match the professional context (Annink & van Mook, 2019; Klein, 1998; Ward et al., 2013). Being cognitively and practically 'ready' to operate at the edge of their knowledge, skills and abilities during the CDX is key to transforming thinking and action.

3.7 Research ethics

The project was based on unclassified and unrestricted data. At no stage during the project was the researcher exposed to sensitive or restricted information. The methodology required that the researcher talked and interviewed people from various organisations in Norway. The subject of cyberpower raised sensitive issues among respondents and in Paper 1 required the researcher anonymize individuals. The information the researcher received was handled with sensitivity and in line with regulations of the Norwegian Centre for Research Data.

During CDXs responsible and authorized personnel from the Norwegian Defence executed procedures that are illegal if they were to be conducted outside of a controlled cyber-range environment. Such practices were well planned, prepared and rehearsed prior to implementation. The NDCA CDX is an annual exercise conducted in accordance with common and approved military guidelines for exercising and training in Norway. Joining the exercise to collect data meant falling into line with ethical rules and guidelines for military education in Norway.

Data were collected by observation and elicited from cadets attending the NDCA. The researcher ensured that the cadets signed consent forms and were informed that they had the option to withdraw from the research participation at any stage without any disadvantages for them. The project was approved and registered with the Norway Authority for Data Protection (NSD; project number 43901).

Summary of Work

This chapter presents a summary of the work done for this thesis. Table 4.1 formulates the papers included in this thesis showing the year, type of outlet, title and outlet. Each paper is summarized, starting with the research question, followed by a summary, analysis and bridge to the next published paper. The overarching question this project aimed to answer was:

“Identifying approaches to support performance among novice cyber operators.”

Attempting to improve thinking and actions among novice level cyber operators in situations affected by the growing influence of cyberpower meant investigating individual processes occurring in a hierarchical system. These individuals are the front line in cyber operations and therefore have the most to learn when it comes to managing cyberpower effects. When this is understood, paths to improved leadership models and better cyberpower praxis can be introduced to educational platforms, across sectors.

To support the overarching research question, each research paper in this thesis had a separate research question, hypothesis or goal. Each contribution had a separate aim that intended to ground the study further, whilst also building towards the next step of the project. The seven research papers that constitute the main contribution of this thesis are:

- I. Knox, B. J. (2018). **The Effect of Cyberpower on Institutional Development in Norway.** *Frontiers in Psychology*, 9, 717.
- II. Knox, B. J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Ødegaard, T., Lugo, R. G., and Sütterlin, S. (2018). **Socio-technical Communication: The Hybrid Space and the OLB Model for Science-Based Cyber Education.** *Military Psychology*, 30(4), 350-359.
- III. Knox, B. J., Lugo R. G., Jøsok, Ø., Helkala, K., Sütterlin, S. (2017). **Towards a Cognitive Agility Index: The Role of Metacognition in Human Computer Interaction.** In: Stephanidis C. (eds) HCI International 2017. Communications in Computer and Information Science, 713, 330-338, Springer, Cham.
- IV. 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: Schmorow D., Fidopiastis C. (eds) Augmented

Cognition: Intelligent Technologies. AC 2018. Lecture Notes in Computer Science, 10915. 369-382, Springer, Cham.

- V. Knox, B J., Lugo, R. G., Helkala, K., and Sütterlin, S. (2019). **Slow Education and Cognitive Agility: Improving Military Cyber Cadet Cognitive Performance for Better Governance of Cyberpower.** *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 9(1), 48-66.
- VI. Lugo, R. G., Firth-Clark, A., Knox, B. J., Jøsok, Ø., Helkala, K., Sütterlin, S. (2019). **Cognitive Profiles and Education of Female Cyber Defence Operators.** In: Schmorow D., Fidopiastis C. (eds) *Augmented Cognition. HCII 2019. Lecture Notes in Computer Science, 11580, 563-572, Springer, Cham.*
- VII. Knox, B. J, Lugo, R., Sütterlin, S. (2019). **Cognisance as a Human Factor in Military Cyber Defence Education,** Proceedings of The 14th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems.

Paper	Year	Type	Title	Outlet
I	2018	Journal (Level 2)	<i>The Effect of Cyberpower on Institutional Development in Norway.</i>	Frontiers in Psychology
II	2018	Journal (Level 1)	<i>Socio-technical communication: the hybrid space and the OLB model for science-based cyber education.</i>	Military Psychology
III	2017	Book Chapter (Level 1)	<i>Towards a cognitive agility index: the role of metacognition in human computer interaction.</i>	Communications in Computer and Information Science (CCIS, volume 713)
IV	2018	Book Chapter (Level 1)	<i>Development and application of the hybrid space app for measuring cognitive focus in hybrid contexts.</i>	Lecture Notes in Computer Science (LNCS, volume 10915)
V	2019	Journal (Level 1)	<i>Slow Education and Cognitive Agility: Improving Military Cyber Cadet Cognitive Performance for Better Governance of Cyberpower.</i>	International Journal of Cyber Warfare & Terrorism

VI	2019	Book Chapter (Level 1)	<i>Cognitive Profiles and Education of Female Cyber Defence Operators.</i>	Lecture Notes in Computer Science (LNCS, volume 11580)
VII	2019	Conference proceedings (Level 1)	<i>Cognisance as a Human Factor in Military Cyber Defence Education.</i>	Lecture notes in IFAC Human-Machine Systems

Table 4.1: Overview of articles and outlets

4.1 The Effect of Cyberpower on Institutional Development in Norway.

Research Question:

To what extent is cyberpower affecting institutional development in Norway?

The aim of **Paper I** was to conduct an initial thematic analysis of qualitative data. This enabled an initial empirical investigation of the ways in which the growing phenomenon of cyberpower - defined as using cyberspace for advantage and influence - impacts on institutional development in Norway. The purpose was to open space for discussion regarding why rapid developments arising from digitalization are transforming the way individuals, organizations, institutions and states behave, relate and make decisions. It was important to include data from across the institutional spectrum in order to gather a broader understanding of the key issues and where tensions lie. Military and civilian defensive cyberspace operations share many of the same characteristics as they seek the same outcome: to counter and limit the negative effects of cyberpower, preserve the ability to use the defended cyberspace and ensure the right cyberspace conditions enabling own mission assurance. For this reason, the institutions chosen were political, military, economic, social, informational, infrastructure and diplomatic (Operations, 2013).

Summary: Due to concerns of bias it was important to establish if earlier assumptions and research conducted at the NDCA was domain specific or if the effects of cyberpower were impacting other institutions and their cyberpower praxis.

The research findings reflected an uncertain institutional landscape as a digital dependency vs. digital vulnerability paradox shapes values, rules and norms across instruments of power in Norway. This suggests that organizations in Norway are in a

survival-mode that is blocking collaboration. This occurs as national governance systems, human capacity and cyberpower effects lack synergy.

Analysis: This lack of synergy makes for an uneasy arena where complexity, contestation and emerging challenges frame institutional development. To improve long-term prospects of governing cyberpower effects requires a cross-sectorial conflation of time and human resources. This means: a) consciously taking steps to merge organizational and institutional boundaries through expressive innovative collaborations that foster a shared and holistic agenda, b) further research to build a richer understanding of the term cyberpower from different perspectives, c) investment in building the human factor skills and capacities necessary for the co-creation of new models and strategies for managing the effects of cyberpower.

Synthesis (and bridge to Paper II): This final point of investment in building the human factor skills and capacities was crucial to the direction of this project. Through the analysis of the data it was possible to see that management of cyberpower is a shared development activity and attitude founded upon skills such as unstructured problem solving, critical thinking, learning and reasoning. To succeed would require building human capacities through modes of education that focus on non-routine, higher order cognitive skills.

The Hybrid Space framework (Figure 1.1) provides a blueprint for describing the cognitive and behavioural constraints for maneuvering between socio-technical and cyber-physical systems whilst cooperating, coordinating or competing with accompanying cognitive styles in the chain of command.

4.2 Socio-technical Communication: The Hybrid Space and the OLB Model for Science-based Cyber Education.

Research Question:

Can cognitive engineering be applied to communication activities in the cyber domain to improve performance?

The aim of **Paper II** was to produce a theoretical article taking a cognitive engineering approach and applying it to The Hybrid Space framework. The Orientating, Locating and Bridging (OLB) model aims to prevent communication failures arising from individual differences driven by factors such as hierarchy, bias or effort. Based on the

educational principles of the NDCA, this paper discusses the required skillsets and knowledge in which cyber cadets are trained and taught, how these refer to the theoretical framework of The Hybrid Space, and the key principles of communication as defined in cognitive engineering.

Summary: The study found that it is possible to take a cognitive engineering process and apply it to communication activities conducted by military personnel operating in the cyberspace domain. When co-constructing a shared mental model, communication partners should apply techniques to enhance situational awareness, information-processing resources such as working memory, cognitive flexibility, metacognitive awareness, and perspective-taking. The Hybrid Space framework (Figure 1.1) allows for the introduction of applied cognitive science into cyberspace domain education. The OLB model is based on this framework and dissects maneuvering within The Hybrid Space into three core phases (see Figure 4.1). The educational implications are illustrated in Figure 4.2.

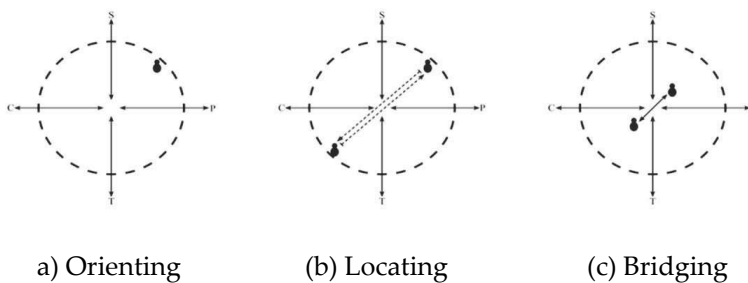


Figure 4.1. The OLB model as a procedure to communicate across The Hybrid Space (S-strategic, T-tactical, P-physical, C-cyber). (a) Orienting. (b) Locating. (c) Bridging.

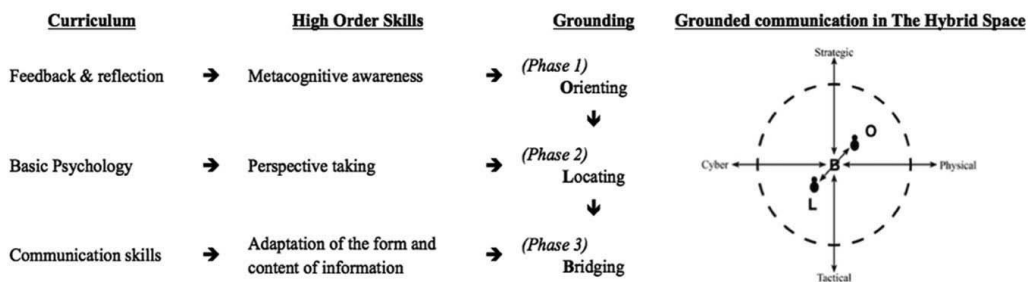


Figure 4.2. Pedagogic path for OLB – a practice to reduce the cognitive cost of communication in The Hybrid Space.

Analysis: Taking a pedagogic approach (Figure 4.2) to OLB in cyber education can potentially reduce the cognitive load and ease communication challenges in complex and critical cyberspace operations. This knowledge can easily be applied to civilian applications of cyberspace, such as protection of critical infrastructure, personal privacy protection and informing educators in how to enhance performance and decision-making in the cyberspace domain.

To improve cyberpower praxis will require transformative actions at educational institutions. A simple start-point is for educators and trainers to implement a systematic and pedagogic approach to developing metacognitive skills among learners/participants.

Synthesis: (and bridge to Paper III): Research on human factors in the cyberspace domain is lacking. It was therefore a logical progression to build on the pressing need to develop the human-in-the-loop, and higher order cognitive skills for better performance in the cyberspace domain. Metacognitive awareness and regulation have been shown to be important factors in performance, but research integrating metacognitive strategies in socio-technical systems is scarce.

4.3 Towards a Cognitive Agility Index: The Role of Metacognition in Human Computer Interaction.

Research Question:

Is it possible to measure cognitive agility in cyber defence scenarios with The Hybrid Space framework?

The aim of **Paper III** was to conduct a quantitative and applied practice study looking at data collected from the NDCA during a CDX. This study aimed to investigate metacognition as a potential index of evaluating individual cognitive performance in cyberspace operations. Cyber military cadets were tested to see how metacognitive awareness and regulation influenced performance in The Hybrid Space conceptual framework (Figure 1.1). This was achieved by measuring metacognitive abilities, understood as a cyber operators' subjective movements in The Hybrid Space. Data for this paper was gathered via questionnaires and pen and paper self-report.

Summary: Metacognition could predict movement in The Hybrid Space, but not for Y-axis movements. Y-axis movements may be dependent on fundamental cognition (i.e., rumination, worry, and self-efficacy) that may better explain vertical manoeuvring. Total Distance Travelled in The Hybrid Space (HSDT) was predicted by metacognitive debugging strategies, defined as a regulation of cognition used to correct comprehension and performance errors, and self-regulation. Evaluative metacognitive regulatory behaviours predicted X-axis movements, and along with triggering behaviours, searching for solutions, and implementing new strategies was associated with more quadrant changes.

Analysis: Metacognitive strategies could explain Hybrid Space performance outcomes and support the development of a *Cognitive Agility Index* for cyber operators. Future research and training programs for cyber personnel may well benefit from incorporating metacognition as performance measurement outcome, and in training to help index development and performance over time.

Synthesis (and Bridge to Paper IV): The findings from Paper III indicate impulsive cognitive movement due to the sample group acting without conscious thought. This is typical for people who have not undergone formal educational programmes of metacognitive learning.

To build on this initial study, participants needed to undergo metacognitive training and experience greater exposure to metacognitive learning. There was also the need for a less intrusive method of collecting cognitive focus data. To achieve this, specific teaching interventions were initiated and implemented, and a Hybrid Space application was developed.

4.4 Development and Application of The Hybrid Space App for Measuring Cognitive Focus in Hybrid Contexts.

Research Question:

To turn the Hybrid Space cognitive framework into an applied tool for measuring cognitive agility.

The aim of **Paper IV** was to introduce The Hybrid Space app. This application was designed and applied for collecting and analysing individual cognitive focus data when military cyber cadets were engaging in cyber defence tasks during a four-day

CDX at the NDCA. This paper details the motivation, how The Hybrid Space can be used as a tool for measuring cognitive focus, and the development of the data collection self-report software. Developing this software made data collection and handling more efficient compared to the pen & paper process applied in paper III. The software includes a real-time visual representation of the data. This is useful for interpretation, data-point integration and allows Exercise Control (EXCON) and mentors greater situational awareness.

Summary: The Hybrid Space app was able to help capture, visualize and analyse the cognitive focus of individuals and teams operating in hybrid contexts. In a real-time analysis, this gives researchers, mentors and leaders access to individual cognitive focus, levels of control, or where they put in effort. Compared with the EXCON knowledge of scenario developments and task requirements, this data can shed light on how participants cognitively manoeuvre and focus to make sense of information emerging from cyber and physical domains. Figure 4.3 is a snapshot of one participant’s cognitive manoeuvre in The Hybrid Space, as well as that individuals reported feeling of ‘control’ and ‘effort’, at the time of marking their cognitive location.

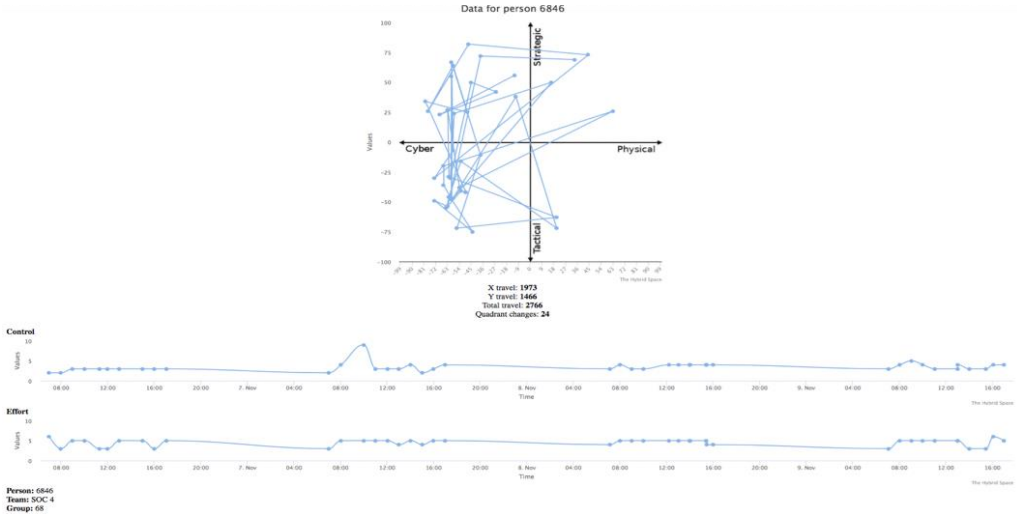


Figure. 4.3. Example of data collected with The Hybrid Space app

Analysis: The Hybrid Space app demonstrated ease of use for real-time analysis opportunities, as well as a reliable data collection, computation and visualization tool. In the context of education and training, the app can give insight into so far unexplored cognitive dynamics on individual and group level performance. From an EXCON perspective, the data might be useful for observing cognitive focus during the course of an exercise. The software can also be used for debriefing and/or as a complementary tool for conducting Cognitive Task Analysis (CTA) (for further reading about CTA see Hoffman and Militello, 2009) after a training cycle is completed. Further research can be conducted applying statistical analysis of The Hybrid Space movements with data from other inventories measuring i.e., self-regulation, metacognitive awareness or other constructs known to support cross domain performance. Such combinations of data can shed light on beneficial cognitive traits and competencies supporting agile manoeuvre in The Hybrid Space. Over time, and in combination with valid performance measures, further research can produce knowledge about cognitive skills that are beneficial for developing self-governance and understanding when operating in hybrid contexts.

Synthesis (and Bridge to Paper V): The data collected during the CDX, where The Hybrid Space app was deployed, was able to be analysed with the use of the same method and operationalisations for measuring performance as presented in paper III. If the results could be seen in relation to the intended outcomes of specific pedagogical educational interventions, designed to promote metacognition skills. Then it could be possible to form an argument that Slow Education approaches are able to support cognitive agility, for understanding and self-governance in a military cyberspace context.

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

Research Question:

Can slow education and training interventions designed to improve metacognitive skills support performance in cyber cadets.

The aim of Paper V was to conduct a quantitative study and applied practice review looking at how a Slow Education approach has the potential to improve cognitive

performance among military cyber cadets. Slow techniques, based on three principles (metacognitive instruction, metacognitive activities and prolonged periods of training) were applied to 37 cyber cadets during a three-year bachelor program at the NDCA. The quantitative data for this study was gathered during a two-week CDX with the use of The Hybrid Space app.

Summary: Combining and applying a novel, adaptive non-standards based pedagogic method with psychological techniques suggests reflective pondering, self-regulation and metacognition as being associated with cognitive agility. Reflective pondering and self-regulation were significant variables that influenced Hybrid Space movements for Distance Travelled and X-axis movements and almost significant for Y-axis movements. Self-regulation was the only significant predictor for distance travelled, X-axis and Y-axis movements.

Analysis: This study is the first to provide descriptive data on measures of cognitive performance in cyber defence scenarios. These data suggest that Slow Education interventions, capable of improving learners' cognitive repertoire, may help support good governance in military cyberspace operations and utilisation of cyberpower. Specifically, the cognitive strategies of self-regulation and reflective pondering correlated with cognitive agility, measured as movements in The Hybrid Space. As the goal of Slow Education methods is to improve high order thinking skills, such as reflective cognitions, then these findings can be seen as positive outcomes for measuring performance.

Synthesis (and Bridge to Paper VI): Data being analysed in a separate study relating to gender differences in military exercises revealed interesting results concerning female cadets at the NDCA. Grounding the findings in the context of this thesis adds a level of validity to this applied approach. Paper VI is the outcome of this research collaboration.

4.6 Cognitive Profiles and Education of Female Cyber Defence Operators.

Research Question:

What are the protective and risk factors of the Norwegian Defence Cyber Academy in female cyber cadet retention?

The aim of **Paper VI** was a qualitative analysis of psychological factors tested on participants from the NDCA and controlled with age and gender matched non-technical students from Inland Norway University of Applied Sciences (INN). This research focused on assessing the educational setting of the NDCA, its factors in promoting female student retention during their Bachelor of Engineering program and profiling female officer cadets to see if any differences in personality, cognitions, and behaviour strategies exist between male and female cadets.

Summary: The results showed that female cyber cadets score as other related fields (engineering) and as their male counterparts do in cognitive styles (field independence/dependence). The female cyber cadets did though have some findings that could put them at risk of dropping out of schooling. They reported higher anxiety and maladaptive emotion regulation strategies than both fellow male cyber cadets as well as when compared to age and gender matched controls. They also reported significantly less self-efficacy than all other groups.

Analysis: Anxiety, low self-efficacy, and maladaptive emotion regulation styles are all risk factors in academic underperformance. But these factors do not seem to contribute to drop-outs at the NDCA. This may be due to qualitative factors of the institution such as mentoring in military and academic fields, small class sizes, individualization catering for specific needs, peer-support to share the academic burden meaning individual and team workload demands can be more easily overcome, female role models in uniform, and a culture of high performing female cadets and teachers breaking down gender barriers in military contexts.

Synthesis (and Bridge to Paper VII): Over the course of the project, the goal of developing the 'understand function' (U.K. MOD, 2015) for better governance of cyberpower effects has been an ever-present theme. Paper VII ties together the learning and the applied approach taken to improve cyber cadet performance through increasing their levels of self and domain understanding.

4.7 Cognisance as a Human Factor in Military Cyber Defence Education.

Research Aim:

To present an approach to cyber defence training that supports better cyberpower praxis

The aim of **Paper VII** was a theoretical paper that describes the approach taken by the NDCA during their annual CDX. As a tool for efficient training, and grounded in the authors learning and research, a mentoring concept was developed and implemented. The concept was operationalised and involved the production and analysis of cyber defence retrospective timelines. This was achieved by the cadets in collaboration with expert and practitioner (highly proficient) level mentors. The retrospective timelines differentiate between performance relevant hard- and soft-skills and leads progressively towards an alignment of team, individual, and the expert mentors' judgment of performance.

Summary: Findings from this empirical study, observations and learning from applied research settings, show how Slow Education methods and mentoring are fundamental to enabling the advancement of domain cognisance among cyber cadets.

The identified cognitive-psychological predictors of performance (that have been written up in Papers I, II, III, V, VI and published in earlier co-authored articles by the researcher: see for example Helkala et al., 2016a & 2016b; Lugo et al., 2016 & 2017) for learning success of future cyber operators, are deeply embedded into educational practice at the NDCA. They include critical processes such as metacognition, self-regulation, coping, communication and shared mental modelling.

Analysis: The argument proceeds that this pedagogic concept and approach facilitate educational benefits. This is based upon insight, accurate self-perception, motivation and decreased team workloads following more efficient collaboration and communication. By applying a rigorous expert mentor model that incorporates retrospective reporting and building it into the design and architecture of a capstone CDX, the NDCA can preserve complexity during protracted periods of training. The outcome supports novice cyber operator performance as it develops the understand function, self-governance, as well as wider domain cognisance for novice level cyberspace operators.

4.8 Limitations

In Paper II little was discussed about information ‘cues’ the locator might use to locate another individual, or how these may differ depending on one’s own and a communication partner’s relative location in The Hybrid Space. Further consideration for differences and some identification of the informational and communication cues that may be used in each type of location task (i.e., each permutation of quadrant-to-quadrant locating) would be beneficial to improve how OLB (see Paper II in this thesis) is taught, practiced and the influence of external events such as time pressure, relevance of issues and hierarchy are better understood.

The latest research into ‘reactivity’, and how this can disturb online methods of measuring metacognition by self-report (Double & Birney, 2019) was published after Papers III & IV were published. The Hybrid Space app attempted to minimize reactivity compared to a typical questionnaire, but still it is there providing cues, and according to the latest research it changes the very thing you want to measure. This is a limitation that will need to be considered in future research and application of the app. To an extent this invasiveness was addressed in Paper VII through the introduction of retrospective timelines and assessing relevant cognitive processes retroactively. This also has its limitations due to limitations of reduced detail and time criticalness when reflecting on action.

The role of expert mentors in Paper V and VII may not as a rule lead to better performance among novices. For example, experts, just like novice cadets, need good metacognitive skills in order to give expert judgment. By having done something very often and achieved a high level of fluency, one can feel more confidence (self-efficacy) without necessarily having improved one's own decision-making to the same degree. Similarly, experts may rely on established and well-trained heuristics and thus overlook relevant novel cues. The definition of expertise should be related to performance, not to formal qualifications, making it very difficult to assess. Thus, expert-status has always to be critically assessed/considered.

Conclusion

5.1 Contributions

This thesis contributes by addressing the need for increased proficiency levels as workplace demands increase due to complex socio-technical systems. The nature of work today is cognitive and collaborative requiring high levels of knowledge, reasoning skills and critical thinking skills. By studying this challenge from the perspective of educating military cyberspace personnel and answering the question: *Identifying approaches to support performance among novice cyber operators*, this research is a significant contribution to ensuring their “cognitive readiness” (Morrison & Fletcher, 2002, p. ES-1) for understanding and self-governance in the cyber domain. More significantly, the fact that this readiness is anchored in adaptive, resilient and robust human capabilities that can be taught, trained on and applied in real world contexts, means the wider application of the outcomes of this thesis are manifest.

Contributions in five key areas can be identified:

- This thesis contributes to the development management of cyber security education by proposed approaches and suggested methods that are suitable to evaluate human performance in cyberspace operations and training. Through investment in building the cognitive readiness skills necessary for the co-creation of new knowledge based upon advanced understanding; then praxis that supports how governance at a human behaviour level can support how cyberpower effects are managed.
- Distinctly, this thesis shows that metacognitive development is key to achieving a holistic approach to managing the positive and negative effects of cyberpower. Given that metacognition can be taught and developed, this thesis shows how and why it is necessary to introduce metacognitive skills training - as an explicit component in cyberspace domain teaching and training contexts - in a manner introduced in this thesis and applied by the researcher at the NDCA. This method of improving domain understanding and governance competence, enables individuals to not only think about the problem correctly

(cognitive skill), but also know that they are thinking about the problem correctly or not (metacognitive skill) so that thinking and behaviour can change if necessary.

- Developing the understand function among cyber cadets relies just as much upon building technical competence as it does on developing human factors such as cognitive agility and domain cognisance. This contribution reveals how these functions of performance can be facilitated by alternative educational processes. In combination with traditional educational processes and methods in a military cyberspace context, this research affords the reader the opportunity to change fixed mindsets. It highlights the need for a more hybrid and adaptive approach concerning what is the correct method of recruitment, selection and education. One such alternative approach is Slow Education. This is an approach that relies upon methods of self-reflective practice to allow for progress evaluation and adaptation where necessary to achieve goals; mentoring as dynamic assessment; and applied learning to develop adaptability and cognitive flexibility in complex situations when working with especially tough cases at the edge of skill and knowledge. Slow pedagogy reveals pathways to improved performance. As opposed to following only conventional (e.g., classroom) instructionist methods of education/training. The latter are largely ineffective at helping learners acquire the skills and knowledge needed for understanding and self-governance in the complex and unpredictable cyberspace domain.
- Alternative approaches to education, such as Slow pedagogies, Self-directed and Student-centered learning can support the construction and acquisition of metacognitive skills (Moely et al., 1995; Schraw, 1998). Applying metacognitive strategies supports performance as they can facilitate the human performance attributes of 'cognitive flexibility' and 'adaptive expertise' (Spiro, 1998; Spiro et al., 2019). Being cognitively agile means applying these attributes to meet the demands of a situation generated by an agile and/or intelligent adversary, in a complex and chaotic dynamic fast-moving situation (Hutton & Turner, 2019).

The implications for education lie not with significant changes to content, rather with adaptations to how the current content is delivered. Teachers, instructors, exercise planners and mentors would benefit from improved understanding relating to 'cognitive flexibility' and 'adaptive expertise' as enabling factors for general thinking and decision-making

performance. Invariably, but often unknowingly, faculty members have strong metacognitive skills and assume that learners either have them or will naturally develop them over time. Teachers should not overestimate their students' metacognitive skills. They should also not underestimate the need for thoughtful instruction in order to teach and reinforce these skills (Ambrose et al., 2010). It can be as simple as considering how much space a learner is given to think for herself. For alternative interventions to succeed, there is a need for learning support structures to ensure adaptations to content delivery develop the required cognitive skills and knowledge. To develop cognitive agility requires approaches to improving all the aspects of cognitive work. For this reason, educators should be guided in the process of a. understanding what cognitive work entails, b. the critical role they play in helping students develop metacognitive skills and c. support educators to rethink their subject and content, to identify opportunities for interventions that can improve cadets' cognitive agility.

- As institutions develop and embrace the benefits of digitalisation they face the unavoidable bargain of trading their new digital efficiency with increased vulnerability. Significant lessons can be taken from the aforementioned contributions and applied by institutions educating cyber personnel. This thesis helps leverage positive effects and mitigate the negative effects of cyberpower by focusing on the human, and her proficiency potential. There is a greater reach and potential impact of this thesis for institutional development. The need to invest in developing the technical and social skills of learners includes employees within institutions who are interfacing with digital effects. Organisations and their workforce need to adjust in order to remain robust and resilient to the outcomes of digitalisation. As the contributions in this thesis show, when a pedagogical approach designed to develop metacognitive skills, is applied in conjunction with The Hybrid Space framework and The Hybrid Space app for measuring cognitive focus movements, then individuals and teams from all levels of hierarchy, with varying skill-sets and competence fields have a pathway to improve their cyberpower praxis. This happens through better understanding and governance capabilities when conducting operations in cyberspace.

5.2 Future Research

From a cyber-military perspective, The Hybrid Space is a framework that reflects the novel demands of the future operating environment. More instrumentally though, it mirrors a complex thinking and operating environment that can support research intended to define and reveal not just skillsets, but also cognitive processes and potentially aptitude for performance in the cyberspace domain.

The OLB model presented in Paper II has yet to be empirically validated. This is especially true when considering the dyadic process between for example individuals in the same team with the same academic background; between teams from a different discipline; between organisations with different motivations and business goals; between sectors that may have opposing risk perceptions; across borders where cultures and language impact communication. Validating the OLB can lead to developing a standardized way to assess OLB through observations, self-assessment, scenarios with virtual-agents (for the latter see Frankel, 2017), or assessing task mental model accuracy (Kwei-Narh et al., 2016). An OLB assessment tool can have the purpose of supporting aptitude testing for potential suitability for specific roles in a cyber workforce. Identifying, selecting and cultivating talent in the cyberspace workforce involves recognizing that the people drawn to this field are likely to demonstrate distinctive social psychological traits and tendencies making them uniquely suited to perform in this space (Dawson and Thomson, 2018; see also Chen and Cotoranu, 2013; Cook, 2014; Dark, 2015; Fontenele and Sun, 2016; Gonzalez, 2015; Lugo, 2016 & 2017).

It is not only metacognition that occurs and controls movements within The Hybrid Space, although it is an important predictor/prerequisite of conscious cognitive control over these movements. Other environmental and cognitive factors may trigger movements. This cognitive action is constant and should be considered as normative movements in The Hybrid Space, not to be confused with conscious metacognitive movements triggered by understanding, control, and manipulation of one's cognitive processes. This research lacks the empirical data to judge whether The Hybrid Space app measures cognitive flexibility or instability (the former is voluntary and under control, the latter is movement due to uncontrolled internal or external effects (intrusions or distractions)). An investigation to resolve if movement is 'good' (as suggested and theoretically explained in this thesis) or is it bad. The causal relationship between cognitive agility in The Hybrid Space and performance indicators requires

further investigation to move beyond the performance related proxies used thus far (see Paper III, IV, and V in this thesis). Disentangling voluntary Hybrid Space movement from involuntary is still to be done.

The use of retrospective timelines as a method for scaffolding performance during a CDX is an area that should be explored further. Successful at the anecdotal level (see Paper VII in this thesis), data has been gathered from a later CDX that may support the validity of this method. A more pressing research goal related to this is the need to identify the attributes of mentors in this domain. It has been reported that little is known about what makes a good mentor in a modern socio-technical context (Ward et al., 2006 & 2013). Qualifying to be a mentor in an educational cyberspace domain context goes beyond having high technological expertise, it means having a broader skillset that is capable of developing a learner's core human factors. Further research is needed to learn and develop a methodology for identifying the right mentors and how to use them in this domain to achieve goals, in an efficient and appropriate way.

The cognitive manoeuver seen in Figure 4.3 is an example of a novice level operator. As noted in the conclusion of Paper III this may indicate impulsive cognitive movements occurring without conscious thought, typical of people who may not have undergone formal metacognitive learning programmes. For comparison it would be beneficial to conduct the same experiment on expert / high proficiency level operators. One might assume, in light of Buchler et al. (2018) that movements may be less i.e., more focused. As effective collaboration (well-grounded OLB), experience (supports cognitive flexibility), and functional role-specialization are factors that affect human performance in cyber defence.

The contributions of this thesis can not only be applied and replicated, but the outcome is a foundation from which further research can grow. Reflecting on the process of investigating and learning how performance can be improved among persons charged with governing the effects of cyberpower, highlights the cross-discipline collaborations embraced and leveraged throughout this project. Establishing a pedagogic methodology for improved proficiency in the cyberspace domain cannot be pursued from one singular field of view. It requires multiple perspectives.

References

- Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research--challenges and benefits. *Journal of Education and Learning*, 5(3), 288-296. <https://doi:10.5539/jel.v5n3p288>
- Almond Tree (2020). Strategic Consulting. Retrieved from <https://www.almondtreeconsulting.co.uk/blog/behavioural-governance>
- Ambrose, S. A., Bridges, M. W., DiPietro, M., Lovett, M. C., & Norman, M. K. (2010). *How learning works: Seven research-based principles for smart teaching*. Hoboken, NJ: John Wiley & Sons, Inc.
- Annink, C., & van Mook, N. (2019). The impact of educational characteristics on the development of cadets from novices to experts. In *NL ARMS Netherlands Annual Review of Military Studies 2019*, 181-193. TMC Asser Press, The Hague.
- Bandura, A. (1986). *Social foundations of thought and action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall.
- Bandura, A. (1993). Perceived self-efficacy in cognitive development and functioning. *Educational psychologist*, 28(2), 117-148.
- Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: W.H. Freeman and Company.
- Barrett, E. (2013). Warfare in a new domain: The ethics of military cyber-operations, *Journal of Military Ethics*, 12(1), 4-17. <https://doi.org/10.1080/15027570.2013.782633>
- Bashir, M., Wee, C., Memon, N., Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, 65, 153-165, <https://doi.org/10.1016/j.cose.2016.10.007>
- Bloom, B. S. (1984). The 2 sigma problem: The search for methods of group instruction as effective as one-to-one tutoring. *Educational researcher*, 13(6), 4-16.
- Boleng, J., Schweitzer, D., & Gibson, D. S. (2008). Developing cyber warriors. In 3rd International Conference on Information Warfare and Security.
- Boud, D., & Feletti, G. (Eds.). (1998). *The challenge of problem-based learning*. Psychology Press. London: Routledge.
- Bousquet, A. (2009). *The scientific way of warfare. Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press.
- Brunswik, E. (1956). Perception and the representative design of psychological experiments. Univ of California Press.
- 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. In: *Frontiers in Psychology*, 7(937), <https://doi.org/10.3389/fpsyg.2016.00937>
- Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L. R., & Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Frontiers in psychology*, 9(2133). DOI: 10.3389/fpsyg.2018.02133
- Casson, D. J. (2011). *Liberating Judgment: Fanatics, Skeptics, and John Locke's Politics of Probability*. Princeton: Princeton University Press.
- 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>
- Chen, L. C., Cotoranu, A. (2013). Enhancing the interdisciplinary curriculum in cybersecurity by engaging high-impact educational practices. Cornerstone 3 Reports: *Interdisciplinary Informatics*. Paper 91. New York, NY: Pace University.
- Chi, M. T., Siler, S. A., Jeong, H., Yamauchi, T., & Hausmann, R. G. (2001). Learning from human tutoring. *Cognitive Science*, 25(4), 471-533.
- Cisco, V. N. I. (2018). Cisco visual networking index: Forecast and trends, 2017–2022. *White Paper*, 1. Retrieved from <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>
- Cobb, S., & Lee, A. (2014). Malware is called malicious for a reason: The risks of weaponizing code. In *2014 6th International Conference On Cyber Conflict (CyCon 2014)* 71-84. IEEE.
- Conti, G., & Raymond, D. (2011). Leadership of cyber warriors: Enduring principles and new directions. Military Academy West Point, NY, Department of Electrical Engineering and Computer science. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a545300.pdf>
- Cook, M. (2014). Cyber acquisition professionals need expertise (but they don't necessarily need to be experts). Fort Belvoir: Defense Acquisition University. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a608765.pdf>
- Cooper, J. (1990). Cooperative learning and college teaching: Tips from the trenches. In M. Weimer (Ed.), *The teaching professor* (pp. 114-139). University Park, PA: The Pennsylvania State University.
- Crisp, G., & Cruz, I. (2009). Mentoring college students: A critical review of the literature between 1990 and 2007, *Research in Higher Education*, 50(6) 525-545.
- 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:10.1177/154193120504900304
- 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*, 19-37. Berlin, Heidelberg: Springer Berlin Heidelberg. DOI:10.1007/978-3-540-78243-8_2
- Dark, M. B., Bishop, M., Linger, R., & Goldrich, L. (2015). Realism in teaching cybersecurity research: The agile research process. In Bishop M., Miloslavskaya N., Theocharidou M. (Eds.), *Information Security Education Across the Curriculum*. WISE 2015. IFIP Advances in Information and Communication Technology, 453, 3–14, Springer, Cham. https://doi.org/10.1007/978-3-319-18500-2_1
- Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology*, 9, 744. <https://doi.org/10.3389/fpsyg.2018.00744>
- Department of Homeland Security (DHS), (2019). Critical infrastructure security, Retrieved from <https://www.dhs.gov/topic/critical-infrastructure-security>
- Dhami, M. K., Hertwig, R., & Hoffrage, U. (2004). The role of representative design in an ecological approach to cognition. *Psychological bulletin*, 130(6), 959-988.
- Doffman, Z., (2019). China set traps to capture dangerous NSA cyberattack weapons: New Report, Retrieved from <https://www.forbes.com/sites/zakdoffman/2019/09/05/secret->

chinese-hacking-group-set-traps-to-steal-nsa-cyberattack-tools-new-report/#308900aa48ce

- Dombrowski, P., & Demchak, C. C. (2014). Cyber war, cybered conflict, and the maritime domain. *Naval War College Review*, 67(2), 70-96.
- Double, K. S., & Birney, D. P. (2019). Reactivity to measures of metacognition. *Frontiers in Psychology*, 10, 2755. <https://doi.org/10.3389/fpsyg.2019.02755>
- Feltovich, P. J., Spiro, R. J., Coulson, R. L. (1997). Issues of expert flexibility in contexts characterized by complexity and change. In P. J. Feltovich, K. M. Ford, & R. R. Hoffman (Eds.), *Expertise in Context: Human and Machine*, 5, 125-146. Menlo Pk. CA: AAAI/MIT Press.
- Feltovich, P. J., Coulson, R.L., & Spiro, R. J. (2001). Learners' (mis)understanding of important and difficult concepts: A challenge to smart machines in education. In K. D. Forbus & P. J. Feltovich (Eds.), *Smart machines in education*, 349-375. Menlo Park, CA: AAAI/MIT Press.
- Feltovich, P. J., Hoffman, R. R., Woods, D., & Roesler, A. (2004). Keeping it too simple: How the reductive tendency affects cognitive engineering. *IEEE Intelligent Systems*, 19(3), 90-94.
- Feltovich, P, Spiro, R, & Coulson, R. (1997). *Expertise in context: Human and machine*, MIT Press, Cambridge, MA. Fink, G., Best D., Manz D., Popovsky, V., Endicott-Popovsky, B., (2013). Gamification for measuring cyber security situational awareness. In: *International Conference on Augmented Cognition*. Springer, 656-665.
- Fink, G., Best, D., Manz, D., Popovsky, V., & Endicott-Popovsky, B. (2013). Gamification for measuring cyber security situational awareness. In Schmorrow D.D., Fidopiastis C.M. (Eds.), *Foundations of Augmented Cognition*. AC 2013. Lecture Notes in Computer Science, 8027. 656-665. Springer, Berlin, Heidelberg.
- Flavell, J. H. (1979). Metacognition and cognitive monitoring: A new area of cognitive-developmental inquiry. *The American Psychologist*, 34(10), 906-911.
- Flick, U. (2018). *An introduction to qualitative research*. London: Sage Publications. Sixth edition
- Flick, U. (2007). *Managing Quality in Qualitative Research*. London: Sage Publications
- FMFM 1, (1989). Warfighting, Department of the Navy, Headquarters U.S. Marine Corps. Washington, D.C.
- Fontenele, M., Sun L. (2016). Knowledge management of cyber security expertise: an ontological approach to talent discovery, in *Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* 1-13. IEEE.
- Forsythe, C., Silva, A., Stevens-Adams, S., Bradshaw, J. (2013). Human dimension in cyber operations research and development priorities. In: *International Conference on Augmented Cognition*. 418-422, Springer, Berlin, Heidelberg.
- Forsvarets Høgskole. (2020). Utdanning ved Forsvarets høgskole, Bachelor i ingeniørfag, studieretning telematikk. Retrieved from <https://utdanning.forsvaret.no/nb/program/bachelor-i-ingeni%C3%B8rfag-studieretning-telematikk/studieplan>
- Frankel, J. (2017). PTSD Treatment: How AI is helping veterans with post-traumatic stress disorder, *Newsweek, Tech & Science*. Retrieved from <https://www.newsweek.com/ptsd-treatment-how-ai-could-help-veterans-post-traumatic-stress-disorder-682857>
- Freire, P. (1996). *Pedagogy of the oppressed* (revised). New York: Continuum.

- Freire, P. (1970) *Pedagogy of the Oppressed*. New York: Continuum Books.
- Fulp, J. D. (2003). Training the cyber warrior. In *Security education and critical infrastructures* 261-273. Springer, Boston, MA.
- Gálik, S., & Tolnaiová, S. G. (2019). Cyberspace as a new existential dimension of man. In *Cyberspace*. IntechOpen.
- Gilboy, M. B., Heinerichs, S., & Pazzaglia, G. (2015). Enhancing student engagement using the flipped classroom. *Journal of nutrition education and behavior*, 47(1), 109-114.
- Giroux, H., & McLaren, P. (1989). *Critical pedagogy, the state, and the struggle for culture*. Albany: State University of New York Press
- Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, 8(4), 597-606.
- Gonzalez, M. D. (2015). Building a cybersecurity pipeline to attract, train, and retain women. *Business Journal for Entrepreneurs*. 2015(3), 24–41.
- Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Towards a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis*, 11(3), 255-274. DOI: 10.3102/01623737011003255
- Greer, L. L., de Jong, B. A., Schouten, M. E., & Dannals, J. E. (2018). Why and when hierarchy impacts team effectiveness: A meta-analytic integration. *Journal of Applied Psychology*, 103(6), 591-613.
- Greitens, S. C. (2013). Authoritarianism Online: What can we learn from internet data in nondemocracies?. *PS: Political Science & Politics*, 46(2), 262-270.
- Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds), *Handbook of qualitative research*, 2(105-117). Thousand Oaks, CA: Sage.
- Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59(1) 322-326. Sage CA: Los Angeles, CA: SAGE publications.
- Gutzwiller, R. S., Ferguson-Walter, K. J., & Fugate, S. J. (2019). Are cyber attackers thinking fast and slow? Exploratory analysis reveals evidence of decision-making biases in red teamers. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 63(1), 427-431. Sage CA: Los Angeles, CA: SAGE Publications.
- Hannafin, M. J., & Hannafin, K. M. (2010). Cognition and student-centered, web-based learning: Issues and implications for research and theory. In *Learning and instruction in the digital age*, 11–23. Springer, Boston, MA.
- Hardison, C. M., Payne, L. A., Hamm, J. A., Clague, A., Torres, J., Schulker, D., & Crown, J. S. (2019). Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers. *Cyber Workforce Interview Findings*. Santa Monica, CA: RAND Corporation.
- Hydén, G., Court, J., & Mease, K. (2004). *Making sense of governance: empirical evidence from sixteen developing countries*. Boulder, CO: Lynne Rienner Publishers.
- Helkala, K., Knox, B. J., Jøsok, Ø., Knox, S., and Lund, M. (2016a) Factors to affect improvement in cyber officer performance." *Information & Computer Security* 24(2), 152-163.
- Helkala, K. M., Knox, B. J., Jøsok, Ø., Lugo, R., Sütterlin, S. (2016b). How coping strategies influence cyber task performance in the Hybrid Space. *Communications in Computer and Information Science*, 617. 192-196.
- Hoffman, R. R., Feltovich, P. J., Fiore, S. M., Klein, G., & Ziebell, D. (2009). Accelerated learning (?). *IEEE Intelligent Systems*, 24(2), 18-22.

- Hoffman, R. R., LaDue, D. S., Mogil, H. M., Roebber, P. J., & Trafton, J. G. (2017). *Minding the weather: How expert forecasters think*. MIT Press.
- Hoffman, R. R., & Militello, L. G. (2008). *Perspectives on cognitive task analysis: Historical origins and modern communities of practice*. Psychology Press. Taylor & Francis, New York, NY.
- Hoffman, R. R., and Ward, P. (2015). Mentoring: A leverage point for intelligent systems? *IEEE Intelligent Systems*, 30(5), 78-84. DOI: 10.1109/MIS.2015.86
- Holt, M. (2002). It's time to start the slow school movement. *Phi Delta Kappan*, 84(4), 264–271.
- Hornby, A. S. (2010). Oxford advanced learner's dictionary of Current English, 8th Edition, Oxford: Oxford university press.
- Hutton, R., & Turner, P. (2019). Cognitive Agility: Providing the Performance Edge, Wavell Room, Contemporary British Military Thought. Retrieved from <https://wavellroom.com/2019/07/09/cognitive-agility-providing-a-performance-edge/>
- Hutton, R., Turner, P., & Jones, M. (2020). Cognitive Agility & The Thinking Approach Space, Wavell Room, Contemporary British Military Thought. Retrieved from <https://wavellroom.com/2020/02/18/cognitive-agility-the-thinking-approach-space/>
- Ikeda, S. (2019). Chinese hackers demonstrate their global cyber espionage reach with breach at 10 of the world's biggest telecoms. Retrieved from <https://www.cpomagazine.com/cyber-security/chinese-hackers-demonstrate-their-global-cyber-espionage-reach-with-breach-at-10-of-the-worlds-biggest-telecoms/>
- Inkster, N. (2016). *China's Cyber Power*. London: Routledge.
- Jenson, J., de Castell, S., Thumlert, K., & Muehrer, R. (2016). Deep assessment: An exploratory study of gamebased, multimodal learning in Epidemic. *Digital Culture & Education*, 8(2), 20–40.
- Jøsok, Ø., Knox, B. J., Helkala, K. M., Lugo, R; Sütterlin, S., Ward, P. (2016). *Exploring the Hybrid Space: Theoretical framework* Applying cognitive science in military cyberspace operations. *Lecture Notes in Computer Science*; 9744. 178-188
- Kallberg, J. (2016). *Strategic cyberwar theory-A foundation for designing decisive strategic cyber operations*. West Point, New York: Army Cyber Institute, West Point.
- Kallberg, J., & Thuraisingham, B. (2013). State Actors' Offensive Cyberoperations: The Disruptive Power of Systematic Cyberattacks. *IT Professional*, 15(3), 32-35.
- Kampenens, I., & Røislien, H. (2019). Cyberforsvaret er avhengig av sivilsamfunnet, Forsvarets Forum, Retrieved from: <https://forsvaretsforum.no/cyberforsvaret-er-avhengig-av-sivilsamfunnet>.
- Kember, D., Leung, D. Y. P., Jones, A., Loke, A. Y., McKay, J., Sinclair, K., & Yeung, E. et al., (2000). Development of a questionnaire to measure the level of reflective thinking. *Assessment & evaluation in higher education*, 25(4), 381–395. DOI:10.1080/713611442
- Kennedy, G. E., K. Krause, K. Gray, T. S. Judd, S. Bennett, K. Maton, B. Dalgarno and A. Bishop. (2006). Questioning the net generation: A collaborative project in Australian higher education. Proceedings of the 23rd annual ascilite conference: Who's learning? Whose technology?
- Klein, G. (1998). *Sources of Power: How people make decisions*. Cambridge MA: MIT Press.
- Klein, G., & Baxter, H. C. (2006). Cognitive transformation theory: Contrasting cognitive and behavioral learning, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC 2006): Training the 21st Century 4- 7 December 2006, Orlando, Florida, USA.

- Klein, G., & Baxter, H. C. (2009). Cognitive transformation theory: Contrasting cognitive and behavioral learning. In *The PSI handbook of virtual environments for training and education: Developments for the military and beyond, Vol. 1, Education: Learning, requirements and metrics*, 50-65. Praeger Security International.
- Knowles, M. S. (1975). *Self-directed learning: A guide for learners and teachers*. Broadway, NY: Association Press.
- Koopman, P., & Hoffman, R.R. (2003). Work-arounds make-work and kludges, *IEEE Intelligent Systems*, 18(6), 7075.
- Krekel, B., Adams, P., & Bakos, G. (2014). Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage. *International Journal of Computer Research*, 21(4), 333-349.
- Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*, 77(6), 1121.
- Kuehl, D., Kramer, F. D., Starr, S. H., and Wentz, L. K. (2009). *Cyberpower and National Security*. Dulles, VA: Potomac Books, Inc.
- Kwei-Narh, P. A., Valaker, S., Hærem, T., & Lervik, J. E. (2016). Monitoring and team performance: The mediating role of task mental model accuracy. In *Academy of Management Proceedings, 2016(1)* 17012. Briarcliff Manor, NY 10510: Academy of Management.
- Lewis, J. A. (2015). The role of offensive cyber operations in NATO's collective defence. *Tallinn Paper*, 9.
- Libicki, M. C. (2016). *Cyberspace in peace and war*. Annapolis, Maryland: Naval Institute Press.
- Libicki, M. C. (2017). The coming of cyber espionage norms. In *2017 9th International Conference on Cyber Conflict (CyCon)*, 1-17. IEEE.
- Lindlof, T. R., & Taylor, B. C. (2017). *Qualitative communication research methods*. Thousand Oaks, CA: Sage.
- Longhurst, R. (2003). Semi-structured interviews and focus groups. *Key methods in geography*, 3, 143-156.
- Lopez, T (2017). Future warfare requires 'disciplined disobedience,' Army chief says, U.S.Army, Retrieved from https://www.army.mil/article/187293/future_warfare_requires_disciplined_disobedience_army_chief_says
- Lugo, R. G. (2018). *Micro-and Macrocognitive Factors of Performance in Cyber Defence Operations*. (Doctoral dissertation). Johannes Gutenberg-Universität Mainz, Germany.
- Lugo, R. G., Knox, B. J., Jøsok, Ø. & Sütterlin, S. (in press). Variable self-efficacy as a measurement for behaviors in cyber security operations. *Lecture Notes in Computer Science (LNCS)*. HCI International 2020.
- Lugo, R. G., Kwei-Nahra, P., Jøsok, Ø., Knox, B. J., Helkala, K., and Sütterlin, S. (2017). Team workload demands influence on cyber detection performance. In *Proceedings of 13th International Conference on Naturalistic Decision Making*, 223-225.
- Lugo, R. G., Sütterlin, S., Knox, B. J., Jøsok, Ø., Helkala, K., and 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.

- Lund, M. S., Knox, B., & Røislien, H. E. (2014). What do cyber soldiers need to know? In *International Conference on Cyber Warfare and Security*, 37. Academic Conference International Limited.
- Lynch, J. (2018). *Why recruiting cyberwarriors in the military is harder than retaining forces*, Retrieved from <https://www.fifthdomain.com/dod/2018/11/01/why-recruiting-cyber-warriors-in-the-military-is-harder-than-retaining-forces/>
- Mackey Sr, R. H. (1992). *Translating vision into reality: The role of the strategic leader*. ARMY WAR COLL CARLISLE BARRACKS PA.
- Mallet, V., and Chilkoti, A. (2016). How cyber criminals targeted almost \$1bn in Bangladesh Bank heist, Retrieved from <https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8>
- Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014). Human factors in cyber warfare II: Emerging perspectives. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 58(1), 415-418. Sage CA: Los Angeles, CA: SAGE Publications.
- Martelle, M., (2019). *Fighting ISIS and learning cyber-war*, Retrieved from <https://unredacted.com/2019/09/13/learning-from-isis-for-cyber-war/>
- McChrystal, G. S., Collins, T., Silverman, D., & Fussell, C. (2015). *Team of teams: New rules of engagement for a complex world*. UK: Penguin.
- Meichenbaum, D. (1985). Metacognitive methods of instruction: Current status and future prospects. *Special Services in the Schools*, 3(1-2), 23–32. DOI:10.1300/J008v03n01_03
- Metcalf, J., & Shimamura, A. P. (Eds.), (1994). *Metacognition: Knowing about knowing*. MIT press.
- Miller, C. C., Cardinal, L. B., & Glick, W. H. (1997). Retrospective reports in organizational research: A reexamination of recent evidence. *Academy of management journal*, 40(1), 189-204.
- Ministry of Justice and Public Security. (2017). *Cyber Security - A Joint Responsibility (Meld. St. 38 (2016–2017))*. Oslo: Norwegian Government Security and Service Organisation. Retrieved from <https://www.regjeringen.no>.
- Moely, B. E., Santulli, K. A., & Obach, M. S. (1995). Strategy instruction, metacognition, and motivation in the elementary school classroom. In Weinert, F. E., and Schneider, W. (eds) *Memory performance and competencies: Issues in growth and development*, Hillsdale, NJ: Erlbaum, 301-321.
- Morgan, S. (2019). *Cybersecurity almanac: 100 facts, figures, predictions and statistics*. Retrieved from <https://cybersecurityventures.com/cybersecurity-almanac-2019/>
- Morrison, J. E., & Fletcher, J. D. (2002). *Cognitive readiness* (No. IDA-P-3735). Institute for Defense Analysis, Washington, DC.
- Neag, M. M. (2018). Physiognomy of military operations answer to hybrid threats. In *International conference on Knowledge-based organizations* 24(1), 163-170. Sciendo.
- North Atlantic Treaty Organization (NATO). (2016a). *Warsaw Summit Communiqué*. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en
- North Atlantic Treaty Organization (NATO). (2016b). *Cyber Defence Pledge*. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en
- Nietfeld, J., & Schraw, G. (2002). The effect of knowledge and strategy training on monitoring accuracy, *The Journal of Educational Research*, 95(3), 131-142.
- Northouse, P. G. (2015). *Leadership: Theory and practice*. Thousand Oaks, CA: Sage.

- Nye, J. (2010). *Cyber Power*. Harvard Kennedy School, *Belfer Center for Science and International Relations*. Retrieved from <https://www.belfercenter.org/publication/cyber-power>
- Onwuegbuzie, A. J., & Johnson, R. B. (2006). The validity issue in mixed research. *Research in the Schools*, 13(1), 48-63.
- Ognyanova, K. (2019). In Putin's Russia, Information has you: Media control and internet censorship in the Russian Federation. In I. Management Association (Eds.), *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*, 1769-1786. Hershey, PA: IGI Global.
- Operations, A. C. (2013). *Comprehensive Operations Planning Directive COPD Interim V2. 0. Supreme Headquarters of Allied Power Europe, Belgium*, 4.
- Panadero, E. (2017). A review of self-regulated learning: Six models and four directions for research. *Frontiers in Psychology*, 8, 422. DOI:10.3389/fpsyg.2017.00422
- Patton, M. Q. (2005). Qualitative research. *Encyclopedia of statistics in behavioral science*. In Brian S., Everitt & David C. Howell, (Eds.), 1633-1636. Hoboken, NJ: John Wiley & Sons, Inc. DOI:10.1002/0470013192.bsa514
- Pedler, M. (2011). Leadership, risk and the impostor syndrome. *Action Learning: Research and Practice*, 8(2), 89-91. DOI: 10.1080/14767333.2011.581016
- Petushek, E., Aarsal, G., Ward, P., Upton, M., Whyte IV, J., & Hoffman, R. R. (2019). Learning at the Edge: The Role of Mentors, Coaches, and Their Surrogates in Developing Expertise. In P. Ward, J. M. Schraagen, J. Gore, & E. M. Roth (Eds.), *The Oxford Handbook of Expertise*, 1021-1057. Oxford: Oxford University Press.
- Piaget, J. (1964). Part I: Cognitive development in children: Piaget development and learning. *Journal of Research in Science Teaching*, 2(3), 176-186.
- Pfaffenberger, B. (1992). Social anthropology of technology. *Annual review of Anthropology*, 21(1), 491-516.
- Popper, K. (1963). *Conjectures and refutations: The growth of scientific knowledge* (2nd ed., Routledge Classics). Oxfordshire, England.
- Porpora, D. V. (1983). On the prospects for a nomothetic theory of social structure. *Journal for the Theory of Social Behaviour*, 13(3), 243-264.
- Price, D. D., McGrath, P. A., Rafii, A., & Buckingham, B. (1983). The validation of visual analogue scales as ratio scale measures for chronic and experimental pain. *Pain*, 17(1), 45-56.
- Rhodes, J. (2008). Improving youth mentoring interventions through research-based practice, *American Journal of Community Psychology*, 41(1-2), 35-42.
- Regjeringen. (2016). Forskrift om rammeplan for ingeniørutdanning. Retrieved from <https://www.regjeringen.no/contentassets/389bf8229a3244f0bc1c7835f842ab60/ny-forskrift-om-rammeplan-for-ingeniorutdanning-fastsatt-18.05.18.pdf>
- Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon* 9(5): 1-15.
- Sadler, T. D., & Zeidler, D. L. (2005). Patterns of informal reasoning in the context of socioscientific decision making. *Journal of Research in Science Teaching: The Official Journal of the National Association for Research in Science Teaching*, 42(1), 112-138.
- Sandhurst Trust. (2015). Army launches new leadership code, The seven leadership behaviours, Retrieved from <https://www.sandhursttrust.org/news/army-launches-new-leadership-code/>

- Schroefl, J. (2020). Cyber power is changing the concept of war. Hybrid CoE Strategic Analysis / 21. Retrieved from https://www.hybridcoe.fi/wp-content/uploads/2020/03/Strategic-Analysis_21_Cyber-Power.pdf
- Schermerhorn, J. R. (1997). Situational leadership: Conversations with Paul Hersey. *Mid-American Journal of Business*, 12, 5–12.
- Siedler, R. E. (2016). Hard power in cyberspace: CNA as a political means. In 2016 8th *International Conference on Cyber Conflict (CyCon)*, 23-36. IEEE.
- Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law applicable to cyber operations* (2 ed.). Cambridge: Cambridge University Press.
- Schmitt, M. (2011). Cyber operations and the jus in bello: key issues. *International Law Studies*, 87(1), 89-110.
- Schraw, G. (1998). Promoting general metacognitive awareness. *Instructional science*, 26(1-2), 113-125.
- Schraw, G., & Gutierrez, A. P. (2015). Metacognitive strategy instruction that highlights the role of monitoring and control processes. In Peña-Ayala A. (Eds.), *Metacognition: Fundamentals, applications, and trends*. Intelligent Systems Reference Library, 76, 3–16. Cham: Springer.
- Shaw, P. A., Cole, B., & Russell, J. L. (2013). 19: Determining our own tempos: Exploring slow pedagogy, curriculum, assessment, and professional development. *To Improve the Academy*, 32(1), 319-334.
- Schön, D. A. (1987). *Educating the reflective practitioner*. Jossey-Bass, San Francisco.
- 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*, 43-47. DOI: 10.1145/2808006.2808038
- Spidalieri, F., & McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review*, 1(1), 141-164.
- Spiro, R. J. (1988). Cognitive flexibility theory: Advanced knowledge acquisition in ill-structured domains, *Center for the Study of Reading Technical Report*, no. 441.
- Spiro, R. J., Feltovich, P. J., Gaunt, A., Hu, Y., Klautke, H., Cheng, C., Clemente, I., Leahy, S., and Ward, P. (2019). Cognitive Flexibility Theory and the accelerated development of adaptive readiness and adaptive response to novelty. In P. Ward, J. M. Schraagen, J. Gore, & E. M. Roth (Eds.), *The Oxford Handbook of Expertise*, 951-976. Oxford: Oxford University Press.
- Stake, R. E., & Trumbull, D. J. (1982). Naturalistic generalizations. *Review Journal of Philosophy and social science*, 7(1), 1-12.
- Strauss, A., & Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Thousand Oaks, CA: Sage.
- Szyska, A. (2010). Behavioral anatomy of the financial crisis. *Journal of Centrum Cathedra*, 3(2), 121-135.
- Tapscott, D. (1998). *Growing up digital: The rise of the net generation*. New York: McGrawHill.
- Thomas, T. (2011). *Recasting the red star: Russia forges tradition and technology through toughness*, Foreign Military Studies Office, Fort Leavenworth, Kan.
- Thomson, R. (2019). The Cyber Domains: Understanding expertise for network security. In P. Ward, J. M. Schraagen, J. Gore, & E. M. Roth (Eds.), *The Oxford Handbook of Expertise*, 718-739. Oxford: Oxford University Press.

- Tikk-Ringas, E., Kerttunen, M., & Christopher, S. (2014). Cyber security as a field of military education and study. *Joint Force Quarterly*, 75.
- Tracy, S. J. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative inquiry*, 16(10), 837-851.
- U.K. Ministry of Defence. (2015). *Future Trends Programme - Future Operating Environment 2035*. United Kingdom.
- Van Gog, T., Paas, F., Van Merriënboer, J. J., & Witte, P. (2005). Uncovering the problem-solving process: Cued retrospective reporting versus concurrent and retrospective reporting. *Journal of Experimental Psychology: Applied*, 11(4), 237-244. DOI: 10.1037/1076-898X.11.4.237
- Vygotsky, L. (1978). Interaction between learning and development (M. Lopez-Morillas, Trans.). In M. Cole, V. John-Steiner, S. Scribner, & E. Souberman (Eds.), *Mind in society: The development of higher psychological processes*, 79-91. Cambridge, MA: Harvard University Press.
- Ward, P., Suss, J., Eccles, D. W., Williams, A. M., & Harris, K. R. (2011). Skill-based differences in option generation in a complex task: A verbal protocol analysis. *Cognitive processing, International Quarterly of Cognitive Science*, 12(3), 289-300. doi:10.1007/s10339-011-0397-9
- Ward, P., Fiore, S. M., Feltovich, P. J., Hoffman, R. R., DiBello, L., & Andrews, D. H. (2013). *Accelerated expertise: Training for high proficiency in a complex world*. Psychology Press. New York, NY.
- Ward, P., Williams, A. M., & Hancock, P. A. (2006). Simulation for performance and training. In K. A. Ericsson, N. Charness, R. Hoffman, & P. Feltovich (Eds.), *Cambridge handbook of expertise and expert performance*, 243–262. Cambridge: Cambridge University Press.
- Ward, P., Gore, J., Hutton, R., Conway, G. E., & Hoffman, R. R. (2018). Adaptive skill as the *conditio sine qua non* of expertise. *Journal of applied research in memory and cognition*, 7(1), 35-50.
- Waterhouse, T. A. (2013). *Hindre for digital verdiskapning [Challenges to Digital Prosperity] (NOU 2013:2)*. Retrieved from <https://www.regjeringen.no/contentassets/e2f0d5676e144305967f21011b715c16/nou/pdfs/nou201320130002000dddpdfs.pdf>.
- Weick, K. E. (2007). The generative properties of richness. *Academy of management journal*, 50(1), 14-19.
- Weimer, M. (2002). *Learner-centered teaching: Five key changes to practice*. Hoboken, NJ: John Wiley & Sons.
- Wells, G. (1999). *Dialogic inquiry: towards a sociocultural practice and theory of education*. Cambridge: Cambridge University Press.
- Wentzel, K. (2019). Students relationships with teachers. In J. Meece & J. Eccles (Eds.), *Handbook of research on schools, schooling and human development*, 93-109. London: Routledge.
- Wessels, P. L., & Steenkamp, L. P. (2009). Generation Y students: Appropriate learning styles and teaching approaches in the economic and management sciences faculty. *South African Journal of Higher Education*, 23(5), 1039-1058.
- West Point. (2019). Bugle notes. Retrieved from <https://www.west-point.org/academy/malo-wa/inspirations/buglenotes.html>
- Whyte, J., Ward, P., & Eccles, D. W. (2009). The relationship between knowledge and clinical performance in novice and experienced critical care nurses: An application of the

- expert performance approach. *Heart & Lung: The Journal of Acute Clinical Care*, 38(6), 517-525.
- Wilby, P. (2019). Eaton master who wants pupils to learn very slowly, *The Guardian*. Retrieved from <https://www.theguardian.com/education/2019/aug/13/eton-master-wants-pupils-learn-slow-education-mike-grenier>
- Williams, A. M., Ward, P., Knowles, J. M., & Smeeton, N. J. (2002). Anticipation skill in a real-world task: Measurement, training, and transfer in tennis. *Journal of Experimental Psychology: Applied*, 8(4), 259-270.
- World Health Organisation (WHO). (2019). WHO health workforce - data and statistics. Retrieved from <https://www.who.int/hrh/statistics/en/>
- Wright, S. (2014). Are you ready to join the slow education movement? *Powerful Learning Practice*. Retrieved from <http://plpnetwork.com/2014/08/26/time-fight-slow-education/>
- Zimmerman, B. J. (2000). Attaining self-regulation: A social social cognitive perspective. In I. Pintrich, P.R., Zeidner, M. & Boekaerts, M. (Eds.), *Handbook of self-regulation*. 13-39. San Diego, CA: Academic Press. DOI: 10.1016/B978-012109890-2/50031-7
- Zimmerman, B. J. (2001). Theories of self-regulated learning and academic achievement: An overview and analysis. In Zimmerman, B. J., & Schunk, D. H. (Eds.), *Self-regulated learning and academic achievement* (2nd ed) 1-38. Hillsdale, NJ: Erlbaum.

PART 2

PAPER I

The Effect of Cyberpower on Institutional Development in Norway

Benjamin J. Knox^{1,2*}

¹ Norwegian Defence Cyber Academy, Lillehammer, Norway, ² Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Through analysis of empirical interview data this research undertakes to investigate the ways in which the growing phenomenon of cyberpower – defined as using cyberspace for advantage and influence – is impacting on institutional development in Norway. Exploring this governance challenge through the conceptual framework of complexity, difference and emergence opens space – political or otherwise – for discussion regarding why rapid developments arising from digitalization are transforming the way individuals, organizations, institutions and states behave, relate and make decisions. Cyberpower is creating an uncertain institutional landscape as a dependency vs. vulnerability paradox shapes values, rules and norms. Findings from this thematic analysis of qualitative data reflect this paradox and suggest that organizations in Norway are in a survival-mode that is blocking collaboration. This occurs as national governance systems, human capacity and cyberpower effects lack synergy making for an uneasy arena where complexity, contestation and emerging challenges frame institutional development. To improve long-term prospects of governing cyberpower effects requires a cross-sectorial conflation of time and human resources. This means consciously taking steps to merge organizational and institutional boundaries through expressive innovative collaborations that foster a shared and holistic agenda. The emerging challenges cyberpower is presenting across multiple domains means further research is recommended to build a richer understanding of the term cyberpower from different perspectives. The investigation recommends investment in building the skills and capacities necessary for the co-creation of new models and strategies for managing the effects of cyberpower.

Keywords: cyberpower, institutional development, governance, sector-principle, cyber-security, Norway

INTRODUCTION

Improving cyber security prospects, nationally and internationally, involves key institutions taking the greater share of responsibility in deciding how to govern the growing influence of power being exercised through cyberspace (Tapscott, 2014; Hagen, 2016; Norwegian Centre for Information Security [NorSIS], 2016). In real world terms, this emphasizes the importance of shared responsibility (Thomas, 1996) when managing powerful actions that occur through cyberspace, such as those that threaten democracy itself (Vatu, 2017). Despite this, cyber security is largely: "...controlled by the private sector and other nonstate actors" (Peña-López, 2016, p. 223). Therefore, negotiating and brokering this fragmentation to bring together those with complementary needs (Thomas, 1996) becomes a governance challenge. This study takes a cross-sectorial approach aiming to build knowledge by identifying how different organizations within seven key sectors, all of whom are notable cyberpower stakeholders, in Norway (political, military, economic, social, informational, infrastructure and diplomatic) manage increased levels of uncertainty arising from complex and emerging challenges presented by cyberpower effects.

The Norwegian state is governed through a national sector- principle framework. This strategy was formally implemented in the 70s but has been practiced since the 1800s. Each Government Ministry is highly autonomous and specialized within its own domain. By encouraging sector-orientated development, ministries are empowered and responsible for their own policy formulation and implementation. From a critical perspective this has been described as creating segmentation within the state (Egeberg et al., 1978) resulting from poor cross-sectorial coordination and selective action (Organisation for Economic Co-operation and Development [OECD], 2005). However, the culture of skepticism toward centralization of

power – retained from days of Swedish and Danish rule – means the sector principle takes precedence. To ease tensions that can emerge between centralized and cross-sector power dynamics, inter- sectorial relationships are encouraged beyond ministerial level and are expected to work on the assumption that they are based upon trust, shared values and goals; when managing threats, challenges and vulnerabilities to systems of shared national interest. Recently, in light of the 22 July 2011 terror attacks in Oslo as well as threats presented through cyberspace (Meld. St. 10, 2016–2017); such as a significant increase in cybercrime and targeted cyber-operations by Russian hackers on Norwegian defense and security officials (The Guardian, 2017); the government has been required to take a more central role in for example, national crises management (Gjørsv, 2012).

Given their power and autonomy, sectors have institutionalized certain cyberpower capacities particular to their individual needs and goals. For example military use of sensor capabilities in support of national and international computer network defense; the application of advanced software to remain competitive in global financial markets; information operations to project a national narrative through digital media outlets; or the utilization of digital command and control technologies for increased efficiency in the energy and diplomatic sectors. Whatever the capacity, it is essential to understand that, similar to other well-intentioned institutionalized practices, advantages are often undermined by related vulnerabilities. In this case, dependency and reliance upon cyberspace provides opportunities for opponents with cyberpower capacities to also: “. . .use cyberspace to create advantages and influence events [. . .] across the instruments of power” (Kuehl et al., 2009, p. 38). This dynamic is redefining institutional rules of the game in society (North, 1990; Tapscott, 2014). In developmental terms, cyberpower has the capacity to bring about “good change” (Chambers, 1995, p. 174) by providing opportunities for expanded agency leading to innovative collaborations. For example, the rise of inter-enterprise computing allows for the blurring of inter-organizational boundaries (Ostrom, 1996) enabling new relationships to emerge that transform business models and strategies (Tapscott, 2014). Entrepreneurship can now reach far beyond physical borders due to globally integrated markets and rapidly expanding networks unhindered by time zones (Castells, 2011). Simultaneously though, cyberspace gives agency and opportunity to antagonists and criminals to challenge and undermine systems of governance, coordination, cooperation and competition within and beyond cyberspace (Nye, 2011). In 2014 the global costs of cybercrime was estimated between US\$375 billion and US\$575 billion, that’s 0.6 percent of global GDP (Center for Strategic and International Studies and McAfee [CSIS], 2014, p. 2). The same report puts Norway’s loss as 0.64% of national GDP (p. 9). Norwegian GDP in 2014 was US\$498 billion (World Bank, 2017, online), which equates to a loss of US\$3.2 billion.

Cyber security can be understood as attempting to protect cyberspace and those tangible and intangible assets that function within it: “. . .relating to the wellbeing of either individual or society at large” (von Solms and van Niekerk, 2013, p. 101). The Norwegian state takes a multi-stakeholder approach (Chehadé, 2014) to cyber security. According to Muller (2016) the multi- stakeholder model is an extension of neo-liberalist thinking as the intention is to achieve streamlined Internet governance through decentralization of responsibility and power to promote cooperation between the state, private sector and civil society. Although this approach is generally seen internationally as best practice for cyber security (Carr, 2015), even in Norway, where public-private trust relationships are deemed to be good, there are tensions arising from established power dynamics between actors, as those stakeholders deemed to be the most appropriate for good governance have so far failed to come together to address the key challenges and vulnerabilities presented through cyberspace (Helkala and Svendsen, 2014; Muller, 2016).

The fact that the Norwegian government allows sectors to develop with relative autonomy makes it important to understand cyberpowers influence on how institutional development processes associated with cyberspace operate across sectorial domains. The typology of this rapidly developing phenomenon mean appreciating motivations and conflicts related to value-based decisions – that frame selective actions and implementation of protocols intended to prevent abuses of cyberpower – become crucial if trust, holistic approaches and collaborations are to form the foundations of development actions (Hartley et al., 2002; Tapscott, 2014). This is corroborated by earlier research that highlighted key national challenges relating to cyber governance across government institutions; and a lack of inter-organizational coordination and public-private partnerships leave uncertainty concerning implementation of: “. . .international standards, recommendations and best practices into national strategies and guidelines” (Helkala and Svendsen, 2014, p. 10).

Multiple complex processes and interactions occur at the interface of institutional, organizational and individual development (Hartley et al., 2002; Leftwich and Sen, 2011). When interfaces are less visible and shifting in a context of value-based conflicts it is important to learn from different perspectives and understand how competing processes create tensions, due to inappropriate structures or inefficient practices. Deeper appreciation for and understanding of the institutional landscape can support better governance action capable of coping with and responding to: “tensions, conflict and (re) negotiation” (Wuyts, 1992, p. 280).

In this study, the complex issues around the governance of cyberpower will be treated as emerging and increasingly dominant orthodoxies that are disrupting established patterns of living (Thomas, 2000). By deductive analysis of empirical interview data (Elo and Kyngäs, 2008) this research explores perspectives from key organizations within seven Norwegian sectors; this research seeks to deepen understanding and inform for greater appreciation of the discourse convergence and divergence involving multiple stakeholders, disciplines and governance levels in society, that all contribute to an institutional landscape that is being shaped by a new form of power. The State of Art for this paper is structured in a Complexity, Difference, and Emergence conceptual frame. The Section “Methodology” describes the qualitative research approach and design. The Results are categorized and presented thematically. Further, the Section “Discussion” frames key findings in the wider problem context. The Section “Conclusion” makes a number of concrete recommendations as well as plan for Section “Future Work” to add depth and validity to this initial work.

STATE OF ART

Around the world, governments of both developed and developing economies are taking action at national level to address cyber security concerns [. . .] there are few obvious policy recommendations. . . (Peña-López, 2016, p. 223)

In Norway, the unevenness between sectors, i.e., their relative autonomy – represents institutional contradictions that can lead to unintended consequences (Engberg-Pedersen, 1997) as processes of divergence and convergence occur as reactive/un- planned policy, practice, and governance responses to emerging challenges.

The CoDE conceptual framework (Pinder, 2016) is a highly relevant device for opening up and deriving insights into the ways in which cyberpower penetrates across *Complex* institutional landscapes – in Norway as well as globally – characterized by multiple interested parties, multiple fields and multiple levels of governance. Appreciating how the *Difference* in organizational identities and understandings might affect institutional development processes as each sector comes with its own interests, values, agendas, and culture may help to explain why cyberpower – as an *Emerging* and dynamic governance problem, characterized by uncertainty and unpredictable outcomes – is difficult to grasp beyond military applications.

The independent and overlapping elements of the CoDE framework can help to explain an environment where the effects of cyberpower are delivering impacts upon social change processes that cannot be known in advance (Thomas, 1996). The CoDE framework implies that institutional development processes, taking place in over-lapping spheres (Leftwich, 1996) occur in a multitude of ways and that, given the trans-boundary nature of the cyberpower phenomenon, situating organizations in their national institutional context may not necessarily define: “what is deemed possible, acceptable and legitimate” (Hartley et al., 2002, p. 394). Instead there are competing paradigms as values, rules and norms (Brett, 2000) within one institution may not be compatible with emerging institutional characteristics of another. One outcome of this could be constrained action, as the effects adversely impact organizational processes at the social and cultural system levels (Hartley et al., 2002). This reinforces the importance of building connections between institutions through cooperation – that may require forms of interagency collaboration (The Open University, 2000) – and vertical and horizontal co-ordination. It also shows how institutions: “. . .by producing stable, shared and commonly understood patterns of behavior, are crucial to solving the problems of collective action amongst individuals” (Brett, 2000, p. 18).

Complexity

From a development management perspective, it is understood that institutions provide the frameworks within which organizations operate. Similarly: “effective organizations depend on the existence of institutions which constitute the rules which everyone – including the managers – must accept” (Brett, 2000, p. 19). This builds on the idea that institutional change cannot be achieved by a single agency with control over resources and processes (Thomas, 1996). This was echoed in a recent Norwegian Government document that specified that a direct consequence of being one of the world’s most digitized nations is the level of vulnerability that digital dependency brings, and dealing with this operational problem at sector or national level cannot be managed by one single agency (Stortingmelding, 2016–2017).

Authors such as Nye (2011) and Jasper (2012) identify the state as the balancing agent when complex tensions arise from the dependency vs. vulnerability paradox in conditions where: “The more advanced a nation becomes, the more it relies on access to the commons and the more vulnerable it becomes to the loss of access” (Jasper, 2012, p. 60). This captures the Norwegian context in relation to the complex implications of cyberpower and how effects can influence institutional development across domains. Norwegian researchers and cyber security experts have called for greater governmental responsibility and control in securing a cross-sectorial approach (Helkala and Svendsen, 2014; Norwegian Centre for Information Security [NorSIS], 2016). For example, analysis of Norway’s cyber and information security strategy identified three levels of potential target; national, organizational, and individual. Each level has assets to protect, but irrespective of criticality, each is vulnerable to nefarious actors using cyberpower to target them. In a context of digital dependency, the study identified a lack of know-how and functioning legal frameworks across multiple fields within which to manage the positive and negative effects of cyberpower (Helkala and Svendsen, 2014). This raises management questions when sectors have designed, developed, and directed independent cyber security solutions, meaning vulnerabilities and dependencies are embedded in cultural collectives and institutions (Crewe and Axelby, 2013) that span multiple interested parties, multiple fields and multiple levels.

In Long’s (2001) definition of power he states how power is: “the outcome of complex struggles and negotiations [. . .] and necessitates the enrolment of networks of actors and constituencies” (p. 71). When we consider that the real world effects of cyberpower are only emerging through an ever expanding and entangled digital network of known and unknown actors, then the outcomes, or the potential of power exercised through cyberspace: “. . . clashes with our habitual patterns of the classification of things” (Betz and Stevens, 2011, p. 128) on the basis of authority, status, and reputation. Threats to any one of these can present institutional and capacity constraints to the effective functioning of inter-organizational relationships and policies on many levels, and across sectorial fields (Kickert et al., 1997).

Working for effective collaboration – the type that creates collaborative advantage for broader social objectives (Huxham, 1993) – between different organizations becomes a complex struggle as each one independently seeks to manage tensions created by various forms of power delivered through cyberspace. This reveals how cyberpower, in line with other dimensions of power is relational, its struggles lie at the heart of institutional development and it needs to be interpreted in the complex context in which it is being conveyed (Rowlands, 1997; van Haaster, 2016).

Difference

We can no longer take for granted what Thomas (1996) wrote about in terms of understanding development as a: “. . . long-term process of social change” (p. 98) or that it: “cannot be controlled by human agency” (p. 97). What we are witnessing today is human agency empowered by cyberpower influencing and driving social change at rates traditional good governance systems, and codes of practice cannot control (Stevens, 2015). When state frameworks are unable to manage dynamics central to multi actor steering, such as communication and control (Rosenau, 1995); then good purposive governance is challenged. From a global macro level, we are witnessing technological advancements outpacing and outperforming human agency (Castells, 2011). Simultaneously at state level – as Norway is experiencing – there are concerns regarding how to manage and govern consequences of cyberpower, such as tensions arising from the aforementioned digital dependency vs. digital vulnerability paradox.

When the rules of the game are changing (North, 1990) and tensions lead to: “imperfect compromises” (Nye, 2011, p. 16), then managing and operating in this complexity may require greater appreciation of the digital environment and the space it opens up for cyberpower to influence institutional landscapes. These conditions reflect the idea that understanding where relative power lies and identifying room for maneuver may be more important than specific skills (Thomas, 1996). A national study into Norwegian cyber security stated that appreciating cyber security culture: “. . . touches upon some of the most profound questions for development” (Norwegian Centre for Information Security [NorSIS], 2016, p. 13). For some, technology and its power can: “. . . take us into an age of barbarism that will make fascism look like an exercise in charity and human progress (Courneyeur, in Tapscott, 2014, p. 387); for others, it creates a new environment for collaborating on shared interests (Tapscott, 2014). These polarized perspectives resonate with the idea of: “bringing together those with complementary needs” (Thomas, 1996, p. 107) and presents the opportunity to move governance approaches and thinking to: “conceptualizing a whole development management arena as an inter-organizational domain” (ibid, p. 107).

It is generally accepted that best practice for mitigating negative effects and leveraging positive effects of cyberpower is for organizations to adopt a holistic approach (Castells, 2011; Nye, 2011; Jasper, 2012; Tapscott, 2014; Hagen, 2016; Norwegian Centre for Information Security [NorSIS], 2016). Inevitably though, rather like evaluating good practice (Everitt, 1996), agreeing on a best practice is contested. If organizations are to avoid collaborative pitfalls arising from known and unknown vulnerabilities (Huxham, 1993); then a holistic approach will require negotiation of values, goals, interests and meaning agendas between organizations prior to any formal or informal process of co-ordination/co-operation or collaboration occurring.

The key to achieving the profits of digitalization is: “collaboration and openness” (Peña-López, 2016, p. 223). Implicit in collaboration are the functions of negotiation, information sharing, and transparency (Robinson et al., 2000). As valuable as these concepts are for institutional development, they generate feelings of vulnerability at a personal and organizational level, as they demand the giving up of power for progress. In a development landscape with no clear architecture or governance systems, attitudes to collaboration can harden, pushing organizations apart as they are less willing to embrace collaborative opportunities (Turkle, 2011; Norwegian Centre for Information Security [NorSIS], 2016); due to the value-based conflict between them and the transaction costs (Ouchi, 1980) involved in collaboration. Even so, these functions are seen as necessary for implementing holistic approaches to managing the effects of cyberpower (Thomas, 1996; Nye, 2011; Castells, 2011; Tapscott, 2014).

There will come a point when the requirement for inter-organizational negotiation becomes real and organizational collaboration needs to aspire to more than just a token concept (Huxham, 1993). This assumption is drawn from the idea that: “Before embarking on a strategy of coordination it is important to check that the potential for collaboration exists” (The Open University, 2007, p. 70) among different stakeholders. In this context, aligning collaboration with coordination and cooperation, will see collaboration going beyond its role of achieving influence in public action (Thomas et al., 2001), to one of adding a deeper level of understanding concerning how might cyberpower be driving inter-organizational behavior.

In an uncertain or shifting landscape (Hartley et al., 2002) understanding management approaches across critical sectors may reveal organizational blind spots, blurred boundaries, and how different organizational types are responding to emerging cyberpower effects in contexts characterized by value-based conflicts and multiple competing actors (Thomas, 1996). Aligning governance frameworks with real world emerging cyberpower effects driving institutional development, can build inter-organizational relationships that support collaboration within a digital society.

Emergence

Considering the level of digital resource dependency in Norway, one could assume that the state backed sector-principle and a multi-stakeholder approach to cyber security forms a solid: “. . . basis for organizational linkages” (Salancik and Pfeer, 1978; in Thomas, 1996, p. 107). In this context, multiple stakeholders have a part to play in managing factors that impinge on Norway establishing: “the necessary preconditions” (Muller, 2016, p. 2) for protecting assets from vulnerabilities presented through cyberspace. This is critically important as it reveals that environments – framed by cyberpower – are emerging and

presenting interesting challenges to theories and practice of governance. Most significant is the idea, referred to above, of development and its management as being a shared responsibility (Thomas, 1996).

Learning from the Norwegian context may have wider applications. For example, Crewe and Axelby (2013) discuss the idea of time following linear anthropological steps in modernity theory. This idea is challenged as Internet access becomes ubiquitous and the North and South experience the effects of cyberpower together. Additionally, ideas of dependency and paternalism can be revisited as mechanisms of power are redistributed, creating an environment conducive to collective self-mobilization capable of unsettling democracies, as everything has become dependent upon a system that: "... makes it easier to subvert and harder to govern" (Betz and Stevens, 2011, P. 135). As digital citizenry expands, the need for leadership and systems of governance with the capacity to operate in ways that mitigate the negative effects of cyberpower are necessary to support transformations in developed and less mature institutions in developing countries (Goodhand, 2006; Tapscott, 2014; Bellinger, 2016).

New tensions and conflicts created by the effects of cyberpower add uncertainty to processes of institutional development. For example on the one hand, governments have to devolve: "... responsibilities and authority to private actors" (Nye, 2011, p. 16) in order to ensure state cyber security. This makes for fragmentation and inefficiency in operationalizing cyber security provision. On the other hand, governments are being accused of not taking enough responsibility to ensure citizens are correctly educated, or being told they need to do more to: "... ensure an efficient and unified approach..." (Norwegian Centre for Information Security [NorSIS], 2016, p. 79) to meet the challenges presented by cyber. Investigating amongst key stakeholders the processes, structures and capacities required to manage such tensions, uncertainties and emerging concepts can provide insights into achieving organizational collaborative capabilities (Huxham, 1993). This is consistent with the literature study that identified the need for greater collaboration, if managers hope to effectively control development in a digital society (Huxham, 1993; Nye, 2011; Tapscott, 2014; Hagen, 2016).

METHODOLOGY

The purpose of the methodology was to open up conceptual boundaries and where possible build a more coherent understanding for the term cyberpower, and its real-world effects. Where people don't have knowledge due to lack of data or experience, this exploration can support understanding (Blackmore and Ison, 2007).

The levels of uncertainty surrounding the effects of cyberpower show how it is both a real and emerging challenge. This necessitated a principled investigation to ensure the researcher gained an evidence-based understanding of the kinds of institutional and capacity constraints that restrict or facilitate different organizations to get things done – or not – within this environment of uncertainty. Establishing what is good or what is bad practice in uncertain institutional landscapes can become blurred when moral, empirical and ethical narratives vary. The intention of the methodology was to support an exploration of a shared, contested and emerging problem that is revealing itself as a dominant force over the developed and the developing.

The author purposely chose to sample individual stakeholder respondents from within seven sectors: Political, Military, Economic, Social, Infrastructure, Information, and Diplomatic as the focus of the analysis. This list is not exclusive but represents institutions that use cyberspace to: "create advantage and influence events" (Kuehl et al., 2009, p. 38) in Norwegian society, as well as internationally. The respondents were coded for in text referencing when citing evidence as follows: **PR** (political respondent: Senior member of Parliament); **DefR** (defense respondent: senior leader for military operations); **ER** (economic respondent: senior digital security engineer); **SR** (social respondent: international security & defense expert); **IR** (infrastructure respondent: head engineer for an energy directorate); **MR** (Media respondent: expert in media leadership and innovation); **DipR** (Diplomatic respondent: leader for digital strategy).

It was expected that the researcher would hear respondents presenting complex, different and emerging themes relating to cyberpower effects. Based on key themes that came out of defining and analyzing the problem, five categories were identified: *cyber governance*, *holistic approach*, *multi-stakeholder model*, *new approaches*, and *behavior of interested parties*. It was hoped that specific opinions and perspectives concerning these thematic areas would emerge.

To reflect the goals of the research, qualitative data gathered through semi-structured interviews was used as the primary method to inform about the development of operational strategies to manage cyberpower effects. The Overarching Questions (OQ) listed below in **Table 1** represent the main lines of enquiry. They were designed and applied to act as prompts, in order to allow for assessment and discussion within each of the five categories.

The limited sample size means data is partial and only presents selective visibility of each sector (Mukherjee and Wuyts, 2014). However, deciding to secure subjective information from senior respondents as the primary data source helped the researcher learn from people who know within operational environments (Hanlon, 2014). A consequence of this method is possible bias and value laden data as: "...those in positions of power may also be in good positions to see and explain what is going on, even though their self-justifications are likely to be biased" (Thomas and Chataway, 2014, p. 333).

TABLE 1 | Presents the overarching questions listed by category.

- (1) Cyber governance
 - (1.1) What is understood by the term cyberpower?
 - (1.2) What do key stakeholders understand by the terms *dependency* and *vulnerability* in the context of the operation of cyberpower? In what ways are the terms seen as being in tension (or not)?
- (2) Holistic approach
 - (2.1) In what ways are the tensions between vulnerability to and dependency upon cyberpower manifested in operational-terms?
- (3) Multi-stakeholder model
 - (3.1) What kinds of processes and structures could support managing the tension between vulnerability to, and dependency upon cyberpower?
- (4) New approaches
 - (4.1) What might a bottom-up approach to managing the effects of cyberpower entail?
- (5) Behavior of interested parties
 - (5.1) What kinds of institutional and capacity constraints work against effective collaboration/co-ordination between organizations, and how might those constraints be managed and negotiated?

Given the emerging and non-boundaried nature of this problem (Woodhouse, 2014) the researcher was aware that organizational culture would frame language. This presented potential contestations based on partiality of knowledge consisting of multiple truths. When perceptions are being framed by the wider context within which they operate (Everitt, 1996), then questions arise relating to what each respondent considered and evaluated as good practice when managing cyberpower in a democratic society. This richness supported the choice of conceptual framework as it brought forward the complexity and emergence of a developing landscape around cyberpower. Additionally, the researcher needed to be aware that each organization is living with pressures exerted on them from the broader environment. These shape the organization's actions and influence how they choose to respond to interview question (Roche, 2014).

Reflecting on the idea of shared responsibility (Thomas, 1996) highlights the fact that citizens have a participatory role in shaping and defining how institutions need to develop in response to cyberpower. However, concerns about data quality arising from the lack of problem knowledge amongst random samples meant the researcher decided not to interview members of the public. Not having this data leaves a gap in perspectives that would have contributed to the project. Especially considering the earlier definition of cyber security as protecting individual and societal wellbeing. This is certainly true in light of the current view that participatory – or what appears to be commonly referred to now as a holistic approach – is deemed the most appropriate for managing digital uncertainties (Tapscott, 2014; Hagen, 2016).

Respondents answered critically to interview questions as they reflected on the complex problem. This triggered the researcher to formatively question how their appreciation for the problem was developing. In almost all cases the respondent reported a change in understanding and perception. This shows how the line of questioning prompted focused reflection on this emergent theme, indicating that respondents were willing to embrace complexity and seek to understand it: "...rather than oversimplifying reality..." (Mayoux and Johnson, 2014, p. 186) or simply taking issues for granted.

The seven informants – two female/five male – are leading in a field they have not yet mastered, nor fully understood its true complexity; yet they act in, on and around this continually contested space every day (Goodhand, 2006).

This study was carried out in accordance with the recommendations of The Norwegian Data Protection Authority. All subjects gave written informed consent to be interviewed. The subjects have been anonymized, no sensitive personal information was collected, and no data has been stored electronically.

RESULTS

Data was analyzed using the five thematic areas: cyber governance, holistic approach, multi-stakeholder model, new approaches and, behavior of interested parties. Within these categories a number of key sub-themes appeared. These sub- themes are presented in **Table 2** and will form the basis for discussion in the next section. The results analysis also looked for correlations and differences between respondents and the literature study. Attention is drawn to themes of variations in perspectives, complexity, uncertainty, and emergence.

TABLE 2 | Lists the key sub themes that appeared during interviews.

Cyber governance	Holistic approach	Multi-stakeholder model	New approaches	Behavior of interested parties
Political role	Sharing	Best practice	Challenge institutional norms	Value conflicts
Influence	Informal collaborations	Conflicting interests	Human factors	Approach to the Sector-principle
Institutional uncertainty about how to govern	Organizational culture relating to risk	Systems of governance	Framed by uncertainty	Willingness to co-operate
Dependency vs. vulnerability		Power relation		Lack of trust
Complex intra-organizational relationships				Collaboration for survival

Cyber Governance

Perspectives varied depending upon how different sectors experience or use cyberpower. One respondent stated that cyberpower is: “not cyberwar” (SR) contra DipR who considered cyberpower to be a term that describes cyber warfare. Another respondent bridged these two polarized perspectives by using the contemporary ‘Hybrid War’ concept to describe cyberpower’s real world capacity to: “undermine and influence another State’s political authority” (PR).

As the examples above show, the *political role* of cyberpower emerged as a common theme among different respondents. Further, respondents commented that it can be used to: “gain power to influence for a purpose” (ER) and, it is how we: “influence people through different levels of power” (SR). For some this was a positive development as it: “protects values, people, info, property, reputation, and operational ability” (DipR). While for others: “it’s a difficult grey-zone” (DefR), and its role has more negative connotations: “using and modifying information technology for your own purpose” (ER). Also, and in line with the problem definition, it can be both: “Cyberpower is maybe the power to influence a target group, or a population, through cyber means; for personal objectives – good or bad” (IR).

Corresponding with the Kuehl et al. (2009) definition of cyberpower, all respondents, including those who had either not heard the term before, were unfamiliar with it or found it “comprehensive” (DefR), used the term *influence* when describing their understanding of cyberpower.

Further discussions revealed *uncertainty how to govern* based upon institutional understanding. All respondents were not surprised different organizations/respondents had different understandings of cyberpower. As one respondent explained: “organizations have different cultures, and each is expected to look at cyber risk and threats differently” (IR). This can be related to political tensions around usage, i.e., the military uses the same national infrastructure that citizens do. Or as another commented: “cyber is creating an arena for political development” (PR).

Uncertainty was an emerging shared theme concerning small vulnerabilities that can present massive consequences. This uncertainty is driving immediate reactive practices (ER; DipR; IR) over long-term strategies. All respondents agreed that dealing with the volume of network vulnerabilities complexifies and negatively affects longer-term planning. For example, in journalism, a consequence of the operation of cyberpower is: “the amount of uncertainty today means so much confusion looking into tomorrow” (MR).

Governance uncertainties were again revealed as dependency and vulnerability were reported to frame an uncertain institutional landscape as organizations may well act in ways that have consequences for social change, as traditional systems of governance and codes of practice are challenged (Stevens, 2015). As one respondent commented: “traditional means of protecting sovereignty lack the necessary control instruments to manage cyber effects” (DipR).

If the operation of cyberpower is creating the above context then a respondent opinion that attempts to resolve tensions from the *dependency vs. vulnerability* paradox will follow the same developmental path as the analog world did, presents an interesting discourse. The respondent stated: “People and their ideas have not changed [. . .] we are not more honest, our intentions are no better, our wishes for intake and welfare do not change” (PR). The PR respondent followed this by saying mechanisms for managing the operation of cyberpower will: “become more dramatic” and “need to involve national digital borders” (PR).

Inevitable tensions for a small nation like Norway – that has physical territory but everything it does is dependent upon digital interactions with the international community – arise from the scenario presented by PR. These were emphasized by DefRs description of future tensions if the state controls Internet freedoms through digital borders and monitoring. This the respondent said: “threatens a human right, the economy and welfare security” (DefR).

Tensions are apparently being hidden as a result of vulnerability: “tensions don’t manifest, if they did, then actions would be taking place to address the problem” (SR). Soon after this interview Norway’s largest digital provider Telenor was accused of failing to take their responsibility to society seriously. The company apparently chooses not to report all digital crime because they are afraid to lose control and do not wish to co-operate with the police. In response, Telenor stated they do not have time to review and report all incidents (Njie, 2017).

The DipR presented an interesting situation that adds complexity and highlights that difference in *intra-organizational relationships* affects institutional development processes. The respondent explained how one group within the Norwegian Foreign Office runs cyber business, i.e., daily operations. Whilst another group runs the international political policy face of cyber, rarely do the two groups meet to calibrate policy, practice or governance.

Holistic Approach

As a member of the committee who established the national cyber incident reporting process, IR was insightful and un-surprisingly loyal to the system designed to be inclusive and ensure information *sharing* across sectors. The IR did acknowledge that the process is not universally applied or governed across sectors.

A comment by ER revealed how *informal collaborative* processes can take place beyond institutional frames. The ER explained how they communicate with online groups who analyze malicious malware, as a means of finding solutions to new vulnerabilities. Similarly, MR noted how journalists have to look elsewhere to find the truth, i.e., away from: “institutions of democracy such as the White House” (MR).

The ER formally worked in the Defense sector and highlighted how different *organizational cultures* shape how they respond to tensions. The ER described how availability is an exercise in accepting risk in the Norwegian economic sector. Meaning they prioritize network availability, such as BYOD or mobile banking. However, the Defense see this exercise in risk acceptance as unnecessary or not a priority.

Multi-Stakeholder Model

The IR commented that sharing knowledge makes knowledge and power grow. This reflects the literature that calls for increased power and understanding through sharing of information beyond institutionalized boundaries (Thomas, 1996; Castells, 2011; Nye, 2011; Tapscott, 2014). Interestingly, IR followed this statement with skepticism toward cross sector collaboration. In IRs view, the core business of cyberpower for the military is different to other sectors and: “It’s not necessarily true that if you are good in one domain you can be good in another” (IR). It was unclear if this was an organizational culture issue or a question of *best practice* relating to skills and capacities not matching.

Similarly, MR stated that journalistic organizations are working hard to develop ethical standards and new institutional best practices in response to cyberpower effects such as online fake news. However, they are unwilling to coordinate outside of their sector for fear of diminishing the integrity of the journalistic profession.

The ER and DipR called for more government regulation to: “address concern and confusion about what is going on in cyberspace” (ER). SR acknowledged some top-down efforts were in place, however, complexity arises due to *conflicting interests* as: “everyone has different premises and therefore how do you know the model is correct” (SR). Meaning theoretically: “Things will never be fine; we are always on our way to an improved state” (IR). Or the problem is so complex and emerging, that finding/negotiating an ethical balance between dependency and vulnerability is severely contested when authorities: “start watching what you are doing on the net [. . .] then the state becomes something else” (DefR). This is significant when compared to comments about mechanisms for managing cyberpower made by PR in section 4.1 Cyber Governance.

There were differences in perspectives regarding *systems of governance*. PR judged a digital society needed a political system that was up to date with the challenges, and Norway: “being small and democratic should be OK” (PR). In contrast, DefR questioned how the Norwegian democratic system is going to cope with big emerging challenges expedited by cyberpower that see voters seeking: “less uncertainty, less integration, and less globalization” (DefR).

If each sector develops independently with its own values and cultural dimension, cultivating: “truths of practice” (Everitt, 1996, p. 179) in relation to managing vulnerabilities. Then they are able to justify (in theory) their unique role in contributing to a just, open, safe, and secure society. As SR commented: “The problems are not new, they are just more interconnected. We need to identify what is different” (SR). However, without a common platform for collaboration the status quo - represented by *power relations* framed in the sector-principle - is not challenged. This is significant when institutional development depends upon the level and sum of relationships between people and organizations (The Open University, 2007).

New Approaches

All respondents agreed that leadership and generational factors have a role in managing the effects of cyberpower. The DefR called for new leadership philosophies that mirror technological solutions and reach beyond a: “fenced in physical domain” (DefR). This was explained as leadership driven by capabilities and creating effects in wider networks. Moving from leadership being simply about position, ownership and power, to styles that operate with bigger pictures in mind. This concept echoes with the idea of knowledge sharing making power grow (see IR, section “Multi-Stakeholder Model”). These ideas present a value-based conflict as they *challenge institutional norms* for those currently occupying senior positions. As they imply relinquishing forms of power.

Considering the above, with regards to preparing the next generation of leaders/managers, implies the requirement for scaffolding innate technical skills and encouraging flexible cognitive strategies for operating in the new digital economy (Homan and Hancock, 2017; Knox et al., 2017). The PR respondent gave an opinion that presents a challenge to these ideas when describing a real-world context: “The younger generation is more segmented and have no need for broad perspectives” (PR). The PR explained that this has a negative/weakening effect on democratic development as it can lead to political polarization and a

less dynamic political debate. These contrasting views emphasize the uncertainty surrounding *human factors* in digital societies.

The PR and IR respondents commented that state apparatus such as banks, critical infrastructure and democratic process are being threatened in: “new ways” (PR); leading to increased political responsibility to manage it. This can be seen as a call for new approaches to managing cyberpower effects that require *new literacies* (Kellner, 2002) at political governance level. Another respondent noted that a vulnerability arising from mass-media is that people: “. . .are not skilled enough to know how to trust it” (MR). New literacies identified in the literature study are those that mirror the digitally interactive environment today's students have grown up in and have the potential to answer the question: “where does trust come from?” (Harriss, 2000). As a respondent noted: “Leadership today is more about the kind of person you are not the kind of age you are” (IR).

Behavior of Interested Parties

Individual and organizational *value conflicts* surfaced that create uncertainty and tension for effective collaboration. Surprisingly, little was presented to indicate longer term solutions that go beyond institutional frames (The Open University, 2000) to manage these tensions. Norway is rapidly digitalizing as a condition of a modern society (Stortingmelding, 2016–2017); and by doing so, is knowingly increasing vulnerability to negative development (Jasper, 2012). A respondent made this point clear: “we are pushed to use the cyber domain” [and establish a] “shared security culture within a domain that is inherently vulnerable” (DipR).

It would appear that *approaches to the sector-principle* may be leading to negative developments in the face of cyberpower challenges. This may be due to multiple conflicting formal and informal policy and practice agendas shaping progress. The sector-principle was described as: “good, but a big challenge” (DefR). Further, three constraining factors were presented; “It’s very hard to coordinate cross sector as each sector has its own Department; threats in one sector may not get heard by another; the principle makes it hard for effective use of time and resources” (DefR). These conditions are compounded by powerful unwritten rules that incentivize or sanction depending on different interpretations (Brett, 2000). One such example is: “When it comes cyber, its effects and managing collaborations, industry is the one leading the way and setting the agenda” (IR).

The *willingness to co-operate* across sectors is restricted for the exact reason that: “. . .it implies reciprocal sharing of rights and responsibilities” (Robinson et al., 2000, p. 226). When cyberpower is added to this context, with its power to outpace traditional good governance and codes of practice (Stevens, 2015), then a conflicted institutional development landscape is manifest. If interested parties want to develop, then it: “may require a new way of collaborating” (DipR) as conventional models of sharing/information exchange may no longer apply. However, when generalizing about current behaviors, a respondent commented: “You can build a network, but it doesn’t exist if it is not used” (PR).

In a time when *lack of trust* – due to multiple vulnerabilities – is a major factor shaping action, all respondents believed there is a will to collaborate and co-ordinate to improve management of vulnerabilities arriving through cyberspace. However, when each sector investigated; political, defense, economic, diplomatic, infrastructure, media and social has its own policies, domain of responsibility and private sector service providers; then the idea of co-operating with another sector – that has a completely different set of operating conditions and core business relating to how it applies or manages cyberpower – was seen as something that would create tension (IR; MR).

The MR gave an example of *collaboration for survival*. In the financial sector banks are collaborating to build power in the area of digital payment via mobile apps. This way smaller banks gain strength and improve their survivability against future ‘online’ – international – competitors (Reuters, 2017). In the media sector: ‘no option’ collaboration was described as ‘convergence’ and exemplified by the amount of mixed content online (MR). The MR commented that agreeing the ethics of media and journalism when cyberpower is reshaping the core of the industry is a major persistent challenge. This is a consequence when the rules of the game are changing (North, 1990) and tensions lead to: “imperfect compromises” (Nye, 2011, p. 16).

DISCUSSION

The following evidence-based discussion relates empirical findings to the characteristics of the problem. The intent is to nudge thinking to avoid taken-for-granted practices that may be blocking institutional development (Everitt, 1996) and where possible; open the debate among stakeholders concerning the complexity, difference and emerging ways cyberpower is impacting institutional development.

The different cross sector perspectives revealed by respondents contribute to explaining why cyberpower is not yet a fully understood term. As the results reveal, cyberpower was shown to influence organizations differently depending upon their domain of interest. Significantly, the results not only align with the literature, they extend our understanding regarding the ubiquity of cyberpower. Critically the way cyberpower affects institutional development, across all levels of society, make its role inherently political (Standt, 1991) and therefore a governance challenge. The complex characteristics of cyberpower – most prominently seen as emerging positive uses and negative abuses – ranging from those that enrich human life through access to information, to those that undermine another land's political authority; imply the need for a wider political space if there is to be a common platform for collaboration (Wood, 2003). Taking a shared responsibility (Thomas, 1996) approach to cyber security – in the form of jointly developed national strategies and guidelines (Helkala and Svendsen, 2014) – could present opportunities for improving certainty around governance policy and practice. This may in turn encourage better intra and inter-organizational relationships for institutional development.

The finding that one respondent found cyberpower a difficult term (IR), another didn't use it (PR), and one viewed it as comprehensive (DeFR), is a valuable outcome. Not only does it emphasize the richness of the problem, the fact that respondents were able to locate themselves and their organization within the problem space, means it has some level of relevance for them. Going forward, defining cyberpower in a way that demands less explicit knowledge of the term 'cyberspace' and less effort to unpack the slightly abstract terms: 'operational environments' and 'instruments of power' (Kuehl et al., 2009, p. 38) could make the concept more approachable. In practical terms this would help penetrate the consciousness of a wider demographic by situating the word *cyberpower* into their everyday lexicon. This would support moving understanding forward from the current state where cyberpower has relevance, but conflicting interests and value conflicts mean it is not yet a well categorized or operationalized concept.

The interview responses from ER, DipR and IR build on the understanding that organizations are relying on individualized assets to seek immediate security priorities ahead of pursuing long-term goals (Wood, 2003). If this deliberate survival strategy response to dealing with uncertainty reflects organizational best practice in digitally advanced Norway; then the likelihood is that governance uncertainties in developing states – with weaker institutions and governance mechanisms – could be more of destructive and destabilize their digital moral universe (Wood, 2003; UNWOMEN, 2015). The operation of cyberpower is increasing vulnerability and creating consequences for dependency that present a new 'Faustian bargain': staying dependent, staying vulnerable. This occurs as the negative effects appear to frame: "dysfunctional time preference behavior" (Wood, 2003, p. 455). As reported by ER, DipR, IR, and MR, institutional governance uncertainty when dealing with immediate vulnerabilities and insecurities arriving through cyberspace, displaces individuals and organizations ability to focus on long-term strategies (Wood, 2003).

The near horizon debate in Norway concerning digital borders will be framed by governance uncertainty and could have destabilizing effects as it concerns not just: "human rights, the economy and welfare security" (DeFR). It will also influence organizational cultures, environmental factors and power dynamics between government, the private sector and citizens. Institution leaders need to learn from these tensions and share knowledge gained, good and bad. This is necessary to support longer-term strategies designed cope with cyberpower effects. A number of respondents described the non-collaborative practices of interested parties and unwillingness to share. When attempting to manage the effects of cyberpower, such issues should be addressed, and institutional building should be seen as: ". . .an incremental, sequential process which depends on learning and stimulates self-transformation" (Harriss, 2000, p. 234). Meaning that collaboration, in the form of information sharing, can form the foundation of co-operation based upon communication, reframing of problems and shared learning. If building co-operation is a step to institution building (Harriss, 2000), then the results of this research reveal the pressing need for new approaches that build collaboration capacities capable of facilitating better co-operation over time.

Institutionalized systems of governance and practices framed in policies: “crafted to meet the needs of the past” (Tapscott, 2014, p. 390) are struggling to: “get ahead of the game for long enough to really commit resources for the future” (Wood, 2003, p. 458). This may be the case in Norway as national governance structures limit the prospect of open collaboration in the face of emerging vulnerabilities arising from digital dependency. The comments by DefR that the sector-principle is a big challenge and makes it hard for effective use of time and resources counter the assumption that the sector-principle and a multi-stakeholder approach to cyber security form any kind of best practice (Carr, 2015), or solid enough basis for organizational linkages (Salancik and Pfefer, 1978; in Thomas, 1996). Any delay or failure to adapt to a problem that is redefining institutional rules of the game in society (North, 1990; Tapscott, 2014) will only increase transaction costs in the long term (Ouchi, 1980).

As the results indicate, the effects of cyberpower are creating an institutional landscape framed by leadership uncertainty and a complex struggle about what is: “getting the work done by the best means available” (Thomas, 1996, p. 100). A consequence of this may be more government control (Helkala and Svendsen, 2014; Tapscott, 2014; Norwegian Centre for Information Security [NorSIS], 2016) resulting in top-down command and control mechanisms (Fayol, 1916/1949). For the respondents in this research, this development may represent a ‘more dramatic’ governance mechanism (PR), the idea of the state becoming something different than it is today (DefR), or an approach that may falter due to conflicting interests concerning models of governance (SR). In Norway, this praxis would run against cultural norms and meet significant resistance. Therefore, maintaining the status quo and pursuing the management policy of empowering and enabling (Paton, 1991) sectors – that is “molded to the interests of [...] the state” (Thomas, 1996, p. 104) – will require greater space for expressive innovative collaborations if Norway is going to manage the tensions between vulnerability to, and dependency upon cyberpower.

The problem definition identified that managing cyberpower may require new and more adaptive approaches beyond current institutional frames (Conklin, 2006; McDonnell, 2016). The results build on this as respondents identified new human factor capability-based leadership models that create effects in the wider network (DefR) and are less about age and more about personality and knowledge (IR). Further, when Castells (2011) and Tapscott (2014, p. 89) refer to building relationship capital through a collaborative infrastructure, then the above approaches may well support prosperity through the practice of trust, and joint decision-making by providing the: “cultural glue [for the] ... new [digital] developmental paradigm” (Castells, 2011, p. 213).

New literacies that integrate conceptual and skill areas (Thomas, 1996, p. 100) are those that include critical thinking, complex problem-solving, expert communication and applied knowledge in real world settings (Peña-López, 2016). At a personal and organizational level this implies the need to develop a range of capacities capable of building the relationship capital necessary for managing engagement with the digital world.

The interview data highlighted that modes of governance for managing cyberspace – and the vulnerabilities it presents to public and private entities – could lie beyond the current sector-principle institutional frame. Power dynamics between sectors (Muller, 2016) need to become more than barriers to comprehensive cyber security. Power needs to become the catalyst for development of new knowledge through improved collaborative behavior. All respondents stated the need for better organizational strategies, a greater capacity to find long-term solutions to novel vulnerabilities and identified the understand function as a weakness across sectors. Choosing *not* to manage the dependency vs. vulnerability paradox could be a source of failure as the negative effects of cyberpower lead to institutional decay.

CONCLUSION

We are witnessing powerful effects arriving through cyberspace that present real world shared problems that could not have been foreseen. A consequence of this is the political reality that existing national structures of governance may be struggling to cope. When a functioning society and all its assets – tangible and intangible – depend upon cyberspace then a holistic approach explicitly frames all parts of the whole (OED, 2017). This means that cyberpower and its unpredictable impacts on social change processes (Thomas, 1996) demands greater attention.

Uncertainties emerging from cyberspace will persist as technology develops, governments support digital rollout for economic development, and increased network capabilities lead to planned positive outcomes and, emerging negative outcomes for people and organizations dependent upon cyberspace. Vulnerabilities are leading to time dysfunctional behavior and possible destructive decision-making in the form of for example imposing digital borders. The implication for institutional development is how to create the necessary national trust conditions across and within sectors that encourage openness, transparency and information sharing for positive institutional development in times of uncertainty.

The idea that understanding is no longer a condition of knowing but an activity involving dialog (Everitt, 1996) frames the current situation regarding man-made cyberspace. Dealing with emerging challenges and: “fundamental changes to society” (Tapscott, 2014, p. 386) may require dialogical activities that realign institutional frames to ensure what we created – but no longer understand (Nye, 2011) – does not undermine institutional development processes. As the data from this study reveals, if sectors and organizations are not mandated to follow national cyber incident reporting structures, or are not: “directly subject to a national cyber security policy” (ER); then this demonstrates why leaders need the capacities to work with uncertainty, to negotiate complex institutional landscapes and relationships, understand threats and identify opportunities to bring stakeholders together.

The extent to which the respondents showed an awareness of the need for these capacities within their organization was inconclusive. What is apparent is that advancing institutional agendas in dynamic environments, where outcomes cannot be predicted is more about maintaining current operational output, than investing in human capacities capable of providing longer- term development solutions.

As one respondent noted:

- *The shared perspective concerning cyberpower is that people are reluctant to look too closely at the problem cos they don't know the right questions to ask if they do, and they lack the imagination about what might come or be about to happen. They are reluctant to accept their own vulnerability (DipR).*

Co-operative processes can reveal organizational common ground and interdependencies as opposed to stressing the differences (Robinson et al., 2000). Where collaboration potential exists beyond organizational boundaries (The Open University, 2007), then a new model of collaboration that activates engagement between stakeholders can become a key feature to support shared understanding, founded on common values and goals. Driven by the need to build capacities capable of managing joint vulnerabilities that arrive through cyberspace and contribute to decay or weakening of institutions (Robinson et al., 2000).

The governance challenge, when policies and practices are institutionalized, is apparent in Norway. Transforming the sector-principles' capability to function in a digital development paradigm means moving from a regime of truth that maintains power relations in Norwegian society (Everitt, 1996) to a model capable of responding to the new approaches, opportunities and challenges posed by cyberpower. This study has shown that this will require management of conflicting values, novel developments and emerging contexts, founded on capacities capable of mobilizing resources and shaping alliances (Thomas, 1996).

Recommending practices that can become the strategic corner stone for managing the ways institutional development is affected by the growing influence of cyberpower – such as the dependency vs. vulnerability conflict – will involve new models of leadership that educate and empower-to- enable younger generations to operate beyond structural frames. This will allow for collaborative advantage in ways that are context orientated rather than restricted by hierarchical norms of communication structures (Knox et al., 2018). This means individuals being free to deliver effects in the broader environment beyond organizational boundaries in collaboration with trusted partners.

To conclude, the following recommendations are made:

(a) Further research aimed at defining cyberpower in a way that is more universally appealing and usable. For example:

Cyberpower is the capability to influence tangible and intangible assets through digital means.

(b) Organizations should commit time and human resources to improve institutional development prospects when faced with effects of cyberpower. Not doing so means continuing to contribute to their own vulnerability leaving them more precarious as they: “stretch [...] out a survival strategy” (Wood, 2003, p. 229).

(c) Conceptualize cyberpower as a whole inter-organizational domain of shared responsibility to improve prospects of achieving a holistic approach.

(d) Encourage the merging of inter-organizational boundaries enabling new relationships – grounded in shared responsibilities – to emerge, that can transform management models and strategies.

(e) Encourage expressive innovative collaborations oriented toward co-creation and: “building up the capacity to maintain influence into the future” (Thomas, 1996, p. 103).

(f) See managing cyberpower as a shared development: “activity and attitude” (Wrangham, 2016) founded upon skills such as unstructured problem solving, critical thinking, learning and reasoning. To build these capacities takes modes of education that focus on: “non-routine, higher order cognitive skills”, relating to: “new [digital] economy skills” (Peña-López, 2016, pp. 123, 267).

FUTURE WORK

Cyberpower is creating a context where a lack understanding about tomorrow's threats, leads to fragmentation, inefficiency and actions that: “favor meeting immediate needs over future ones” (Wood, 2003, p. 231). Firstly, bringing stakeholders together – who would not normally interact over this problem – would support a more principled investigation in terms of relationships between actors. Action research of this type would be a valuable next step, as the outcomes may support more evidence-based recommendations for managing collaborations intended to advance institutional agendas in a dynamic environment where outcomes cannot be predicted. Secondly, to add depth and richer comparative evaluations, further data collection from within individual sectors could reveal internal data patterns, as well as allow for increased comparison across sectors at respective hierarchies.

This research contributes empirical data to an emerging and globally shared phenomenon that is: “...posing more questions than answers” (Tapscott, 2014). Through seeking to ground the term *cyberpower* in the lexicon of change agents through a process of interweaving different perspectives and understanding, this study and related future work could broaden the range of conceptual tools available to development managers when addressing the issues of dependency vs. vulnerability.

AUTHOR CONTRIBUTIONS

BK confirms being the sole contributor of this work and approved it for publication.

REFERENCES

Bellinger, G. (2016). *The Open University, T879-16E, Conflict and Development, Week 18 Working with Conflict and Complexity, 6 Making use of Systemic Approaches, Activity 18.8 There are no Perfect Solutions*. Milton Keynes: The Open University.

Betz, D., and Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-power*. London: International Institute for Strategic Studies.

Blackmore, C., and Ison, R. (2007). “Boundaries for thinking and action,” in *Research Skills for Policy and Development. How to Find out Fast*, eds A. Thomas and G. Mohan (London: Sage), 49–73.

Brett, T. (2000). “Understanding organizations and institutions,” in *Managing Development: Understanding Inter-organizational Relationships*, eds D. Robinson, T. Hewitt, and T. Harriss (London: Sage Publications).

- Carr, M. (2015). Power plays in global internet governance. *Millennium J. Int. Stud.* 43, 640–659. doi: 10.1177/0305829814562655
- Castells, M. (2011). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*, Vol. 1. Hoboken, NJ: John Wiley & Sons.
- Center for Strategic and International Studies and McAfee [CSIS] (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Available at: <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf> [accessed March 23, 2017].
- Chambers, R. (1995). 'Poverty and livelihoods. 'whose reality counts?'. *Environ. Urban.* 7, 173–204. doi: 10.1177/095624789500700106
- Chehadé, F. (2014). *Largest Ever ICANN Meeting Convenes in London Affirmation of Multistakeholder Model for Internet Governance by World Leaders*, Press Release on ICANN Website, 23 June 2014. Available at: <https://www.icann.org/news/announcement-2014-06-23-en> [accessed April 3, 2017].
- Conklin, J. (2006). *Wicked Problems & Social Complexity*. Hoboken, NJ: CogNexus Institute.
- Crewe, E., and Axelby, R. (2013). *Anthropology and Development: Culture, Morality and Politics in a Globalised World*. Cambridge: Cambridge University Press.
- Egeberg, M., Olsen, J. P., and Sætren, H. (1978). *Organisasjonssamfunnet og den segmenterte stat*. Bergen: Maktutredningen.
- Elo, S., and Kyngäs, H. (2008). The qualitative content analysis process. *J. Adv. Nurs.* 62, 107–115. doi: 10.1111/j.1365-2648.2007.04569.x
- Engberg-Pedersen, L. (1997). Institutional contradictions in rural development. *Eur. J. Dev. Res.* 9, 183–208.
- Everitt, A. (1996). Developing critical evaluation. *Evaluation* 2, 173–188. doi: 10.1177/135638909600200204
- Fayol, H. (1916/1949). *General and Industrial Management*. London: Pitman.
- Gjørsv, A. B. (2012). *Rapport Fra 22. juli-kommisjonen. Norges Oentlige Utredningar, 14*. Available at: <https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbe8/no/pdfs/nou201220120014000dddpdfs.pdf> [accessed March 23, 2017].
- Goodhand, J. (2006). "Working in, on or around conflict," in *Civil War, Civil Peace, Milton Keynes*, eds H. Yanacopulos and J. Hanlon (Milton Keynes: The Open University), 260–268.
- Hagen, J. (2016). Cyber security - the Norwegian way. *Int. J. Crit. Infrastruct. Prot.* 14, 41–42.
- Hanlon, J. (2014). "Grabbing attention," in *Research Skills for Policy and Development. How to Find out Fast*, eds A. Thomas and G. Mohan (London: Sage), 74–94.
- Harriss, J. (2000). "Working together: the principles and practice of cooperation and partnership," in *Managing Development: Understanding Inter- Organizational Relationships*, eds D. Robinson, T. Hewitt, and J. Harriss (London: Sage Publications), 225–242.
- Hartley, J., Butler, J., and Benington, J. (2002). Local government modernization: UK and comparative analysis from an organizational perspective. *Public Manag. Rev.* 4, 387–404. doi: 10.1080/14616670210151612
- Helkala, K., and Svendsen, N. K. (2014). *Analysis of Norway's Cyber and Information Security Strategy*. Bodø: Norsk informasjonssikkerhetskonferanse.
- Homan, R., and Hancock, P. (2017). Measuring resilience. *Hum. Factors* 59, 564–581. doi: 10.1177/0018720816686248
- Huxham, C. (1993). Collaborative capability: an intra-organizational perspective on collaborative advantage. *Public Money Manag.* 13, 21–28. doi: 10.1186/2001-1326-3-9

- Jasper, S. (2012). *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*. Washington, DC: Georgetown University Press.
- Kellner, D. (2002). New technologies / new literacies: restructuring education for a new millennium. *Teach. Educ.* 11, 245–265. doi: 10.1080/713698975
- Kickert, J. M., Klijn, E., and Koppenjan, J. (1997). *Managing Complex Networks: Strategies for the Public Sector*. London: Sage Publications.
- Knox, B. J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Lugo, R., Ødegaard, T., et al. (2018). Socio-technical communication: the hybrid space and the OLB-model for science-based cyber education. *Mil. Psychol.*
- 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 International Conference on Human-Computer Interaction*, (Berlin: Springer), 330–338. doi: 10.1007/978-3-319-58750-9_46
- Kuehl, D., Kramer, F. D., Starr, S. H., and Wentz, L. K. (2009). *Cyberpower and National Security*. Dulles, VA: Potomac Books, Inc.
- Leftwich, A. (1996). “On the primacy of politics in development,” in *Democracy and Development*, ed. A. Leftwich (Cambridge: Polity Press), 3–24.
- Leftwich, A., and Sen, K. (2011). “Don’t mourn; organize” institutions and organizations in the politics and economics of growth and poverty-reduction. *J. Int. Dev.* 23, 319–337. doi: 10.1002/jid.1773
- Long, N. (2001). *Developing Sociology. Actor Perspectives*. London: Routledge. doi: 10.4324/9780203398531
- Mayoux, L., and Johnson, H. (2014). “Investigation as empowerment: using participatory methods,” in *Research Skills for Policy and Development. How to Find out Fast*, eds A. Thomas and G. Mohan (London: Sage), 180–207.
- McDonnell, E. (2016). T879-16E, Conflict and Development, Week 16, Working with Conflict and Complexity. Milton Keynes: The Open University.
- Mukherjee, C., and Wuyts, M. (2014). “Thinking with quantitative data,” in *Research Skills for Policy and Development. How to Find Out Fast*, eds A. Thomas and G. Mohan (London: Sage), 231–253.
- Muller, L. P. (2016). Makt og avmakt i cyberspace: hvordan styre det digitale rom? *Int. Politikk* 74, 1–23. doi: 10.17585/ip.v74.428
- Nje, R. (2017). *Kripes Advarerer:-Stor Økning I Datakriminalitet, NRK*. Available at: https://www.nrk.no/norge/kripes-advarerer_-_stor-okning-i-datakriminalitet-1.13436174 [accessed April 3, 2017].
- North, D. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511808678
- Norwegian Centre for Information Security [NorSIS] (2016). *The Norwegian Cyber Security Culture*. Available at: <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf> [accessed March 25, 2017].
- Nye, J. (2011). Power and national security in cyberspace. *Am. Cyber Future* 2, 5–23.
- OED. (2017). *Oxford English Dictionary, The Definitive Record of the English Language*. Available at: <http://www.oed.com/> [accessed April 3, 2017].
- Organisation for Economic Co-operation and Development [OECD] (2005). *Governance of Innovation Systems: Case Studies in Innovation Policy*, Vol. 2. Paris: Organisation for Economic Co-operation and Development.
- Ostrom, E. (1996). Crossing the great divide: coproduction, synergy and development. *World Dev.* 24, 1073–1087. doi: 10.1016/0305-750X(96)00023-X

- Ouchi, W. (1980). Markets, bureaucracies and clans. *Adm. Sci. Q.* 25, 129–141. doi: 10.2307/2392231
- Paton, R. (1991). *Managing with a Purpose. (Book 1 of Open University Course B789 Managing Voluntary and Non-Profit Enterprise.)*. Milton Keynes: The Open University.
- Peña-López, I. (2016). *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank.
- Pinder, R. (2016). *Capacities for Managing Development, T878, Part 1, Week 1*. Milton Keynes: The Open University.
- Reuters. (2017). *BRIEF-Norway Banks Allowed to Merge Electronic Payment Solutions'-Regulator*. Available at: <http://www.reuters.com/article/brief-norway-banks-allowed-to-merge-elec-idUSO9N1G102B> [accessed April 2, 2017].
- Robinson, D., Hewitt, T., and Harriss, J. (eds) (2000). *Managing Development: Understanding Inter-Organizational Relationships*. Thousand Oaks, CA: Sage.
- Roche, C. (2014). "Organizational assessment and institutional footprints," in *Research Skills for Policy and Development. How to Find out Fast*, eds A. Thomas and G. Mohan (London: Sage), 275–300.
- Rosenau, J. N. (1995). Governance in the twenty-first century. *Glob. Gov.* 1, 13–43.
- Rowlands, J. (1997). *Questioning Empowerment: Working with Women in Honduras*. Oxford: Oxfam. doi: 10.3362/9780855988364
- Salancik, G. R., and Pfefer, J. (1978). A social information processing approach to job attitudes and task design. *Admin. Sci. Q.* 23, 224–253. doi: 10.2307/2392563
- Standt, K. (1991). *Managing Development: State, Society and International Contexts*. London: Sage. doi: 10.4135/9781483325798
- Stevens, T. (2015). *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9781316271636
- Stortingmelding. (2016–2017). *Meld. St. 10, Risiko i et Trygt Samfunn, Samfunnsikkerhet*. Available at: <https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf> [accessed December 15, 2016].
- Tapscott, D. (2014). *The Digital Economy ANNIVERSARY EDITION: Rethinking Promise and Peril in the Age of Networked Intelligence*. New York, NY: McGraw Hill Professional.
- The Guardian (2017). *Norway Accuses Group Linked to Russia of Carrying out Cyber-Attack*. Available at: <https://www.theguardian.com/technology/2017/feb/03/norway-accuses-group-linked-to-russia-of-carrying-out-cyber-attack> [accessed April 6, 2017].
- The Open University (2000). *Managing Development, Understanding Inter- Organisational Relationships, TU872*. Milton Keynes: The Open University.
- The Open University (2007). *Capacities for Managing Development, TU870, Part 3, Learning in Development Management, Evaluation, Advocacy and Strategy*. Milton Keynes: The Open University.
- Thomas, A. (1996). What is development management? *J. Int. Dev.* 8, 95–100. doi: 10.1002/(SICI)1099-1328(199601)8:1<95::AID-JID348>3.0.CO;2-
- Thomas, A. (2000). Development as practice in a liberal capitalist world. *J. Int. Dev.* 12, 773–787. doi: 10.1002/1099-1328(200008)12:6<773::AID-JID716>3.0.CO;2- 7
- Thomas, A., Carr, S., and Humphreys, D. (eds) (2001). *Environmental Policies and NGO Influence: Land Degradation and Sustainable Resource Management in Sub-Saharan Africa*. New York, NY: Routledge.

Thomas, A., and Chataway, J. (2014). "Conclusion: personal effectiveness and integrity," in *Research Skills for Policy and Development. How to Find out Fast*, eds A. Thomas and G. Mohan (London: Sage), 325–335.

Turkle, S. (2011). *Alone Together*. New York, NY: Basic Books.

UNWOMEN (2015). *Cyber Violence Against Women and Girls, A World- Wide Wake-Up Call*. Available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259 [accessed March 28, 2017].

van Haaster, J. (2016). "Assessing cyber power," in *Proceedings of the 8th International Conference on Cyber Conflict, CYCON*, Vol. 2016, eds N. Pissanidis, H. Rõigas, and M. Veenendaal (Tallinn: NATO CCD COE Publications), 7–21. doi: 10.1109/CYCON.2016.7529423

Vatu, G. (2017). *NATO Warns Cyber Attacks Are a Threat to Democracy Itself, Cyber Security Review*. Available at: <http://www.cybersecurity-review.com/nato-warns-cyber-attacks-are-a-threat-to-democracy-itself/> [accessed April 1, 2017].

von Solms, R., and van Niekerk, J. (2013). From information security to cyber security. *Comput. Secur.* 38, 97–102. doi: 10.1016/j.cose.2013.04.004

Wood, G. (2003). Staying secure, staying poor: the "Faustian Bargain". *World Dev.* 31, 455–471. doi: 10.1016/S0305-750X(02)00213-9

Woodhouse, P. (2014). "People as informants," in *Research Skills for Policy and Development. How to Find out Fast*, eds A. Thomas and G. Mohan (London: Sage), 159–179.

World Bank (2017). *Trading Economics*. Available at: <http://www.tradingeconomics.com/norway/gdp> [accessed March 26, 2017].

Wrangham, R. (2016). *Capacities for Managing Development, Course T878, Part 1, Week 1. Setting out*. Milton Keynes: The Open University.

Wuyts, M. (1992). "Deprivation and public need," in *Development Policy and Public Action*, eds M. Wuyts, M. Mackintosh, and T. Hewitt (Oxford: Oxford University Press).

Conflict of Interest Statement: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

The reviewer BH and handling Editor declared their shared affiliation.

Copyright © 2018 Knox. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Appendix 1 to Paper 1

1 What is understood by the term cyberpower?

Can you describe your **own personal perception** of CP?

CP is now a political instrument: Could you now describe it from a **political perspective**?

If the above differ, ask: Why might there be a **difference** in perspectives?

How do you think these differences in perspectives can be **reconciled**?

Show him/her the Kuehl (2016) definition of CP and ask if he/she agrees?

What are key '**aspects**' of HOW CP works? (I hope this will be picked up in 1.1)

2 In what ways do perceptions of cyberpower vary between stakeholder respondents?

Inform him/her whom else I am talking to, in order for him/her to give an opinion about how he/she thinks others perceive CP?

Why might different organizations **perceive CP differently**?

What makes the **effects of CP so effective**?

3 In what ways are the tensions (challenges) between vulnerability to and dependency upon cyberpower manifested in operational terms?

CONTEXT: Stortingsmelding 10 stated that increasing digitalization is not a choice; it is a condition of a modern society:

How is CP **influencing organizational relationships**?

Do you see any **new approaches** to how organizations conduct themselves - now they have the opportunity to collaborate more?

We have seen a culture of 'restricting' information (possibly due to the 'vulnerability' aspect). Do you think organizations/sectors are being less **transparent** or do you think they are adopting a more 'open' approach?

How does the culture in organizations of '**conflicting generations**' create tensions?

How does this translate to **levels of tolerance**? AND **levels of understanding**?

Is '**uncertainty**' **driving action or inaction**? Is this influenced by ignorance?

4 **What kinds of processes and structures could support managing the tension between vulnerability to, and dependency upon cyberpower?**

How do you see Norway achieving a holistic approach to coping with CP effects? OR is a solid State structure enough?

What decisions are having to be made and actions taken to manage the vulnerability vs. dependency paradox identified in Stortingsmelding 10?

How is **policy development** occurring (as process or as prescription)?

What **adaptations** are occurring in political terms to cope with the speed of change? Is it more TRUST or more CONTROL?

Can you imagine a bottom-up approach to managing the effects of CP, i.e., the **Norwegian people have a say** on V vs. D?

Given that the effects of CP are shaping how modern society is developing, and we are as dependent as we are vulnerable, do you see CP as a version of a **new 'hegemonic' authority**?

In what ways are the effects of CP **an ethical issue** for organizations?

5 What kinds of institutional and capacity constraints work against effective collaboration/co-ordination between organizations in the management of those tensions?

Do you see a tension in **leadership styles**? (Historical hierarchy vs. unrestricted/less controlled sharing at the lower levels of management)

What issues do you see regarding **speed** of turnaround on effect analysis: e.g., what does that Tweet mean for us...?

What **informal** collaborations happen that develop outside of **formal** networks (any 'old' types of behavior occurring that seem to be counterintuitive to the collaborative nature of digitalization).

Where do you see **power** lies? Inside or outside government? CP creates an environment of **uncertainty**. Sectors are **empowered**, organizations are digitized and driving ahead but there is a 'ghost in the room' influencing **decision making**.

Is there the **capacity to collaborate** (within your organization and between organizations in general)? If so, where in the system does that willingness manifest?

Digitization for collaboration - does it occur, as we would expect?

PAPER II



Full Terms & Conditions of access and use can be found at
<http://www.tandfonline.com/action/journalInformation?journalCode=hmlp20>



MILITARY PSYCHOLOGY
2018, VOL. 30, NO. 4, 350–359 <https://doi.org/10.1080/08995605.2018.1478546>

Socio-technical communication: The hybrid space and the OLB model for science-based cyber education

Benjamin J. Knox^a, Øyvind Jøsok^{a,d}, Kirsi Helkala^a, Peter Khooshabeh^c, Terje Ødegaard^b, Ricardo G. Lugo^b, and Stefan Sütterlin^{e,f}

^aNorwegian Defence Cyber Academy, Defence University College, Lillehammer, Norway; ^bDepartment of Psychology, Inland University of Applied Science, Lillehammer, Norway; ^cUS Army Research Laboratory, Human Research and Engineering Directorate, Los Angeles, California; ^dChild and Youth Participation and Development Research Program, Inland University of Applied Science, Lillehammer, Norway; ^eCHTD Research Group, Oslo University Hospital, Oslo, Norway; ^fFaculty for Health and Welfare Sciences, Østfold University College, Fredrikstad, Norway

ABSTRACT

Lessons from safety-critical sociotechnical systems, such as aviation and acute medical care, demonstrate the importance of the human factor and highlight the crucial role of efficient communication between human agents. Although a large proportion of fatal incidents in aviation have been linked to failures in communication, cognitive engineering provides the theoretical framework to mitigate risks and increase performance in sociotechnical systems not only in the civil sector, but also in the military domain. Conducting cyber operations in multidomain battles presents new challenges for military training and education as the increased importance of psychological factors such as metacognitive skills and perspective-taking both in lower and higher ranking staff, becomes more apparent. The Hybrid Space framework (Jøsok et al., 2016) provides a blueprint for describing the cognitive and behavioral constraints for maneuvering between socio-technical and cyber-physical systems whilst cooperating, coordinating or competing with accompanying cognitive styles in the chain of command. We apply the Hybrid Space framework to communicative challenges in the military cyber domain and suggest a three-phase Orienting, Locating, Bridging model for safe and efficient communication between partners. Based on the educational principles of the Norwegian Defence Cyber Academy, we discuss the required skill-sets and knowledge in which cyber officer cadets are trained and taught early in their education, and how these refer to the theoretical framework of the Hybrid Space and the key principles of communication as defined in cognitive engineering.

KEYWORDS

Cognitive engineering; hybrid space; sociotechnical system; cyber domain; grounded communication; mental models; multi-domain battle; cyber education

What is the public significance of this article? The orientating, locating and bridging (OLB) model is a science-based contribution that aims to prevent communication failures arising from individual differences driven by factors such as hierarchy, bias or effort. A pedagogic approach to OLB in cyber education can potentially reduce the cognitive load and ease communication challenges in complex and critical cyberspace operations. This knowledge can easily be applied to civilian applications of cyberspace, such as protection of critical infrastructure, personal privacy protection and informing educators in how to enhance performance and decision-making in the cyber domain.

In this article, we show how we took a cognitive engineering process and applied it to communication activities conducted by military personnel operating in the cyber domain for improved performance.

Communication in sociotechnical systems¹ and its effect on decision-making are a crucial part of modern society influencing safety, efficiency, and performance. Extensive research, particularly in critical civil environments such as medical acute care and aviation, has improved our understanding of the constraints, risk, and possibilities associated with poor communication (e.g., Entin, 2004; Jacobsson, Hargestam, Hultin, & Brulin, 2012; Mills, Neily, & Dunn, 2008). Unsurprisingly, research interest on the effect of communication in the resource-intensive and safety-critical military context is growing rapidly (e.g., Brun et al., 2003; Cannon-Bowers & Salas, 1998; Espevik, Johnsen, & Eid, 2011; Rosen et al., 2008; Letsky, Warner, Fiore, & Smith, 2008; Trejo, Richard, Van Driel, & McDonald, 2015). Consequences arising from misunderstandings and ineffective communication range from undetected suboptimal performance to potentially fatal incidents with both local and international consequences (see Rosen, Fiore, Salas, Letsky, & Warner, 2008). The cyber domain, which consists of interconnected and networked systems and actors represents a new and important domain for studying communication. Personnel operating in the cyber domain represent a group of actors facing work that is characterized by a unique pattern of human–technological interaction bearing cognitive challenges that span the digital, physical, and the social domain (Jøsok et al., 2016; Von Solms & Van Niekerk, 2013; Whitman & Mattord, 2012). Within the military cyber context, success in the cyber domain requires a new and unique skillset compared to more traditional domains.

The digital context and informational environment has increased mental workloads, shifting demands from physical fitness toward cognitive performance that is novel to military domains. This underlines the importance of versatile preparation of personnel, concepts that go beyond classical military abilities or technological skills, and towards more comprehensive qualifications.

The increased awareness of the multiple social (e.g., cooperation and communication skills) and cognitive demands on cyber officers have been widely acknowledged but are not yet reflected in corresponding empirical research or commonly agreed standards of science-based education and training. The British Ministry of Defence recognized the need for skill development beyond technological domains when it stated that, “The operational commander in 2035 will need to be as focused on cyber as on traditional environmental factors” (Ministry of Defence, 2015). Whereas the US Military Academy at West Point addressed instructor competencies and responsibilities by stating that they have “updated their curriculum and pedagogy so that it now accounts for a cadet’s level of self-development” (Putz & Raynor in Reams, 2005). It is also becoming apparent that educational methods need to correspond to future communication demands placed upon personnel working in all military domains—including those conducting cyber operations.² To achieve a change in praxis, officer cadet educational programs should include development of cognitive characteristics such as, “agility, adaptability, and creative and critical thinking” (Tikk-Ringas, Kerttunen, & Spirito, 2014, p. 58). Military cadets who assume more traditional military training practices with clearly defined concepts, templates, and order-based execution may well struggle to fully cope in such an operating environment (Freedberg, 2016; Tikk-Ringas et al.,

2014). Future operating environments will require soldiers to communicate effectively with multiple agents and entities in the cyber domain.

To meet some of the challenges that the cyber domain poses, as mentioned above, this article suggests a model for teaching prerequisites for improved communication in the cyber domain. The learning model will support practitioners operating in safety-critical environments by reducing the risk of negative consequences resulting from miscommunication. By implementing measures of cognitive engineering designed to improve communication efficiency in sociotechnical systems, the aim is to mitigate miscommunications that may go undetected or underestimated.

We begin this article by reviewing the current research and practice, detailing the theoretical frame-works established in cognitive engineering research, as well as introducing the Hybrid Space conceptual frame- work. Then, we propose a three-phase Orienting, Locating, Bridging (OLB) model for teaching and training to improve outcomes via efficient communication. The Norwegian Defense Cyber Academy (NDCA) is used to exemplify the OLB model's application in a military educational context. Further, we discuss additional applications of the OLB before the article concludes and presents ongoing and future work.

Current research and practice

A novel area of research arising from the formal recognition of cyberspace as a military domain of operations (NATO Cooperative Cyber Defence Centre of Excellence, 2016) is how cognitive engineering can improve communicative challenges in sociotechnical systems. The cyber domain creates a special challenge for efficient communication among military command structures as the digital and the physical domains converge (Tikk-Ringas et al., 2014; Trujillo, 2014). Higher-ranking officers hold the final responsibility for the decisions made. Their routines, command and control activities, and eventual decision-making are most likely rooted in and influenced by their previous experience. However, their situational awareness and decision-making are heavily influenced, if not determined, by the perception, interpretation, and evaluation of a given critical situation by a lower ranking, and often younger officer who comfortably maneuvers in the cyber domain (Røislien, 2015). To promote effective communication, particularly in the cyber domain, there is a mutual need for perspective-taking skills to understand others' need for information, their mental workload, and a metacognitive awareness concerning one's own momentary cognitive states and susceptibilities. Common ground theory provides the theoretical framework for understanding the elements of successful social interaction. It is based on cognitive engineering and provides a framework to systematically approach and consequently mitigate risk factors and enhance efficiency and performance in goal-directed communication (Clark, 1996; Monk, 2009; Morrow & Fischer, 2013). Common ground theory stresses the necessity of a mutual understanding, with which both sender and receiver consider the exchanged information as accurate, understood, and related to the shared goal (Searle, 1969). As a result of grounded communication, both partners are able to co-construct a shared mental model that can support "shared consciousness" and "empowered execution" (McChrystal, Collins, Fussell, & Silverman, 2015).

The aspects described above capture the challenge of developing shared mental models in the military domain, where hierarchy and rank structures can impact perspective taking. In particular the emerging nature of the cyber domain adds layers of complexity that further exasperate the challenge of achieving common ground. Approaches capable of finding common ground in the cyber domain need to be considered in the context of networked intelligence (McChrystal et al., 2015; Tapscott, 2014) and multi-domain battles (Tan, 2016) as these approaches are heavily dependent upon shared situational awareness for sense-making. For example, multidomain challenges influence communication in military domains by merging the need to empower lower

ranks through models of command and control that are context-oriented, rather than reverting them to the norm of restrictive hierarchical communication systems. Communication can be more effective if the actors (i.e., the individuals communicating with one another) can more closely align their mental models in dynamic hybrid operating environments. This will rely upon methods of education and training that aspire to higher levels of consciousness (Joiner & Josephs, 2006; Kegan & Lahey, 2009) in both junior and senior military personnel, as they are expected to undertake mutually beneficial actions of self-orienting and locating each other, to bridge grounded communication.

Because of these new demands, higher-ranking commanders will be required to accept new communication concepts and training for agile maneuvering in the cyber domain. Commanders need to be able to strategically empower lower-ranking soldiers, reduce strict divisions between tactical and strategic personnel, and act to facilitate effective communication that allows for goal-directed and accurate use of information as well as an increased level of openness among involved personnel. The OLB model presented in this article dissects the steps required for successful communication in the Hybrid Space (Jøsok et al., 2016) and provides guidance for both lower and higher ranks to promote grounded communication.

The Hybrid Space framework

A recent theoretical proposal addressed many of the challenges described above by introducing the Hybrid Space conceptual framework (Jøsok et al., 2016) (see Figure 1). The framework represents an individual's range of cognition when involved in tasks that span strategic vs. tactical, or physical (kinetic) vs. cyber operations. Along the spectrum of these dimensions, different cognitive skills are necessary/used, for example, heuristics, social-cognitive perspective-taking, spatial cognition for kinetic, self-regulation for planning, evaluating, and monitoring one's own processes and macrocognition for team performance. The framework acknowledges the new structures and demands by articulating the needs for cognitive flexibility and perspective-taking on an inter- and intra-individual level, which allows for the application of psychological concepts in assessment, in training and action of military cyber personnel. The Hybrid Space not only describes how the individual cognitively maneuvers between dynamic tactical/strategic and cyber-physical/sociotechnical demands, but it also implies the need for objective orientation related to one's own and other communication partner's momentary mental 'location' within these domains. It also reveals the requirements for effective communication bridging to ensure optimal performance levels. This perspective taking is required to co-construct a shared mental model with communication partners.

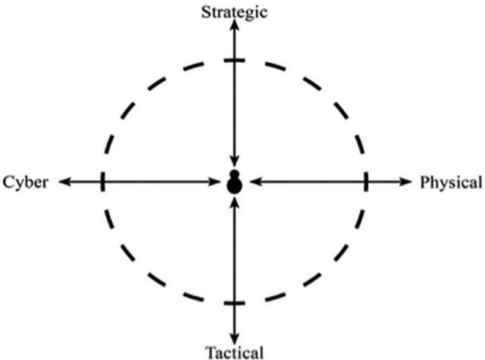


Figure 1. The hybrid Space. Reprinted from exploring the hybrid space - theoretical framework applying cognitive science in military cyberspace operations (pp. 181). Ø. Jøsok, B.J. Knox, K. Helkala, R.G. Lugo, S. Sütterlin, & P. Ward. 2016, Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience LNCS Volume 9744.

In the military context of the cyber domain, the construction of shared mental models leads to mutual understanding and efficient processing of time-critical information, provides the basis for tactical decisions with potentially large strategic implications, and thus requires the reduction of risk factors that lead to mis-communication. Using the two-dimensional structure of the Hybrid Space rather than adapting or copying existing models allows for more straightforward presentation of the unique characteristics of the human factor in military cyber operations typical in today's multi-domain battles.

The OLB model: How to educate for grounding of communication in the cyber domain

When co-constructing a shared mental model, communication partners should apply techniques to enhance situational awareness, information-processing resources such as working memory, cognitive flexibility, metacognitive awareness, and perspective-taking (Morrow & Fischer, 2013). The Hybrid Space framework (Figure 1) allows for the introduction of applied cognitive science into cyber domain education. The OLB model is based on this framework and dissects maneuvering within the Hybrid Space into three core phases (see Figure 2). The educational implications are illustrated in Figure 3.

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.

Orienting

A prerequisite for an accurate placement of one's own cognitive location within the Hybrid Space (orienting) is the metacognitive awareness of factors influencing one's momentary mental state and ongoing cognitive processes. In Hybrid Space terms, this refers to the ability to monitor and regulate thinking along the cyber-physical and strategic-tactical dimensions (horizontal and vertical axis, Figure 2a). An example of orienting could be a junior cyber operator preparing to brief or communicate the recognized cyber picture (RCP) to a senior but nontechnical person. If a network intrusion has occurred, a RCP brief should accurately present the severity and potential known or unknown consequences. Good metacognitive awareness allows the operator to visualize the most appropriate mode, method, and content of communication to ensure he/ she relays an accurate message that is not only received correctly but also understood. Similarly, a nontechnical commander will need to regulate and monitor his/her own thinking, behavior and be open to extending his/ her cognition and modes of communication. This will allow for better understanding and appreciation of critical and quite possibly incomplete information being presented by a junior expert. As the examples above show, failure to orientate prior to receiving an RCP brief could result in a critical communication error occurring. Attempting to orientate to gain mutual understanding or a shared mental model is challenged further when the RCP brief takes place across multiple and heterogeneous communication partners in the Hybrid Space—some face-to-face and others via digital means. This is because the communicator has to be keenly aware of more than one location in the Hybrid Space and be cognizant of the implications for communicating within these different spaces.

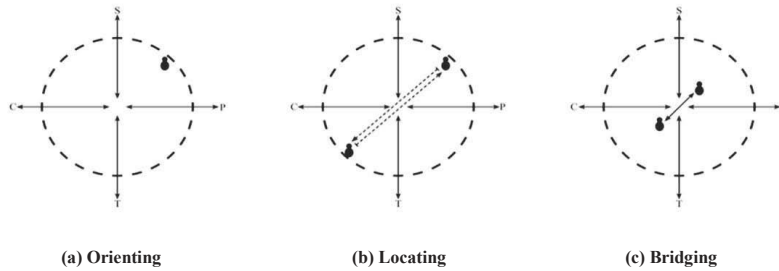


Figure 2. OLB model as a procedure to communicate across the Hybrid Space. (S-strategic, T-tactical, P-physical, C-cyber). (a) Orienting. (b) Locating. (c) Bridging.

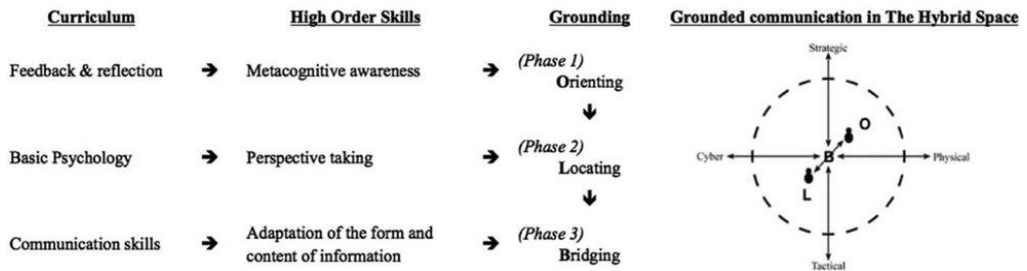


Figure 3. Pedagogic path for OLB – a practice to reduce the cognitive cost of communication in the hybrid space.

Locating

Once an individual has gained metacognitive awareness of his/her location within the Hybrid Space, locating the communication partner constitutes Phase 2 in the OLB model (Figure 2b). Locating specifically involves accurately judging a communication partner’s cognitive location in the Hybrid Space. It also involves identifying factors that can impact a partner’s interpretation of incoming information. For instance, understanding a partner’s knowledge, skills, and emotional state and current cognitive load, as well as cultural background and contextual circumstances (time pressure, external expectation, conflicting task priorities), can help an individual tailor a message to meet their partner’s immediate needs and ensure proper understanding.

The act of perspective taking is an important process in the locating phase of the OLB model. Factors such as a partner’s expertise, experience with a particular topic, and professional conventions may impact how he or she thinks, talks, and interprets information and can thus be used to establish communal command ground (Monk, 2009). For example, rethinking hierarchical systems to empower lower ranking personnel (Tan, 2016) and thus increase their contextual knowledge could positively affect the lower ranking person’s capacity to contribute to effective grounding. Understanding what communities a person belongs to may allow agents to make certain assumptions about existing common ground. They can then use this knowledge to make communication across the hybrid space more effective. In a borderless domain, mediated by electronic communication, this perspective taking might be more relevant than in face-to-face situations where cultural misunderstandings are more easily detected by the use of multiple communication modalities.

Personal common ground gained prior to or during a communication improves the location process further. The personal state of mind such as the level of acute or chronic stress and momentary attentional focus directly influence the quality of grounding and can change at an instant. Individuals who feel observed, monitored, and socially challenged in a conversation within a hierarchical system are more likely to engage in self-monitoring behavior at the cost of their cognitive task performance and ongoing problem-solving or communicative demands. For example, communication failure can occur in a hierarchical system where defensive reasoning flourishes (Argyris, 1991).

Without perspective taking and acknowledging communication partner's needs, a junior expert attempting to present the RCP to a nontechnical commander could negatively affect communication flow by incorrect locating and message framing. In this context, interaction may also suffer at the cost of performance outcomes on an individual and team level if the commander is unwilling to locate—through acknowledging the junior experts' needs and requirements—and engage in learning and knowledge creation, to gain critical understanding. The complexity of locating escalates when a RCP has to be delivered via digital communication means to multiple heterogeneous recipients across the Hybrid Space.

Bridging

The final phase, bridging, describes the adaptation of content and style of grounded communication to co-construct a shared situational model (Figure 2c). When the process of orienting (requiring metacognition) and locating (requiring perspective-taking) has given insight in the relative location of the communication partners, bridging the remaining gap requires an adaptation of the form and content of information provided. This includes a common understanding of the appropriate level of detail, the conventional norms and forms of presentation, knowledge about the degree of tolerated uncertainty, the situationally appropriate level of confidence into one's own judgment or self-criticism, and the openness to admit the need for additional information or simplification. By adapting communicated content and its style in a way that maximizes the overlap of shared cognitive representations, the cognitive distance between two partners within the Hybrid Space is reduced and the risk of misunderstandings and misinterpretations limited. Successful bridging acknowledges the partners' cognitive position along the tactical-strategic and the cyber-physical domain. Preparing the appropriate amount and type of information in a way that acknowledges a partners' cognitive position is key to successful communication in critical situations. For example, bridging for successful communication of a RCP has to be adaptive and able to engage in immediate self-correcting actions in face-to-face communication. In a multidomain context, bridging for good communication of a RCP may require opening multiple lines of communication for adjusted framing of communication. Communicating with more heterogeneous multiple recipients is challenging, as information demands and understandings vary. For this reason, the OLB points out the need for training and development of communication skills to enhance communicating messages simultaneously in face-to-face dyadic mode and in a socio-technical context.

The NDCA approach

The three phases of the OLB model constitute elements fostering grounded communication in a military cyber domain setting. The NDCA emphasizes in their training of cyber officer cadets applied cognitive science and various sub-areas of psychology as a central element of their education program. To facilitate metacognitive awareness for orienting, the NDCA covers topics such as personality psychology, psycho-physiological interaction to sensory perception, effects of acute and chronic stress on cognitive performance, group effects on decision-making, and macrocognition. These are combined with practical experience involving regular peer-group and mentor feedback provided in written and oral form. According to the OLB model, forming a

realistic perspective of oneself in a complex sociotechnical system is a crucial pre-requisite for successfully locating oneself within the Hybrid Space and fostering safe and efficient communication. The NDCA applies the OLB model and aims to enhance individual skills to orientate within the Hybrid Space by the use of reflection logs and frequent feedback. Using reflection and reflective dialogues as a tool to build an evidence base for new perspectives, where a cadet moves from being a detached observer to an involved learner (Brigden & Purcell, 2004), supports the orientation function by enhancing metacognitive awareness. Becoming more aware of yourself through metacognitive training a hybrid-operating environment can provide the necessary scaffolding for success in Phase 2: locating.

Achieving a high level of mutual perspective taking and awareness for communication partners' situational demands in dynamic contexts are central elements of teaching and training at the NDCA. This content is meant to train cadets on the locating phase of the OLB model. A curriculum including subject areas such as intercultural knowledge and international operations acknowledges this need in cyber cadet cohorts. At the NDCA, cadets get exposed to a curriculum equipping them with the knowledge and cultural understanding to mediate their communication efforts in the borderless cyber domain.

In their final year at the NDCA, cadets practice bridging skills by planning activities in complex and varying context, ranging from classroom environments to demanding military exercises. The cadets are expected to lead people—their own cohort and junior cadets—and processes. Teachers and instructors act as facilitators as well as a heterogeneous group of actors within the sociotechnical system. The intent is to encourage cadets to train their skills in adapting the form and content of information being communicated in order to ensure effective bridging. [Figure 3](#) shows how the NDCA applies the model in teaching curriculum.

Furthering understanding and applications of OLB

Other constraints for successful (i.e., efficient and safe) communication—of particular relevance in a military structure—are culture, social norms, conventions, and formal constraints caused by the authority gradient based on formal ranking. These constraints based on an asymmetry of power and agency are commonly associated with the use of indirect speech of a lower ranking person toward someone of higher status, and the tendency to avoid expressions or formulations that could be perceived as critical, disagreeing, impolite, or not sufficiently appreciative (Blum-Kulka, House, & Kasper, 1989; Grice, 1975; Jason, Keys, Suarez-Balcazar, Taylor, & Davis, 2004; Xiao, Seagull, Mackenzie, Ziegert, & Klein, 2003). Conversely, these constraints occur when higher ranking officers incorrectly (consciously or unconsciously) make assumptions about junior officers' level of competence in a particular domain where the junior officer has expertise. This could lead to communication failures (i.e., indirect communication, partial communication or even body language) and result in misinterpretation at the receiving end, having a negative effect for developing shared mental models (DeChurch & Mesmer-Magnus, 2010). Developing (or the emergence of) a shared situational awareness or shared mental model around partially overlapping expertise (probable consequences of action) and responsibilities (tactical and strategic considerations) will be difficult because of the clear role distinctions based on seniority and rank. In this case, higher ranking officers are potentially unaware of factors influencing a young cyber officer's judgment, performance, and goals (Sexton, Thomas, & Helmreich, 2001) thus leading to poor situational awareness and lack of shared mental models. Misinterpretations of critical situations in aviation based on this type of communication failure between pilot and first officer have been termed "monitoring/ challenging error" by the National Transportation Safety Board (NTSB, 1994 in Fischer & Orasanu, 2000). This error was found to occur in over 75% of the air traffic accidents reviewed (Morrow & Fischer, 2013). This type of error has also been acknowledged in acute medical care, where the communication within a surgical team is similarly

challenged by differences in social status between nurses and doctors, and a lack of understanding of the external factors influencing the partners' cognitive abilities (Korb, Geißler, & Strauß, 2015).

Explicit procedures such as reading back information to ensure mutual understanding are supposed to facilitate grounding in both aviation and medical care. To avoid misunderstandings caused by the authority gradient and related conventions, research in aviation found positive effects where communication skills allowed for a good balance of informativeness and social appropriateness (Fischer & Orasanu, 2000), and where crew members stated explicitly how the perceived information was interpreted and how they are about to react on it. Although the speaker (e.g., the cyber officer) has to make sure that the intention of his presented information is mutually understood, it is the receiving person's responsibility to signalize his or her level of understanding. A communication style based on mutual reassurance, openness to correction, re-evaluation, negotiation, and adjustment is also needed in the military to minimize barriers to collaboration and communication bottlenecks and to facilitate effective grounding (McChrystal et al., 2015).

OLB for grounded communication

Grounded communication in the context of cyber operations faces particular challenges that result directly from the location of the individual's cognitive focus across the axes of the Hybrid Space (Figure 1), and the cognitive costs of constant movement along them, leading to depletion of attentional resources (Jøsok et al., 2016). An example of the cognitive implications and changes in decision-making processes when being continuously exposed to the cyber domain, arises from the physical, and consequently, emotional distance to this environment that is directly affected via digital means. The decision maker, empowered by the cyber domain, is less directly confronted with the out-comes of the decision. The anticipation of future action's outcomes is more abstract, less detailed, and typically decision-making processes are under time pressure. These circumstances in the decision-making processes in the cyber domain, together with other assumed, but not yet investigated aspects, such as an increased tolerance to uncertainty, increases the cognitive load on decision stakeholders. To ensure grounded communication, the cyber officer has to be aware of the strategic considerations affecting the situational assessment, awareness, and decision-making process of higher ranking officers to whom he or she reporting (e.g., Krulak, 1999; Lemay, Leblanc, & Jesus, 2015; Liddy, 2004; Stringer, 2009). At the same time, his/her own decisions in the cyber domain relating to cyber operations may affect the strategic goals of the mission. The possibility of strategic impact, the implications and the resulting options concerning how to react to these impacts, needs to be communicated accordingly.

OLB for better regulatory behavior

Monitoring and adjusting one's own cognitive location within the Hybrid Space increases cognitive demands considerably. In a time-critical situation, a relatively young/junior cyber operator with appropriate domain understanding and enough knowledge to allow for strategic consideration may lack the skill-set for grounded communication. In this instance, not being "heard" by a higher-ranking commander prone to biased judgments can affect the strategic goal due to his/her distant relative location on the Hybrid Space's axes (Jøsok et al., 2016). In this example, communication failure results from insufficient grounding. The former lacked training in OLB processes—not necessarily mental capacity—whilst the latter lacked cognitive regulatory resources and reverted to the hierarchy norm to avoid further increasing the cognitive load.

OLB for grounded communication in multi-domain environments

In the context of multidomain battles, grounded communication becomes essential for team and task maneuvering (i.e., cross-domain cyber operations). Historical and contemporary military

norms and practices of communication will not suffice (General D. Perkins in Tan, 2016). Changes in education and training will be necessary to meet the potential consequences of the changing and diverse nature of the battlefield. The increased inter- connectivity, reliance, and conjunction of multiple domains translate to heightened operational complexity, and affects leaders, decision makers, operators, and soldiers on the ground (Ministry of Defence, 2015). The extent and complexity of tasks will likely require domain-specific expertise working in collaboration with expertise from other conflicting or complementary domains, in a form of “multidomain problem solving.” As earlier research in teams and collaboration shows, it is not enough to put people with a particular expertise or the “right” knowledge together in a group and expect them to work seamlessly (Hackman, 1990; Mathieu, Tannenbaum, Donsbach, & Alliger, 2014). This phenomenon occurs as teams of experts are often hierarchically structured (Brun et al., 2003) and their approach to mastering the complexity of the given environment is to divide the given task into manageable pieces and delegate it to the expert team members (Brun et al., 2003). Brun and colleagues (2003) further pointed to the fact that hierarchical structures may have a negative influence on team communication. In hierarchical teams, performance suffers as the level of communication rises through the chain-of-command (Cannon-Bowers, Salas, & Converse, 1993), and communication is characterized by questions and answers. This is contrary to flat structured teams where peer relationship behavior is directed into finding and offering information based on one’s own initiative (Urban, Bowers, Monday, & Morgan Jr., 1995) leading to better communication and performance.

OLB for improved cross-cultural team communication

The momentary need for grounded communication is explored in time-framed tasks, often with routine actions and stable competence demands (i.e., a flight plan from A to B; Morrow & Fischer, 2013). This leads to the use of artifact tools, such as checklists or as in read-back strategies to ensure grounded communication. Although relevant, some conclusions have relied heavily on results from US research on US personnel (Brun et al., 2003). This reliance leads to research implications when a similar task includes cultural aspects or cross-cultural collaboration in a complex multidomain sociotechnical cyber-physical system, where teams operate with overlapping schedules and responsibility gets transferred (Morrow & Fischer, 2013). Training metacognitive skills to support improved orientation in cross cultural multidomain operating environments could give an advantage to military personnel as they attempt to locate communication partners. The cyber domain is creating novel communication challenges compared to direct face-to-face communications framed by physical presence. Digital communication and time-lagged interaction poses particular challenges for the communicators both on the sending and the receiving end. Awareness about these sensitivities is therefore increasingly relevant as more digital, indirect, and asynchronous the communication becomes.

Conclusion

In an era of cyber operations and multi-domain battles, new challenges are presented for military training and education. Cognitive engineering can provide theoretical models to understand the conditions of safe and effective communication and design interventions to increase communication skills, which have been shown to be one of the most frequent sources of human failure or under-performance in safety-critical sociotechnical systems both in the civil as well as military domains. As a consequence, teaching and training in the military cyber domain needs to acknowledge the need for knowledge building in psychological functions as represented in enhanced metacognitive skills and mutual perspective-taking.

By applying the Hybrid Space theoretical framework, we locate communication partners within a cognitive space determined by tactical/strategic and cyber-physical/socio- technical dimensions. The proposed three-phase OLB model describes the consecutive and complementary steps that

lead to a better grounding of communication in a field of overlapping expertise and separated responsibilities along the authority gradient typical for military context.

In an attempt to meet today's challenges and as a means of taking justified science-based steps toward future teaching doctrines in cyber education, the NDCA aims to enhance future cyber operators' communication skills by training and teaching the aforementioned skills from early stages in their education.

Future work

What remains to be studied is if it is enough to rely on momentary grounding measures or whether teams, working in complex hybrid environments should expend greater effort grounding communication ahead of operations. The NDCA are conducting empirical studies aimed at applying the OLB model in various contexts relevant for military cyber operations and in non-military contexts. This includes communicative challenges on the team level, monitoring communicative processes in real time—the role of cognitive agility for grounded communication and performance assessment—and the influence of personality characteristics and the changing role of leadership in a cyberspace context.

Notes

1. Sociotechnical system is the interaction of people and technology, composed of social, management and technical subsystems (Troxler & Lauche, 2015).
2. Cyber operations is defined as the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace (Schmitt; Tallinn Manual, 2013).

References

- Argyris, C. (1991). Teaching smart people how to learn. *Harvard Business Review*, 69, 3.
- Blum-Kulka, S., House, J., & Kasper, G. (1989). Cross-cultural pragmatics: Requests and apologies. *Advances in Discourse Processes*, 31. Norwood, NJ: Ablex Publishing Corporation.
- Brigden, D., & Purcell, N. (2004). *Focus: Becoming a reflective practitioner*. York, UK: Higher Education Academy. [Online] Available at: http://www.heacademy.ac.uk/resources/detail/subjects/medev/Focus_Becoming_a_reflective_practitioner
- Brun, W., Ekornås, B., Kobbeltvedt, T., Pallesen, S., Hansen, A., Laberg, J. C., . . . Johnsen, B. H. (2003). Betydningen av felles mentale modeller for beslutningstaking i operative team. *Norwegian Military Journal*, 11(3), 22-27.
- Cannon-Bowers, J. A., Salas, E., & Converse, S. (1993). Shared mental models in expert team decision making. In N. J. Castellan Jr. (Ed.), *Individual and group decision making: Current issues* (pp. 221-246). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Cannon-Bowers, J. A., & Salas, E. E. (1998). *Making decisions under stress: Implications for individual and team training*. Washington, DC: American Psychological Association.
- Clark, H. H. (1996). *Using language*. Cambridge, UK: Cambridge University Press.

- DeChurch, L. A., & Mesmer-Magnus, J. R. (2010). The cognitive underpinnings of effective teamwork: A meta-analysis. *Journal of Applied Psychology*, 95(1), 32–53. doi:10.1037/a0017328
- Entin, E. E. (2004). Communications and Coordination Across Low and High Fidelity Simulation Environments. Retrieved April 20, 2016, from http://www.dodccrp.org/events/2000_CCRTS/html/pdf_papers/Track_4/027.pdf?ref=Guzels.TV
- Espevik, R., Johnsen, B. H., & Eid, J. (2011). Communication and performance in co-located and distributed teams: An issue of shared mental models of team members? *Military Psychology*, 23(6), 616–638. doi:10.1080/08995605.2011.616792
- Fischer, U., & Orasanu, J. (2000). Error-challenging strategies: Their role in preventing and correcting errors. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 44(1), 30–33. doi:10.1177/154193120004400109
- Freedberg, S. (2016 October 05). Miserable, disobedient & victorious: Gen. Milley's future US soldier. *Breaking Defense, Air, Intel & Cyber, Land, Sea, Strategy & Policy*. Retrieved from <http://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/>
- Grice, H. P. (1975). Logic and Conversation. In P. Cole & J. Morgan (Eds.), *Syntax and semantics* (Vol. 3, pp. 41–58). New York, NY: Academic Press.
- Hackman, J. R. (Eds.). (1990). *Groups that work (and those that don't): Creating conditions for effective teamwork*. San Francisco, CA: Jossey-Bass.
- Jacobsson, M., Hargestam, M., Hultin, M., & Brulin, C. (2012). Flexible knowledge repertoires: Communication by leaders in trauma teams. *Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine*, 20(1), 44. doi:10.1186/1757-7241-20-44
- Jason, L. A., Keys, C. B., Suarez-Balcazar, Y. E., Taylor, R. R., & Davis, M. I. (Eds.). (2004). *Participatory community research: Theories and methods in action*. Washington, DC: American Psychological Association.
- Joiner, W. B., & Josephs, S. A. (2006). *Leadership agility: Five levels of mastery for anticipating and initiating change*. San Francisco, CA: John Wiley & Sons.
- Jøsok, O., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., & Ward, P. (2016). Exploring the hybrid space - theoretical framework applying cognitive science in military cyberspace operations. In Schmorow, D. D., Fidopiastis, C. M. M. (Eds.) *Foundations of augmented cognition: Neuroergonomics and operational neuroscience Lecture Notes in Computer Science*, 9744, (pp. 178–188). New York, NY: Springer.
- Kegan, R., & Lahey, L. L. (2009). *Immunity to change: How to overcome it and unlock potential in yourself and your organization* (1st ed.). Boston, MA: HBR Press.
- Korb, W., Geißler, N., & Strauß, G. (2015). Solving challenges in inter-and trans-disciplinary working teams: Lessons from the surgical technology field. *Artificial Intelligence in Medicine*, 63(3), 209–219. doi:10.1016/j.artmed.2015.02.001
- Krulak, C. C. (1999). The strategic corporal: Leadership in the three block war. *Marine Corps Gazette*, 83(1), 18–22.
- Lemay, A., Leblanc, S. P., & Jesus, T. D. (2015). Lessons from the strategic corporal: Implications of cyber incident response, *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (pp. 61-66), SIGMIS-CPR '15, Newport Beach, CA.

- Letsky, M. P., Warner, N., Fiore, S., & Smith, C. A. P. (Eds.). (2008). *Macrocognition in teams: Theories and methodologies*. London, England: Ashgate.
- Liddy, L. (2004). The strategic corporal: Some requirements in training and education. *Australian Army Journal*, 2(2), 139–148.
- Mathieu, J. E., Tannenbaum, S. I., Donsbach, J. S., & Alliger, G. M. (2014). A review and integration of team composition models: Moving toward a dynamic and temporal framework. *Journal of Management*, 40(1), 130–160. doi:10.1177/0149206313503014
- McChrystal, S. A., Collins, T., Fussell, C., & Silverman, D. (2015). *Team of teams: New rules of engagement for a complex world*. New York, NY: Penguin.
- Mills, P., Neily, J., & Dunn, E. (2008). Teamwork and communication in surgical teams: Implications for patient safety. *Journal of the American College of Surgeons*, 206 (1), 107–112. doi:10.1016/j.jamcollsurg.2007.06.281
- Ministry of Defence (2015, December 14). Strategic Trends programme: Future operating environment 2035. Retrieved from <https://www.gov.uk/government/publications/future-operating-environment-2035>
- Monk, A. (2009). *Common ground in electronically mediated conversation*. San Rafael, CA: Morgan & Claypool Publishers.
- 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* (pp. 178–199). New York, NY: Oxford University Press.
- NATO Cooperative Cyber Defence Centre of Excellence, (2016). NATO Recognises cyberspace as a ‘domain of operations’ at warsaw summit. Retrieved from <https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-war-saw-summit.html>
- Putz, M., & Raynor, M. (2004). Integral leadership: Overcoming the paradox of growth. In J. Reams (2005). What’s integral about leadership? A reflection on leadership and integral theory. *Integral Review*, 1, 118–131.
- Reams, J. (2005). What’s integral about leadership? A reflection on leadership and integral theory. *Integral Review*, 1, 118–131. Røislien, H. (2015). When the generation gap collides with military structure: The case of Norwegian cyber officers. *Journal of Military and Strategic Studies*, 16(3), 23–44.
- Rosen, M. A., Fiore, S. M., Salas, E., Letsky, M., & Warner, N. (2008). Tightly coupling cognition: Understanding how communication and awareness drive coordination in teams. *International Journal of Command and Control*, 2(1), 1–30.
- Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge, England: Cambridge University Press.
- Searle, J. R. (1969). *Speech acts: An essay in the philosophy of language*. Cambridge, England: Cambridge University Press.
- Sexton, J. B., Thomas, E. J., & Helmreich, R. L. (2001). Error, stress, and teamwork in medicine and aviation: Cross sectional surveys. *Journal of Human Performance in Extreme Environments*, 6(1), 5–11. doi:10.7771/2327-2937.1019

Stringer, K. D. (2009, September-October). Educating the strategic corporal: A paradigm shift. *Military Review*, 89(5), 87–95. Tan, M. (2016, October 3). The multi-domain battle. *Defense News Weekly*. Retrieved from <http://www.defensenews.com/articles/the-multi-domain-battle>

Tapscott, D. (2014). *The digital economy anniversary edition: Rethinking promise and peril in the age of networked intelligence*. New York, NY: McGraw-Hill.

Tikk-Ringas, E., Kerttunen, M., & Spirito, C. (2014). Cyber security as a field of military education and study. *Joint Forces Quarterly*, 75(4), 57–60.

Trejo, B. C., Richard, E. M., Van Driel, M., & McDonald, D. P. (2015). Cross-cultural competence: The role of emotion regulation ability and optimism. *Military Psychology*, 27(5), 276–286. doi:10.1037/mil0000081

Troxler, P., & Lauche, K. (2015, July 15). Assessing creating and sustaining knowledge culture in organisations. Retrieved from http://www.academia.edu/1964062/Assessing_Creating_and_Sustaining_Knowledge_Culture_in_Organisations

Trujillo, C. (2014). The limits of cyberspace deterrence. *Joint Forces Quarterly*, 75(4), 43–52.

Urban, J. M., Bowers, C. A., Monday, S. D., & Morgan Jr., B. B., Jr. (1995). Workload, team structure, and communication in team performance. *Military Psychology*, 7(2), 123–139. doi:10.1207/s15327876mp0702_6

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. doi:10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Course Technology.

Xiao, Y., Seagull, F. J., Mackenzie, C., Ziegert, J., & Klein, K. J. (2003, October). Team communication patterns as measures of team processes: Exploring the effects of task urgency and shared team experience. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 47(12), 1502–1506. Los Angeles, CA: SAGE Publications. doi:10.1177/154193120304701228

PAPER III

Not included due to copyright restrictions

PAPER IV

Not included due to copyright restrictions

PAPER V

Not included due to copyright restrictions

PAPER VI

Not included due to copyright restrictions

PAPER VII

Cognisance as a Human Factor in Military Cyber Defence Education

Benjamin J. Knox^{*} Ricardo G. Lugo^{**} Stefan Sütterlin^{***}

^{*} Norwegian Defence University College, Oslo, Norway (e-mail: bknox@cyfor.mil.no)

^{**} Inland Norway University of Applied Sciences, Elverum, Norway (e-mail: ricardo.lugo@inn.no)

^{***} Østfold University College, Halden, Norway (e-mail: stefan.sutterlin@hiof.no)

Abstract: Cyber Defence Exercises (CDX) are common training and learning tools. A recently discussed challenge in cyber defence teaching and training is the gap between the fast technological advancement accompanied by rapidly changing demands on future cyber defence operators, and the lack of science-based teaching and training methods.

A growing body of evidence suggests a crucial role of human factors as a central predictor for human performance in sociotechnical systems. While this has been acknowledged in a wide range of safety-critical applied fields, there is still a lack of knowledge about the impact of human factors on cyber defence performance. The lack of conventional metrics of performance and learning progress contribute to this deficit.

To address this gap, the Norwegian Defence Cyber Academy (NDCA) follows a science-based educational approach that identified in a series of empirical studies cognitive-psychological predictors for learning success of future cyber defence operators. These predictors and elements of a human factors research program are deeply embedded into educational practice and include processes such as metacognition, self-regulation, coping, communication and shared mental modelling. Slow education methods and mentoring are fundamental to enabling the advancement of human factors cognisance among military cyber cadets.

As a tool for efficient training, the NDCA developed and implemented a mentoring concept that involves a cyber defence retrospective timeline analysis involving expert and practitioner level mentors. The timeline differentiates between performance relevant hard- and soft-skills and leads progressively towards an alignment of Security Operation Centre (SOC)- and expert judgments of performance. The NDCA argues that this educational concept facilitates educational benefits based on insight, accurate self-perception, motivation and decreased team workloads following more efficient collaboration.

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

1. INTRODUCTION

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

1.1 Education in Human Factors

The rapid emergence of cyber security and cyber defence as a field of study and practice has led to a mismatch between evidence-based teaching and training methods of future cyber operators on one side, and the rapidly progressing skill requirements for effective and adaptive performance on the other (Hoffman 2014, Upton & Creese 2014). A clear educational and scientific focus is required to ensure cyber operators develop the necessary technical competencies, as well as the mental skills that have the capacity to avoid the natural inclination towards cognitive rigidity and instead promote cognitive flexibility (Feltovich, Spierer & Coulson 1997, Klein & Baxter 2006). Achieving success in the face of adversaries who

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

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

1.2 The role of mentoring for metacognition and motivation

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

1.3 Retrospective verbal reports as an educational tool in CDX

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

2. EDUCATIONAL APPROACH IN THE NORWEGIAN DEFENCE CYBER ACADEMY

At the NDCA the Bachelor of Technology is grounded in a philosophy of mentorship from selection to graduation. The NDCA feeds officers and non-commissioned officers to all defence services. With the right mental competencies, cyber cadets can adapt rapidly after graduation to their chosen operating environment and perform. Mentoring can scaffold cyber hard skills and human soft skills. At the NDCA these two features are constantly combined and tested in order to ensure holistic performance enhancement at individual and cyber-team level. The approach the NDCA takes to educating military cyber cadets is built upon traditional military methods, combined with methods that are founded in cognitive engineering and techniques known to accelerate learning (Hoffman 2014) where interventions are made in an attempt to develop adaptive skills. In their final six months cadets specialize in the areas of network establishment and maintenance or defensive cyberspace operations. The NDCA aims to shape individuals capable of governing cyber power effects in military cyberspace operations following a personal development approach. This centres on certain cognitive skills known to support professional performance, such as metacognition, coping strategies (Helkala et al., 2016) self- regulatory processes (Bandura 1986; Bohlmann & Downer 2016), and communication (Knox et al., 2018).

2.1 Slow Education

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

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

The purpose of the retrospective-timeline construction (Figure 1) is to generate observable events, the main actions that were taken, and key mental events that were important to them. The timeline intends to capture their cognition in context and aims to include key moments they noticed, that caught their attention, that they understood, or when their understanding changed, decisions or judgements they made, or gut feelings experienced, moments of being unsure as to what was going on, actions taken or not taken (but considered),

key moments where they had to just trust, or not trust, times when they had to seek or give input to others, and moments of significant communication (including things that were not said, that in hindsight, needed saying) intended to build self-efficacy, domain understanding, cyber-team performance and where possible; accelerate learning.

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

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

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

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

- **SOC 1:** Two experienced cyber defence practitioner level mentors (one on the cusp of meeting expert criteria). Both were Non Commissioned Officers (NCO) and neither had previous experience or training in retrospective-timeline activity.
- **SOC 2:** One military officer expert mentor and one practitioner level NCO. Neither had experience or training in retrospective-timeline activity.
- **SOC 3:** One civilian expert mentor plus an NCO practitioner. Neither had experience or training in retrospective timeline activity.
- **SOC 4:** One military officer expert mentor with training and experience in retrospective-timeline activity, plus a civilian practitioner with no experience or training in retrospective-timeline activity.

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

3. EFFECTS AND EXPERIENCES

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

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

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

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

4. FUTURE WORK

A next step for the NDCA is to build on earlier slow education approaches (Knox et al., 2019). The intent is to further encourage deeper mental processes in the form of improved cadet situational metacognitive judgements (SMJ). This can be achieved by asking them to rate the three areas judgement of own performance, confidence, and effort. The recommended methodology for this would be cadets answer short questionnaires at key times during the day. For this purpose, the Task Workload Scale should be omitted due to the scales focus on personal (individual) demands, but the Teamwork and Task-Team component should be included.

4.1 Pre-mission questions

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

4.2 Post-mission and post-RT1 questions:

- How well did you think you did?
- How sure are you about this judgment?
- How confident were you during the exercise?
- How much effort did you put in through the exercise?

(Continuous assessment of incr./decr. amounts.)

- How well did your team do?
- How sure are you about this?

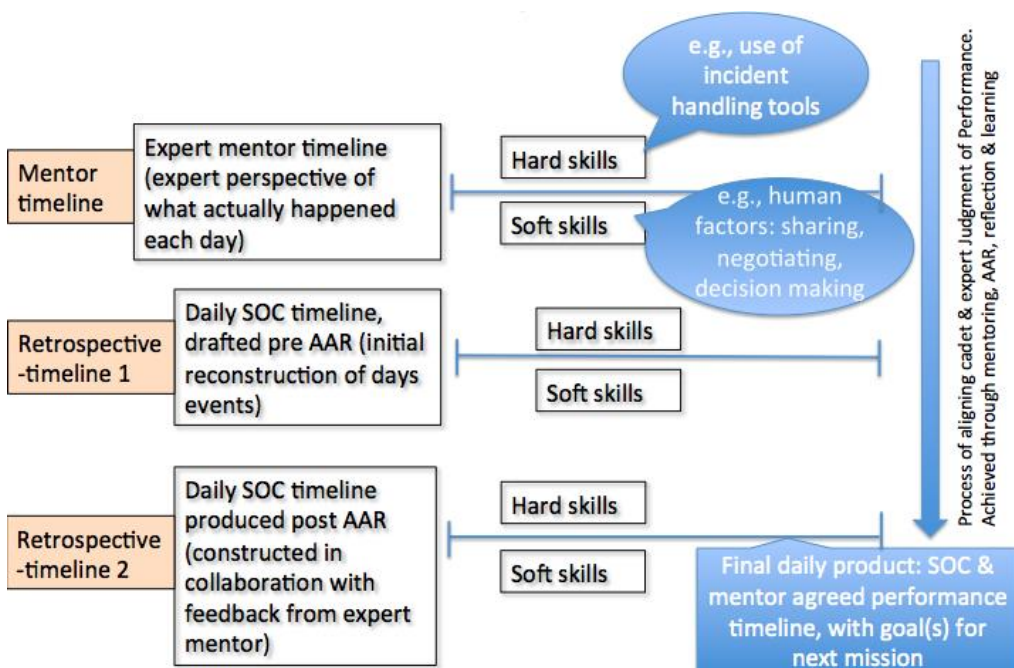


Fig. 1. Mentor concept as implemented in the annual capstone CDX. Three timelines are produced each day in each SOC in accordance with the days cyber related events. This process should enable the cadets to identify realistic and achievable goals for improved performance for the next day.

4.3 Post-RT2 questions:

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

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

5. CONCLUSION

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

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

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

6. REFERENCES

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

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

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

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

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

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

- Ericsson, K, Krampe, R, & Tesch-Roemer, C 1993, The role of deliberate practice in the acquisition of expert performance, *Psychological Review*, vol. 100, pp. 363-406.
- Fadde, P & Klein, G 2010, Deliberate performance: Accelerating expertise in natural settings, *Performance Improvement*, vol. 49, no. 9, pp. 5-14.
- Feltovich, P, Spiro, R, & Coulson, R 1997, *Expertise in context: Human and machine*, MIT Press, Cambridge, MA.
- Giles, K 2016 *Russias new tools for confronting the west: continuity and innovation in Moscows exercise of power*, Royal Institute of International Affairs, Chatham House.
- Gutzwiller, RS, Fugate, S, Sawyer, BD & Hancock, PA 2015, The human factors of cyber network defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 59, no. 1, Sage CA: Los Angeles, CA, pp. 322-326.
- Halpern, D 1998, Teaching critical thinking for transfer across domains: Disposition, skills, structure training, and metacognitive monitoring, *American Psychologist*, vol. 53, no. 4, pp. 449-455.
- Helkala, K, Knox, BJ, Jøsok, S, & Lund, M 2016, Factors to Affect Improvement in Cyber Officer Performance, *Information and Computer Security*, vol. 24, no. 2.
- Hoffman, RR, Ward, P, Feltovich, PJ, DiBello, L, Fiore, SM, & Andrews, D 2014, *Accelerated expertise: Training for high proficiency in a complex world*. Psychology Press, New York.
- Kick, J 2014, *Cyber Exercise Playbook (No. MP140714)*, MITRE Corporation, Bedford.
- Klein G, & Baxter, H 2006, Cognitive transformation theory: Contrasting cognitive and behavioral learning, *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC 2006): Training the 21st Century 4- 7 December 2006*, Orlando, Florida, USA.
- Knox, BJ, Josok, O, Helkala, K, Khooshabeh, P, Odegaard, T, Lugo, RG, & Sütterlin, S 2018, Socio-technical communication: The hybrid space and the OLB model for science-based cyber education, *Military Psychology*, vol. 30, no. 4, pp. 350-359.
- Knox, BJ, Lugo, RG, Helkala, K, & Sütterlin, S 2019, Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower, *International Journal of Cyber Warfare and Terrorism*, vol. 9, no. 1, pp. 48-66.
- Lugo, RG, Sütterlin, S, Knox, BJ, Jøsok, Helkala, K, & Lande, N 2016, The moderating influence of self-efficacy on interoceptive ability and counterintuitive decision making in officer cadets, *Journal of Military Studies*, vol. 7, no. 1, pp. 44-52.
- Meichenbaum, D 1985, Metacognitive methods of instruction: Current status and future prospects, *Special Services in the Schools*, vol. 3, no. 1-2, pp. 23-32.
- Nietfeld, J & Schraw, G 2002, The effect of knowledge and strategy training on monitoring accuracy, *The Journal of Educational Research*, vol. 95, no. 3, pp. 131-142.
- Nolen-Hoeksema, S 1991, Responses to depression and their effects on the duration of depressive episodes, *Journal of Abnormal Psychology*, vol. 100, no. 4, pp. 569-582.
- Rhodes, J 2008, Improving youth mentoring interventions through research-based practice, *American Journal of Community Psychology*, vol. 41, no. 1-2, pp. 35-42.

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

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

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

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

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

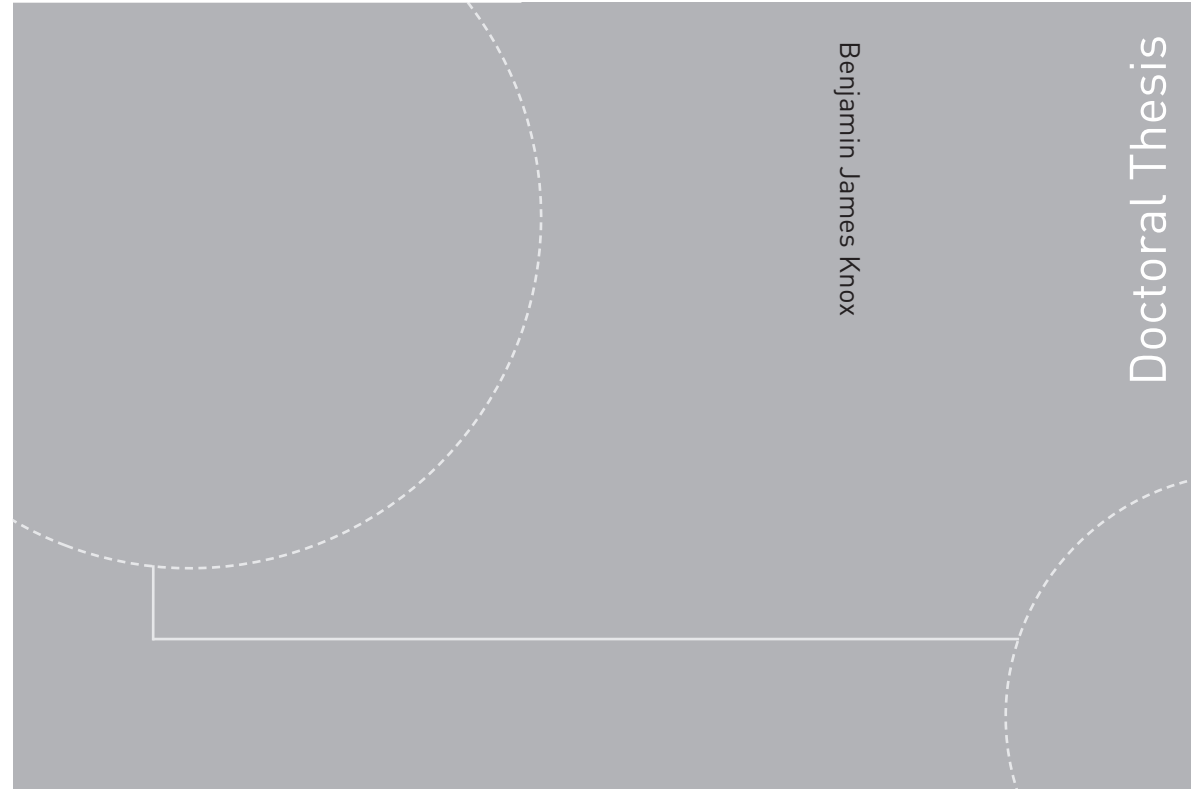
Ward, P & Williams, A 2003, Perceptual and cognitive skill development in soccer: The multidimensional nature of expert performance, Journal of Sport and Exercise Psychology, vol. 25, no. 1, pp. 93-111.

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

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

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

ISBN 978-82-326-4654-8 (printed version)
ISBN 978-82-326-4655-5 (electronic version)
ISSN 1503-8181



Doctoral theses at NTNU, 2020:153

Benjamin James Knox

Cyberpower Praxis: A Study of Ways to Improve Understanding and Governance in the Cyber Domain

Doctoral theses at NTNU, 2020:153

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

 **NTNU**
Norwegian University of
Science and Technology

 NTNU

 **NTNU**
Norwegian University of
Science and Technology