Doctoral theses at NTNU, 2024:278

Torvald Fossåen Ask

Neuroergonomic Approaches to Understanding and Improving Communication of Recognized Cyber Threat Situations

Supervisor:
Dr. Benjamin J. Knox
Co-supervisors:
Prof. Stefan Sütterlin
Dr. Ricardo G. Lugo

Doctoral thesis

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Torvald Fossåen Ask

Neuroergonomic Approaches to Understanding and Improving Communication of Recognized Cyber Threat Situations

Supervisor:
Dr. Benjamin J. Knox
Co-supervisors:
Prof. Stefan Sütterlin
Dr. Ricardo G. Lugo

Thesis for the Degree of Philosophiae Doctor

Trondheim, June 2024

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

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

ISBN 978-82-326-8148-8 (printed ver.)
ISBN 978-82-326-8147-1 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2024:278

Printed by NTNU Grafisk senter

I trow I hung on that windy Tree

nine whole days and nights,

stabbed with a spear, offered to Odin,

myself to mine own self given,

high on that Tree of which none hath heard

from what roots it rises.

None refreshed me ever with food or drink,

I peered right down in the deep;

crying aloud I lifted the Runes

then back I fell from thence.

Nine magic songs I learned from the great

son of Boltorn, Bestla's sire;

And drink I was given, of valued Mead,

Poured by Odrere.

Ere long I bare fruit, and throve full well,

I grew and waxed in wisdom;

word following word, I found me words,

deed following deed, I wrought deeds.

Håvamål, Odin's Quest after the Runes. From Sæmund's Edda.

Summary

Cyber threat situations entail high-stake decision-making processes both within organizations and between the affected organization and external entities. During cyber threat situations, information is shared between individuals tasked with detecting and analyzing cyber threats (cyber operators) and the individuals tasked with making decisions based on receiving that information. This communication often entails technical complexity and is subject to challenges including time pressure, interdisciplinary factors, and frequently an insufficient information basis. These challenges may have a variety of implications for cyber defense decision-making and more research is needed.

Previous research has suggested that there is not enough focus on the role cognition plays in the performance of cyber operators. With cyber threats increasingly challenging the security of digital infrastructures, understanding the cognitive processes underlying human communication becomes crucial. Approaching cognition from the perspective of neuroscience may uncover methodologies that are currently unexplored. This dissertation delves into the application of neuroergonomic approaches to enhance human-to-human communication during cyber threat situations, presenting a theoretical framework grounded in neuroscience findings.

The dissertation includes three foundational studies on the dynamics of team communication and situational awareness in cyber defense settings. The findings highlight the significance of neurophysiological indicators of activity in structures that participate in coordinating cognitive processes and tools that facilitate multisensory integration of cyber threat information as potential influencers of team communication effectiveness and metacognitive situational awareness. A key innovation of this thesis is the exploration of mixed reality technologies in facilitating dyadic team communication and enhancing cyber situational awareness. By comparing 3D mixed reality with traditional 2D representations of network attacks, the study indicates that mixed reality technology can lead to improved communication and awareness among cyber defense teams, although the impact on decision-making requires further exploration.

The dissertation concludes with a critical discussion on the broader implications of these findings for cybersecurity practices and makes suggestions for future research efforts to validate findings. By bridging the gap between neuroscience and cybersecurity, this dissertation lays the groundwork for developing more resilient defenses against cyber threats.

Acknowledgements

A huge thank you to my supervisors Ben, Ric, and Stefan for including me in this project. You have all made this a fun experience and I look forward to continuing our work together.

Ben, it has been a pleasure getting to know you over these last couple of years. I feel a lot of respect for you, and I am genuinely excited about the work that lies ahead of us. This is only the beginning.

To Matt and the CSI core team, I really appreciate all the eye-opening discussions we've had. You are a rare group of creative and driven people (with the right touch of madness) and I always come away from our discussions with a new idea growing inside my brain.

Thank you to CISK for granting me the opportunity to do this research by giving me access to your students and your facilities. It has spawned new questions that will keep me busy for a long time. That is, in my opinion, the best of all outcomes.

To my friends and family, thank you for all the support and understanding throughout this entire journey.

A special thank you to Daniel for all the stimulating discussions that either got my mind off work during coffee breaks or helped me see things from a different perspective. You are a high-powered mutant of some kind never even considered for mass production.

Another special thank you to Ric and Stefan for encouraging me to pursue my interests in science. It has been a defining influence in my life that I can never thank you enough for. I know I am not the only one feeling gratitude towards you two. You guys are special.

T.

Contents

Tables

Figures

Abbreviations

2D	Two-dimensional
3D	Three-dimensional
ACDICOM	Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations
AR	Augmented reality
BT	Blue team
CatCorrect	Category correct
CDG	Cyber defense games
CDX	Cyber defense exercise
CERT	Cyber emergency response team
CEX	Cyber engineering exercise
CIA	Confidentiality, integrity, and availability
CISO	Chief information security officer
CO	Cyber operator
ComCol	Communication and collaboration
CTI	Cyber threat intelligence
CTS	Cyber threat situation
CTSA	Cyber team situational awareness
Cyber SA / CSA	Cyber situational awareness
DLPFC	Dorsolateral prefrontal cortex
DMN	Default mode network
ENISA	The European Union Agency for Cybersecurity
FPN	Frontoparietal network

HFHRV	High frequency heart rate variability
HS	Hybrid space
ICT	Information communication technology
IDS	Intrusion detection system
IPS	Intrusion prevention system
ISPMDV	Interactive stereoscopically perceivable multidimensional data visualization
JOP	Judgment of performance
MELANI	Swiss Reporting and Analysis Center for Information Assurance
MCA	Metacognitive accuracy
MPFC	Medial prefrontal cortex
MR	Mixed reality
NASA-TLX	National Aeronautics and Space Administration Task Load Index
NATO CCDCOE	The North Atlantic Treaty Organization Cooperative Cyber Defense Centre of Excellence
NDCA	Norwegian Defense University College, Cyber Academy
NIST	National Institute of Standards and Technology
NSD	Norwegian Social Science Data Services
OLB	Orient, locate, and bridge
Pcap	Packet capture
PFC	Prefrontal cortex
PRISMA	Preferred Reporting Items for Systematic Evaluations and Meta-Analyses
RCP	Recognized cyber picture
RMSSD	Root mean square of successive NN differences

RT	Red team
SA	Situational awareness
SAGAT	Situation awareness global assessment technique
SAM	Self-assessment manikin
SIEM	Security information and event management
SIS	Security information sharing
SITREP	Situational report
SLDM	Strategic level decision-maker
SOC	Security operations center
sRCP	shared recognized cyber picture
STS	Sociotechnical systems
TDK	Threat and defense knowledge
TMM	Team mental models
TTE	Time-to-end
TTI	Technical threat intelligence
TTP	Time-to-approval
TTX	Tabletop exercise
TWLQ	Team workload questionnaire
TWLS	Team workload scale
VDE	Virtual Data Explorer
vmHRV	Vagally mediated heart rate variability
VR	Virtual reality

Chapter 1

1 Introduction

1.1. The Problem

This thesis aims to address the previously identified communication problems in cybersecurity (Agyepong et al., 2019; Knox et al., 2018). The problems concern human-to-human communication in cyber threat situations, and especially the relay of cyber threat-related information between individuals tasked with detecting, investigating, and reporting on cyber threats (cyber analysts), and between cyber analysts and the individuals who make cyber defense decisions based on those reports (decision-makers). At the level of the cyber analyst, communication can be any verbal or written, structured/rehearsed or spontaneous sharing of information. The communication problems that arise between cyber analysts that work in teams are often related to cognitive load related to the complexity of the information and task environment (Brilingaitė et al., 2022; Champion et al., 2012). The roles of cyber analyst and decision-maker are often divided between different individuals in an organization (Jøsok et al., 2017; Staheli et al., 2016) which poses organizational challenges to communication (Knox et al., 2018). If the communication between cyber analysts and decision-makers is inadequate, for example, if critical information about an ongoing cyber threat is lost in the communication process, it may have a negative impact on subsequent decision-making. This can have severe consequences for an organization, and at the extreme, for national security. Due to the stakes being so high, there is a level of failure intolerance associated with defending against cyber threats. Advancing the scientific understanding of factors that determine the efficiency and accuracy of human-to-human communication of cyber threat information will benefit cybersecurity in both public and private sectors through interventions, as well as through the development of new standards for information exchange. This introductory chapter provides an overview of the context of the research presented in this thesis and how it has approached finding a solution to communication problems in cybersecurity.

1.2. The Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) Project

The work presented in this thesis was conducted as part of the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) project. The ACDICOM project aims to cover the knowledge gap regarding what influences human-to-human communication of cyber threat information as it relates to human limitations in cybersecurity performance. The ACDICOM project is funded by the Norwegian Research Council (#302941). Description of the project can be found in Table 1 (taken from [https://prosjektbanken.forskningsradet.no/en/project/FORISS/302941]).

While cyber resilience on the organizational and national level is subject to rapid technological progress, there is an urgent need for a scientific understanding of the individual human's limitations in cybersecurity performance. Project Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) develops evidence-based standards to improve human interaction in cybersecurity performance. For an organization to maintain control in its cyberspace and to make good cyber defense decisions, having an accurate Recognized Cyber Picture (RCP) is crucial. Security Operation Centers work as teams with technical tasks and decision making assigned to different individuals. In this context RCPs need to be shared and communicated across platforms, in differing modalities, and often across organizational boundaries and societal sectors. Where this communication is challenged due to practical, cultural, or simply logistic hindrances, the resulting shared RCP is inaccurate and critical information gets lost due to the decision-makers lack of situational awareness. This project focuses on dyadic communication to establish a shared RCP, develops common standards for information exchange in collaborative settings across sectors, organizational hierarchies, and cultures. Implemented by means of naturalistic settings in Cyber Defense Exercises as well as experimental research, this interdisciplinary collaboration provides a toolbox for the monitoring of communication efficiency and the implementation of findings in existing educational practices. The close collaboration with educational institutions facilitates sustainable behavioral changes needed for the improvement of human factors in cyber defense education. Actors from the private industry and national as well as supranational cyber defense forces are involved in all stages of the project and provide advice to ensure maximal practical applicability of the research questions and products.

Table 1. ACDICOM project description on the Norwegian Research Council website

In short, the goal of ACDICOM is to ensure good cyber defense decision-making by improving communication of cyber threat information between individuals. Of special interest to the project is communication between individuals with diverse backgrounds and technical competence, including (but not limited to) the analysts doing forensic work in security operation centers, and the decision-makers that decide how to act on the information collected and reported on by analysts.

1.3. Scope

Communication between individuals is affected by factors related to the background of the individuals, including (but not limited to) education, knowledge, experience, organizational hierarchies, how familiar communication partners are with each other, as well as the situational factors influencing the communication setting. Several potential sources of communication problems in cyber threat situations have been reported in the literature. Some of them include decreasing levels of technological understanding between analysts and decision-makers at increasing levels in the organizational and decision-making hierarchy (e.g., Knox et al., 2018), varying information needs due to shifts in priorities at higher levels of management in an organization (Staheli et al., 2016; Tinde, 2022), especially for individuals whose responsibilities are not solely based on dealing with cyber threats (Varga et al., 2018; Tinde, 2022), lack of interaction between chief information security officers (CISOs) and the board of directors in an organization (Oltsik, 2019), communication errors occurring during handovers at the end of long shifts (noted in Veksler et al., 2020), high levels of stress associated with high time pressure and high information load (Champion et al., 2012), as a well as a lack of explicit focus on relevant psychological (or cognitive) communication-related skills and processes in cybersecurity training and education (Knox et al., 2019). Other reported sources of communication problems include non-overlapping standards and mental models regarding how to communicate efficiently during a cyber threat in cyber teams (Champion et al., 2012; Hámornik and Krasznay 2018; Steinke et al. 2015), conflicts between different tasks, cyber operators not knowing how to use platforms for information exchange (Brilingaitė et al., 2022), and negative self-perceptions related to gender stereotypes (Fisher, 2022).

A related, more general problem in the context of cybersecurity is the lack of well-established performance metrics for cyber analysts working in teams, which makes it hard to evaluate the relevance of previous research (Agyepong et al. 2019). The thesis applied a general and broad approach to human communication during cyber threat situations in an initial systematic review that laid the foundation for the rest of the research. However, the scope of the subsequent empirical studies was considerably narrowed down, and concerned identifying neuroscientific performance indicators and interventions, specifically as they relate to how cyber analysts operating in teams navigate complex working environments. The present scope was set to advance our understanding of how cognitive information processing upstream of communication in cyber teams influences their understanding of cyber threats, communication

behaviors, and experienced communication load. The nature of the research in this thesis is applied, where the aim of the research is to solve specific problems for specific groups of people, and where the resulting contributions should translate to actionable outcomes. The participants in the empirical studies consisted of cyber cadet officers at the Norwegian Cyber Defense Academy (NDCA) participating in a defensive cyber operations exercise and a subsequent experiment, both simulating a network attack. Thus, the findings are directly related to naturalistic settings, and especially for individuals who are future cybersecurity experts at the level of national security.

In addressing the aims outlined in the applied scope of the research, the thesis relied on a variety of interdisciplinary methodologies and frameworks, drawing most notably on previous work conducted within the field of human factors, cognitive engineering, and neuroscience.

1.4. Previous Work and Direction of Research

The work presented in this thesis builds on the research conducted previously by Gutzwiller and colleagues (2015, 2016, 2020), Jøsok and colleagues (2016, 2017, 2019), Knox and colleagues (2017, 2018), Lugo and colleagues (2016, 2017a), and Lugo and Sütterlin (2018). This previous research is mainly concerned with how cyber operators navigate their complex and stressful working environments, and the implications it has for communication and performance in cyber operative contexts. Gutzwiller and colleagues has noted that there is a need for more research on cyberspace and human cognition in cybersecurity working-environments (Gutzwiller et al., 2015), especially with respect to the role of human cognition in situational awareness during cyber threat situations (Gutzwiller et al., 2016), and identifying ways of measuring situational awareness in cyber threat situations to assess its impact on human performance (Gutzwiller et al., 2020). In their research, Jøsok and colleagues (2016) has suggested that the cybersecurity working-environment can be understood in terms of the interconnectedness between cyber and physical space, and tensions between tactical, operational, and strategic priorities in decision-making and action. With respect to human cognition, the cyber-physical interconnectedness and the tactical-strategic tensions have been conceptualized as opposing horizontal and vertical dimensions, respectively, in a hybrid space framework (Jøsok et al., 2016), where communication issues can occur if the cognitive focus of individuals are located at different positions along these axes (Jøsok et al., 2016, 2017). Factors such as professional background, as well as current priorities and ongoing tasks have

been proposed to dictate where individuals' cognitive focus is located within the hybrid space. The work of Jøsok and colleagues (2016, 2019), Knox and colleagues (2017, 2018), and Lugo and colleagues (2017a) have suggested that ability to monitor and regulate one's own cognitive processes and behaviors (metacognition; Jøsok et al., 2016, 2019; Knox et al., 2017), and communication and coordination processes (Knox et al., 2018; Lugo et al., 2017) influences an individual's ability to move their cognitive focus, and to facilitate communication, across the hybrid space. This ability is referred to as cognitive agility (Jøsok et al., 2019; Knox et al., 2017). The significance of this work and why the present research builds on it is that it provides a cognitive framework for understanding how cyber analysts navigate (or fail to navigate) their complex working-environments. The work of Jøsok and colleagues (2016, 2019) and Knox and colleagues (2017, 2018) in particular constitute the main theoretical foundation of the work presented in this thesis.

Knox and colleagues (2018) proposed that the deliberate application of metacognitive processes for self-location in the hybrid space and perspective taking can be used to bridge communication across the hybrid space to ensure that critical cyber threat information is not lost during communication. Finally, Lugo and Sütterlin (2018) has emphasized the contribution of emotional processes on the performance of cyber operators, suggesting that the ability to regulate those emotional processes can influence performance, especially in cases where information processing is linked to decision-making tasks that are subject to biased decision-making. The significance of this has been to include the assessment of emotional measurements that relate to emotional biases in information processing with downstream implications for metacognitive processes and situational awareness.

The following issues are currently not addressed by these previous works (Jøsok et al., 2016, 2017, 2018; Knox et al., 2017, 2018; Lugo et al., 2017; Lugo & Sütterlin, 2018). While self-report measures of metacognitive self-regulation were related to self-reported movements in the hybrid space during cyber defense exercises (CDXs; Jøsok et al., 2019), thus indicating cognitive agility (Knox et al., 2017), the research does not establish a performance indicator for navigating complex information environments in a way that is related to cybersecurity-specific information processing outcomes such as situational awareness or the accuracy of metacognitive evaluations of ability to perform in a cyber threat situation, nor is it related to perceived workloads associated with communication, which should be lower for individuals who are more cognitive agile, according to its theoretical foundation (Jøsok et al., 2016, 2019;

Knox et al., 2017, 2018). The work included in this thesis aims to address this shortcoming by including objective (neurophysiological) and subjective (self-report) measures of neurocognitive performance indicators and relating them to outcomes such as metacognitive judgments of performance, situational awareness, and experience communication load in a naturalistic setting. While emotional processes have been related to information processing and subsequent decision-making in cyber cadets (Lugo et al., 2016; Lugo & Sütterlin, 2018), this has not been assessed with respect to situational awareness and metacognition in a naturalistic setting, nor has it been related to determine what role emotion regulation plays in how emotional processes influence information processing in cybersecurity-specific contexts. The work presented in this thesis address this shortcoming by comparing self-reported emotional states with objective measurements of neurophysiological emotion regulation capacities and its subsequent relationship with evaluation of team performance, metacognitive accuracy, and situational awareness. While metacognition is suggested to facilitate navigation of cybersecurity-related information environments (Jøsok et al., 2016), the relationship between situational awareness and metacognition has not been assessed in a naturalistic cybersecurity context. The present thesis addresses this shortcoming both at the individual level and in teams. The thesis also addresses an unanswered theoretical question related to ambiguous observations; if movements along the hybrid space dimensions represent cognitive agility (Jøsok et al., 2019; Knox et al., 2017), if the movements rely on metacognition (Jøsok et al., 2016), and if metacognition facilitates communication across the hybrid space (Knox et al., 2018), but such movements are positively associated with self-reported communication demands (Lugo et al., 2017), then does that mean that individuals who communicate efficiently because of metacognitive abilities experience more communication demands but do more hybrid space movements? How does this relate to observations related to frequent task switching between cyber and physical domains, and possible detrimental effects on performance related to task switching related to task resolution discussions, the negative relationship between communication and situational awareness (Brilingaitė et al., 2022; Buchler et al., 2016; Gutzwiller et al., 2015), and null findings relating metacognition to hybrid space movements (Knox et al., 2017)? What if more self-reported movements represent "being pushed around" the hybrid space rather than making metacognitively controlled movements? This question is partly addressed in paper III by simultaneously assessing self-reported measures of communication demands, observed task resolution communication, and performance on situational awareness items.

Coming from a neuroscience background, building on this research has entailed asking neuroscientific questions and identifying neuroscientific theories and data that may be relevant to the observations, proposed constructs, frameworks, and models reported in previous work. The following argumentation can be made for why including neuroscience in cybersecurity research is useful: It has been proposed that the limitation of cognitive processing is the bottleneck for human performance in cybersecurity, but little is known about cyber operator cognition (Gutzwiller et al., 2015; Lugo & Sütterlin, 2018). Human cognition is the output of the biological processes of the human brain. For the sake of precision, it seems rational to approach the problem of improving human-to-human communication in cyber threat situations by targeting the seat of human cognition, which is the brain:

> "[...] *the basic enterprise of human factors/ergonomics can be considerably enhanced in a fundamental way if we also consider the brain that mediates and makes possible human performance in the real world*" (Parasuraman, 2003, pp. 6).

For instance, if the brain is the component that converts cyber threat information or cyber situational awareness into communication, but the cyber threat information is encoded only through one input channel (e.g., via the visual system through what the eyes can read from a screen), then it could be that the process from encoding to communication will be more efficient if two input channels for encoding can be utilized instead of one (Debashi & Vickers, 2018; Iggena et al., 2023). In this sense, applying neuroscience to human cybersecurity performance implies having a first principles approach to user-centric design and performance optimization. Of specific interest is how the human nervous system processes information in the environment to produce appropriate responses. This includes what permits processing, what impedes, biases, or prevents it, and ways to enhance or improve information processing. As the study of the human brain in relation to performance at work and everyday settings is the definition of neuroergonomics (Parasuraman, 2003), the adoption of neuroergonomic approaches for the current Ph.D. work assumes that a more fundamental approach is necessary due to:

- The type, rate, and amount of information that humans need to process and communicate in cyber threat situations, which leave small margins separating human-environment compatibility from incompatibility (Champion et al., 2012), and
- these margins being accompanied by failure-intolerance, especially in cases where failures have an impact on critical infrastructure and national security.

While building on previous work and addressing its shortcomings, the work included in this thesis also addresses specific gaps identified in other work previously conducted within the field of human communication in cyber threat situations. These gaps have informed the formulation of the research questions that has guided the subsequent work. The next subsection addresses these gaps and research questions.

1.5. Identified Gaps and Research Questions

Throughout the entire process of the thesis work, several gaps in the existing and own research were identified. The systematic review carried out at the start of this research journey identified a general absence of neuroscientific research on cognitive processes underlying human-to-human communication and human performance in cyber threat situations. This prompted an effort towards developing a neuroscientific understanding of human-machine interactions with regards to how humans can flexibly transition from processing technical data related to cyberspace and communicating that information to team members. This effort included a motivation towards identifying neuroscientific performance metrics and interventions to validate the frameworks, theories, assumptions, and observations relating cognitive processes to communication and situational awareness that have been proposed in previous work (e.g., Champion et al., 2012; Jøsok et al., 2016, 2019; Knox et al., 2017, 2018). There were little studies on how to use novel technological tools to predict and improve operational outcomes related to processing information and communicating in complex cyber threat information environments. Consequently, there was a decision to apply sensor technology to measure neurophysiological activity in cyber analysts in naturalistic settings, with practical implications related to the use of wearable technologies in cyber operative contexts. Extended reality technology was applied to improve information processing in cyber threat situations with practical implications for operational communication in naturalistic settings such as CDXs. There was also a lack of studies that operationalized specific communication behaviours in a way that allowed for more quantifiable measurements of human-to-human communication. Few studies simultaneously assessed team-level and individual-level metrics of performance, including a lack of studies on the development of mental models to improve communication of cyber threat information in teams. Considering these gaps, the following research questions were addressed in this thesis work:

1. How do neurocognitive factors such as cognitive control for goal-directed coordination of cognitive processes, mood-related biases, and multi-sensory integration influence the

processing and communication of cyber threat information in cyber threat situations, and

2. Can knowledge about these neurocognitive factors be leveraged to create neuroergonomic approaches for improving human-to-human communication of cyber threat information and decision-making?

The first research question concerns neuroergonomic knowledge generation while the second question concerns neuroergonomic intervention. The research questions were formalized as a series of objectives (Table 2) that were subsequently addressed in 1) the papers included in this thesis, 2) the thesis itself, and 3) ongoing work.

#	Description of objectives
1	Systematically review the literature on human-to-human communication in cyber threat situations to identify how communication has been studied, if they include neuroscientific approaches, and the methodical limitations and unanswered questions in existing cyber threat communication research to inform improvements for novel research designs.
2	Review neuroscience literature relevant to cybersecurity performance (studies detailing how individuals can optimize specific neurochemical activity in specific neural circuits related to e.g. prolonged attention and effective encoding of information during heavy cognitive load; studies detailing the activity in neural circuitry related to specific cognitive functions important for e.g. anomaly detection during processing of complex stimuli) to suggest neuroergonomic approaches (e.g. tests and indicators for cognition, perception, or mental model formation that better matches the cognitive and perceptive demands of cybersecurity personnel) and innovations (e.g. sensory augmentation technology that does not interfere with important attentional resources) to study and optimize threat perception and communication in cyber threat situations.
3	Compare electrophysiological measures, neurocognitive tests, and self-report measures assessing neurocognitive processes, with measures of situational awareness and self-reported team and communication measures during CDXs or other studies investigating detection of cyber threats, to characterize the neurocognitive factors that influence the efficient establishment and communication of situational awareness in simulated cyber threat situations.
4	Conduct neuroergonomically informed experiments assessing the effect of interventions that a) optimize neurocognitive processes for cyber threat information processing, or b) utilize alternative neurocognitive processes for cyber threat information processing c) on team communication, cyber situational awareness, and decision-making.
5	Use findings from the Ph.D. research and the neuroscience and cybersecurity literature to develop neuroergonomic performance metrics and interventions for human-to-human communication in cyber threat situations. These performance metrics and interventions will be validated for expert-expert communication as well as for expert-layperson communication and across organizational hierarchies.

Table 2. Research objectives

The first objective was addressed by conducting a systematic review (Chapter 5.1) of previously conducted research on human-to-human communication in cyber threat situations. The second objective has been addressed in the introduction sections of the studies included as part of the thesis work and in the reviews included Chapter 2 and Chapter 3, and in ongoing work. The third objective was addressed in the second study, which is reported on in Chapter 5.2. The fourth objective was addressed in paper III in Chapter 5.3. The fifth objective was in part addressed in this thesis and is currently being addressed in ongoing work.

1.6. Synopsis of the research

The research journey began by addressing the first objective which entailed conducting a systematic review (Chapter 5.1) of previously conducted research on human-to-human communication in cyber threat situations. The following research questions guided the literature review:

1. How has human-to-human communication in cyber threat situations been studied in the literature?
2. What are the areas where there is potential for developing common standards for information exchange in collaborative settings?
3. What guidance can be provided for future research efforts?

The systematic review led to the identification of critical gaps in the existing literature on cyber threat communication, which helped in the selection of areas to focus the subsequent research. In other words, the review served as the basis for the rest of the thesis work. As mentioned previously, the specific gaps identified in the review were that there were no neuroscientific studies on human-to-human communication in cybersecurity. There was a lack of studies that simultaneously assessed team-level and individual-level measurements of performance. There was a need for operationalization of specific communication behaviors in a way that allowed for quantifiable measurements to study their impact on performance. There was also a need for more studies on the development of shared mental models for communication in cyber threat situations and their possible impact on sharing of cyber threat information.

The lack of neuroscientific research identified in the systematic review highlighted a necessity to explore neurophysiological factors affecting how teams navigate cyber operative information environments and communicate in cyber threat situations. Previous research had suggested that metacognitive processes were involved in cyber threat detection (Sütterlin et al., 2022) and situational awareness (Endsley, 2020), and in the cognitive navigation of the hybrid working-environments associated with cybersecurity (Jøsok et al., 2016, 2019) and subsequently, human-to-human communication. A previous study (Ask et al., 2021) conducted by my colleagues and I also suggested that daily affective variability, used as indicator of emotion regulation (greater variability interpreted as more regulation), was negatively associated with teamwork demands among cyber cadets during a CDX. An important note about this latter study was that the direction of regulation (e.g., if moods went from positive to neutral or negative, or from negative to neutral or positive) was not indicated, just the variability. Surveying the neuroscientific literature suggested that metacognitive processes and the regulation of mood are partly influenced by common brain areas (Boldt & Gilbert, 2022; Fleur et al., 2021; Golkar et al., 2012) and that vagally mediated heart rate variability (or vagal tone), is a potential downstream proxy for activity in these brain areas (Meessen et al., 2018; Schmaußer et al., 2022). Since vagally mediated heart rate variability can be measured noninvasively by the use of wearable sensor technology, it has the potential of being a performance indicator that is relevant for metacognitive influences on communication and situational awareness that could also be used to validate the previous research by (Jøsok et al., 2016, 2019; Knox et al., 2017, 2018) with neuroergonomic data. Together, the systematic review, previous research on cyber operators and situational awareness, and surveying the neuroscientific literature, guided the focus of subsequent empirical research on cognitive and emotional influences on communication and cyber situational awareness. The second study compared electrophysiological measures (vagal tone), and self-report measures assessing affective states and metacognitive prospective judgments of performance, with situational awareness and self-reported team and communication measures during a Cyber Engineering Exercise. The following research question was addressed by the study:

- How do individual differences in dorsolateral prefrontal cortex activity, indicated by vagal tone, influence metacognitive accuracy of cyber situational awareness, communication demands, and mood processing in cyber threat situations?

The study findings suggested that cyber cadets with high vagal tone exhibited better metacognitive accuracy with respect to situational awareness and reported lower communication demands. Cyber cadets with high vagal tone also reported lower (more neutral) moods compared to individuals with low vagal tone, which in turn predicted better metacognition and situational awareness. Interestingly, this latter finding resulted in the questioning of my previously held assumptions, prompting the reinterpretation of findings in research I had conducted (Ask et al., 2021) and read (Lugo et al., 2016) previously. In the world of health research (e.g., clinical neuroscience) that is part of my background, emotional states are often interpreted in terms of negative moods being bad, neutral moods being better, and positive moods being best. A tendency towards negative moods is considered an indicator of dysregulated emotion and reduced adaptive ability. This view of emotion regulation is likely a legacy problem, as a lot of the research on emotion regulation is conducted in a clinical (or pre-clinical) setting, where negative or shifting moods are equivalent with anxiety, depression, and emotional instability. This associate negative moods with pathology, while positive moods are considered diametrically opposite of pathology. While remaining methodically agnostic about the direction of the association between vagal tone and mood in the second study, my personal expectations were that there would be a positive association between vagal tone and mood, that a negative mood would mean having a negativity bias and processing information in congruence with a negative mood, which would mean poor attentional control and lead to worse metacognition and situational awareness. When the opposite was true, it prompted the recollection of older studies on mood congruent processing and investing, where depressed individuals tended to perform better than neutral, angry, or anxious individuals.

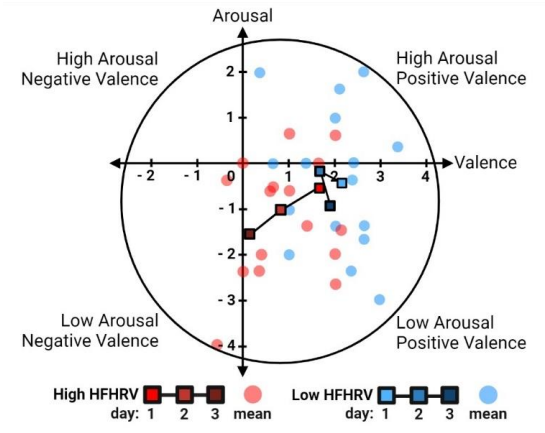

Figure 1. Valence-Arousal plot from study II

HFHRV = High frequency heart rate variability (Taken from Ask et al., 2023; Chapter 5.2).

Plotting the daily affect in a valence (mood)-arousal plot (Figure 1) indicated that moods were about the same on day one for both vagal tone groups, but that individuals with high vagal tone regulated their moods more and more towards neutral for each day while individuals with low vagal tone remained in a positive mood. This finding has added new weight to the notion that it is the situation and the related problems that dictates what is appropriate and adaptive with respect to emotion regulation, not the emotion (or the way it is regulated). It also added more weight to what cognitive flexibility may mean, especially with respect to being cognitively agile in dynamic environments. This has influenced how I approach current and future research related to mood and emotion, especially in the context of goal-directed information processing in complex environments. However, the impact of communication and situational awareness on decision-making was not assessed in the study, which leaves questions about their significance on performance (an issue raised in previous research; Gutzwiller et al., 2020). The need to assess these relationships was addressed in a subsequent third study.

In the third and final empirical study, efforts were made to continue the implementation of findings from the systematic review regarding 1) the need for more research on shared mental models and its impact on cyber team communication, 2) the need for operationalization and measuring of specific communication behaviors to assess their impact on SA, and 3) the simultaneous inclusion of team-level and individual-level measurements. Considering the suggested relationships between information load, communication breakdown, and situational awareness (Champion et al., 2012), the neuroscientific literature was surveyed to identify ways of processing information that could be relevant for cyber operators, specifically to identify alternative ways for humans to process large amounts of complex data without relying solely on the visual system. The relevance would be to reduce the load associated with allocating cognitive resources to information processing in order to make dyadic team communication more efficient. Having been educated at an institute that specializes in the neuroscience of spatial information processing and path integration, attempting to utilize spatial sensory processing as a complement to visual processing seemed attractive, since the spatial navigation systems utilizes information processing pathways that efficiently encode information to memory (Dresler et al., 2017; McCabe, 2015). My supervisors suggested a collaboration with Dr. Kaur Kullman, a researcher at the University of Maryland who had developed a platform for visualizing network data using extended reality (XR) technology (Kullman et al., 2018).

An experiment was designed to compare the effects between visualizations of network topology and activity using 2-Dimensional (2D) graph representations and 3-Dimensional (3D) visualizations in mixed reality (MR). The following research question was addressed by the paper:

- Is a 3D mixed reality representation of a network attack better than a 2D representation for achieving cyber situational awareness, cyber team communication, and decision-making among cooperating dyads during a simulated cyber threat situation?

Cyber cadets at NDCA were recruited as participants that were paired in dyads and asked to collaborate to identify suspicious network traffic during a simulated network attack. Structured observation was conducted to note specific communication behaviors identified as relevant in the systematic review in paper I (Chapter 5.1). The structured observation method assessed the frequency of occurrence for four verbal communication behaviors: (1) OLB behaviors, (2) perceptual shared mental modeling, (3) task resolution, and (4) communication dysfunction. What was identified as OLB behaviors and why they were important was based on the OLB model proposed by Knox and colleagues (2018) and is thought to reflect metacognition and perspective taking. Perceptual shared mental modeling consists of verbal communication related to achieving a shared visual and spatial perception of task relevant information but was mainly assessed through communication behaviors facilitating joint attention. Task resolution communication was identified as important based on observations from a qualitative study (Jariwala et al., 2012). Communication dysfunction behaviors identified as important were based on reports from (Champion et al., 2012; Henshel et al., 2016; Jariwala et al., 2012). One of the dysfunctional behaviors was prolonged silence (considered an indication of communication breakdown; Champion et al., 2012; Jariwala et al., 2012). Other measures of communication were perceived communication demand and written situational reports.

The findings suggested that dyads using 3D MR visualizations had better self-reported and observed communication and slightly improved cyber situational awareness compared to those using 2D visualizations. On a neurocognitive level, this could mean that the visualization of network topology and activity reduced the cognitive load on dyads when relating communication to their mental models of the situation. This could be due to part of the mental model being outsourced to the 3D visualization and identical between communicating dyads.

It could also mean that they were able to encode information about the network through the spatial sensory system by walking around in the visualization (Payer & Trossbach, 2015). However, decision-making improvements were not significantly different between the group using 3D visualization compared to the group using 2D visualizations. With respect to moving towards operationalizing and measuring specific communication behaviors, this step had a special significance with regards to how my view of communication in cyber threat situations has changed during the course of the thesis project. Another assumption I held previously with respect to communicating situational information was that "more is more" (provided that there is time to process the information). More sharing of, for example, situational information means better situational awareness, and more communication regarding team tasks means better coordination and a faster overview of a given situation or problem. Aside from being a central idea in the network-enabled operations framework (Alberts & Garstka, 2004), this assumption was held because previous research suggested that information (thus cognitive) overload leads to communication breakdown and subsequently poor situational awareness (Champion et al., 2012), and that communication demands was associated more cognitive movements in the hybrid space, interpreted as more cognitive agility (Lugo et al., 2017), and teams that communicated more during a cyber capture the flag competition performed better than teams who communicated less (Jariwala et al., 2012). What is important to note here is that most of this data is based on novices, not experts. My assumption that "more communication is more" was challenged by findings reported by Buchler and colleagues (2016, 2018), especially in the (Buchler et al., 2016) study, where individuals who had the best situational awareness had fewer outgoing communications than individuals who had poorer situational awareness. In their paper, Buchler and colleagues (2016) suggested that individuals with higher expertise may need to communicate less than those with lower expertise. This was discussed briefly with respect to communication demands in study two. In study three, however, while not addressed explicitly, the correlation analysis showed that communication regarding task resolution was positively associated with communication demand, and both were negative predictors of correctly identifying red team hosts targeting blue team systems, supporting the interpretation by Buchler and colleagues (2016) that there may be a negative link between communication frequency and proficiency. The lack of significant relationships between the 3D and 2D condition with respect to decision-making may indicate that a different approach to measuring it should be considered in future research.

Table 3 presents the flow of research in this thesis, including main findings and limitations, how initial studies influenced subsequent research, and main contributions.

Title of thesis	Neuroergonomic Approaches to Understanding and Improving Communication of Recognized Cyber Threat Situations
Problem	Inadequate communication between humans during cyber threat situations can result in the loss of critical information which negatively impacts situational understanding and cyber defense decision-making.
Research questions	1. How do neurocognitive factors such as cognitive control for goal-directed coordination of cognitive processes, mood-related biases, and multi-sensory integration influence the processing and communication of cyber threat information in cyber threat situations? 2. Can knowledge about these neurocognitive factors be leveraged to create neuroergonomic approaches for improving human-to-human communication of cyber threat information and decision-making?
Paper I title	Human-human communication in cyber threat situations: a systematic review
Paper I research questions	• How has human-to-human communication in cyber threat situations been studied in literature? • What are the areas where there is potential for developing common standards for information exchange in collaborative settings? • What guidance can be provided for future research efforts?
Key findings	Few studies on human-to-human communication in cyber threat situations. No studies use neuroscientific methods. Few studies include both individual-level and team-level measurements. There is a need for more research on shared mental models and its relationship with communication, and to describe and measure specific communication behaviors.
Implications for subsequent research	The neuroscientific literature was surveyed to identify neurophysiological processes that would be relevant for the processing of information in complex information environments and for communicating in dynamic environments. This survey was used to identify a non-invasive predictor variable for performance (Paper II) and a possible intervention to facilitate shared mental modelling and ease information processing to improve operational communication and decision-making (Paper III). Individual-level and team-level measurements were included in Paper II and Paper III studies. Relevant communication behaviours identified in Paper I were operationalized for structured observation in Paper III to measure the impact of intervention.
Paper II title	Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise
Paper II research questions	How do individual differences in dorsolateral prefrontal cortex activity, indicated by vagal tone, influence metacognitive accuracy of cyber situational awareness, communication demands, and mood processing in cyber threat situations?
Key findings	Cyber cadets with high vagal tone had better metacognitive accuracy, reported less communication demands, and had significantly more negative moods than individuals with low vagal tone. More positive moods were related to poorer SA and metacognitive accuracy. Demonstrates the feasibility of using such methods during a CDX and neurological explanations for performance-related behavioral observations.

Limitations	Small sample size. Sample consisted of novices. Somewhat ambiguous findings with respect to communication demands. Uncertain what consequences findings have for decision-making
Implications for subsequent research	The inability to identify and study a relationship between communication demand and SA, to relate findings to a network topology, and the impact of communication and SA on decision-making, informed the design of the decision-making task and the topology selection task in Paper III.
Paper III title	A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness
Paper III research questions	Is a 3D mixed reality representation of a network attack better than a 2D representation for achieving cyber situational awareness, cyber team communication, and decision-making among cooperating dyads during a simulated cyber threat situation?
Key findings	Dyads using a 3D mixed reality visualization of a network attack had better self-reported and observed communication, and slightly better cyber situational awareness than dyads using a 2D visualization of the same network attack. Decision-making was not significantly different between the groups.
Limitations	Small sample size. Sample consisted of novices thus it is hard to determine what they would mean in an expert setting. The experimental task was not realistic thus the experiment must be repeated in a naturalistic setting with larger sample size.
Main contributions	Novel and neurobiological perspective on human factors in cybersecurity that supports and extends the theoretical frameworks and observations reported in previous work, both for performance in general and for communication specifically. Demonstrated the feasibility and relevance of including non-invasive neurophysiological measurements in CDXs to predict performance-related outcomes including communication demands in cyber teams. Findings can be implemented by using wearable sensor technology. Highlighted the need for increased involvement of stakeholders in cybersecurity research, and increased collaboration between CDX organizers and researchers to improve the quality and impact of research. Demonstrated the potential efficacy of employing user-centric and neuroergonomic technological tools to improve information processing and operational communication in cybersecurity settings. The current maturity of the technology makes it deployable in educational/training settings such as CDXs. This is the next step to validate its efficacy and the main limitations are the willingness and capacity for stakeholders to implement it.
Notes. 3D = 3-Dimensional. CDX = Cyber defense exercise.	

Table 3. Flow of research in thesis.

The following section outlines the main contributions of the research.

1.7. Contributions

The main research questions addressed by this thesis constitute two goals; one being to understand the neurobiological mechanisms underlying human communication and performance in a cybersecurity setting, and the other being to use that understanding to develop interventions that can improve communication and performance. As these goals are related to

solving a specific problem for a specific group of people, the nature of the research is applied, and the contributions should be considered to the extent they offer actionable solutions to this problem in both general and specific terms. As such, the work included in this thesis offers a number of important and novel contributions to the field of human factors in cybersecurity, especially as it pertains to human-to-human communication. Although two decades have passed since the conception of neuroergonomics as an interdisciplinary field of research with explicitly stated goals (Parasuraman, 2003), the comprehensive approach to converging and interdisciplinary research methods, offers a novel perspective on human performance in cybersecurity in general, and the impact of cognitive information processing on cyber team communication specifically.

On a specific level, the thesis work has demonstrated the feasibility of implementing neurophysiological indicators of performance to assess metacognitive abilities in CDXs, suggesting a possible use case for wearable technology in the training of cyber operators. Utilizing wearable technology to measure vagal tone may provide insight into information processing tendencies related to mood and metacognition that also has implications for situational awareness and cyber team communication. The thesis has shown how vagal tone may be used as an indicator that can be measured outside of exercises, that can guide which individuals to monitor in case they need intervention (e.g., mentoring or group-related input) during CDXs with respect to adjusting mood-related information processing that may have consequences for situational awareness and communication. To my knowledge, this is the first study utilizing sensory technology to assess vagal tone in cyber operators during a CDX.

Another notable and practical, thus actionable contribution in the context of conducting applied research to solving human-to-human communication problems in cyber threat situations, is the use of XR as an intervention to improve cyber threat information processing and operational communication. The specific intervention and how it is implemented in terms of its visualization of network topology and activity is based on the mental models of expert cyber operators, making it intuitive to navigate in a user-centric manner, and on neuroscientific principles of multi-sensory perceptual encoding (Bohbot et al., 2017; Iggena et al., 2023), making it neuroergonomic to navigate in an information processing manner. While there were technical challenges with respect to the practical useability of the technology (e.g., battery power life) at the time when the experiments were conducted, the current maturity of the technology (e.g., Apple Vision Pro; Apple Inc., 2024) makes it applicable in training settings

such as CDXs. The main challenge to doing this successfully is the willingness and capacity (e.g., availability of physical space to allow for spatial encoding and group interactions) for stakeholders to allow for optimal implementation. Using the XR technology in CDXs in combination with traditional security information and event management displays while cyber teams are engaged in more naturalistic tasks is the next step in validating its effect on cyber team communication and subsequent decision-making.

On a more general note, this thesis provided an overview of specific communication behaviors that have been reported as relevant in a cybersecurity context, as well as demonstrating how they can be observed and measured in research settings and how they relate to performance in a quantifiable manner. While these efforts only represent a step towards standardized operationalization, the findings in the present work are something that can be used to measure the effectiveness of future interventions. These communication behaviors are also something that mentors and observers at CDXs can use to gauge communication dynamics in teams, use the frequency (or relative occurrence) of such behaviors to infer the workload demands that the teams are experiencing, and infer possible underlying causes. For instance, in our XR experiment, self-reported communication demand was positively associated with observed task resolution communication behaviors, and both were negative predictors of identifying red team hosts targeting blue team systems. While these relationships are confounded by experimental manipulation, on an intervention level, these behaviors may be used to infer how task-load influences what information is prioritized during operational communication. On a skills-to-expertise level, it supports the findings in (Buchler et al., 2016), that certain types of communication may occur less frequently in individuals who are further up the ladder to becoming experts, and that it is related to better situational awareness. Thus, observing the relative need of cyber cadets to discuss how to solve specific tasks may be indicative of their progress, need for focused attention (e.g., need for more technical training), and potentially how their communication behaviors can influence group dynamics in ways that reduce situational awareness. As the individuals that have participated in the studies included in this work are future cybersecurity experts on the level of national security, the discussed contributions are of relevance to the national security context generally, and the Norwegian context specifically.

Another general contribution of the thesis work has been identifying plausible neurobiological mechanisms influencing the flexible navigation of complex information in

working-environments that include human-to-human and human-computer interactions. These mechanisms are related to previous work on cognitive agility, metacognition, and situational awareness, which are theoretical concepts related to human performance in general and to operational communication. In other words, this thesis effectively extends the realm of how previous work can be used to understand performance, as well as the questions that can be asked and answered with respect to communication. Thus, when considered in its entirety, the thesis work offers a neuroergonomic framework to understand and identify human performance gaps. This broadens the scope of hypotheses and interventions that can be generated and tested to address identified performance gaps. This is especially important when understanding counterintuitive observations, which is exemplified in how the thesis explains why persistent positive moods may lead to worse situational awareness and thus performance outcomes in situations requiring analytical processing.

In parallel with highlighting the feasibility and usefulness of neurophysiological measurements and neuro-centric interventions in CDX's, the thesis also offers a very critical discussion of the limitations of the work. This discussion can and should be extended to other human factors research conducted previously and in the future. In practical terms, the critical discussion highlights the need for stakeholders such as CDX organizers to allow for more involved collaboration with human factors researchers to ensure high-quality research. There is a saying in science that goes along the lines of "there are no bad results, only bad methods". When the stakes are as high as they are in a security setting, stakeholders should be motivated to make sure that researchers are able to uphold the highest methodological standards that are feasible within the given research context. The responsibility for communicating this point falls on the shoulders of the researchers. This thesis goes some way in communicating this point by providing the rationale (and associated consequences) that can be used when communicating with stakeholders.

It is important to note that the research conducted in this thesis work is on novices, not experts, and that the implications of findings on decision-making, and cyber analyst-to-decision-maker communication is still unaddressed.

1.8. Scientific Papers in Order of Appearance

Three papers form the basis of this dissertation. The following is an overview of their titles, name of co-authors, and the journal it was published in.

I. Ask, T. F., Lugo, R. G., Knox, B. J., & Sütterlin, S. (2021). Human-Human Communication in Cyber Threat Situations: A Systematic Review. In Stephanidis, C., et al. HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning, and Culture. HCII 2021 (pp. 21-43). *Lecture Notes in Computer Science, 13096*. Springer, Cham.

II. Ask, T. F., Knox, B. J., Lugo, R. G., Helgetun, I., & Sütterlin, S. (2023). Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. *Frontiers in Human Neuroscience, 16*, 1092056.

III. Ask, T. F., Kullman, K., Sütterlin, S., Knox, B. J., Engel, D., & Lugo, R. G. (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *Frontiers in Big Data, 6*, 1042783.

1.9. Overview of Chapters

This thesis has eight chapters. Chapter 1 is the introductory chapter that contextualizes the work and summarizes the significance of contributions resulting from the thesis work. As such, it starts by providing a brief overview of the context that the research was conducted in, the previous work it was based on, identified gaps and the research questions that were formulated to address them, the research journey and the related results, and the main contributions of the thesis work.

Chapter 2 introduces the background information needed to understand the work presented in the thesis. It focuses on describing the challenges of the information environment that cyber teams face. Thus, the chapter defines what cyberspace is, cyber threat situations and security operation centers, sociotechnical systems, challenges to team performance in cyber operations, situation awareness, human-to-human communication in cyber threat situations, the use of visualization aids for team mental models, metacognition, cognitive agility, cognitive control, and neuroergonomics.

Chapter 3 provides a review of the state-of-the-art of existing human-to-human communication research related to the work presented in this thesis. This includes the measurement of relevant constructs and how state-of-the-art knowledge has influenced methodological considerations in the thesis.

Chapter 4 outlines the methodologies that were applied to address the identified research questions.

Chapter 5 contains the scientific papers that are included as part of the dissertation. Chapter 5.1 is a systematic review of papers that have studied human-to-human communication in cyber threat situations. The review provides an overview of how communication in cyber threat situations has been studied, including a synthesis of the findings, shortcomings, and avenues for future research. Some of the key findings included that there was a general lack of studies applying neuroscientific methods, as well as identifying the need for more research on shared mental models and more research that included both individual-level and team-level measurements. These findings influenced the research reported in Chapter 5.2 and 5.3. Chapter 5.2 is a correlational study that looked at the relationship between a neurophysiological indicator, affect, metacognition, cyber situational awareness, metacognition, and self-reported team communication and coordination among cyber cadets participating in the cyber operations track of a cyber engineering exercise organized by the Norwegian Defense Cyber Academy. Chapter 5.3 is an experiment employing a head-to-head design (i.e., it compares the proposed intervention against a more well-established, powerful alternative) that compares the effect of a 3D and 2D representations of network topology and traffic on dyadic communication, cyber situational awareness, and decision-making. The sample consisted of cyber cadets from the Norwegian Defense Cyber Academy.

Chapter 6 contains a critical general discussion of the findings reported in the papers included in the dissertation and of some of the assumptions that the research is based on. This critical discussion can be extended to other human factors studies. The purpose of this critical discussion is to highlight the shortcomings of the research, not to downplay the significance of the findings, but to stress the need for more involvement of stakeholders in research and to allow researchers more involvement in the planning of CDXs, The main challenge to ensuring high-quality human factors research in cybersecurity is gaining access to relevant participants and to be involved in the planning stages in ways that ensure high quality measurements. The main topics of discussion concern issues related to the main contributions of the study, as well as concepts such as situational awareness in cybersecurity and its hypothesized relationship with communication and decision-making. Issues related to sample sizes in the included studies are also addressed along with a need for validation of constructs, instruments, and suggestions

for study designs to replicate and validate the findings. Some basic but unanswered questions are also highlighted.

Chapter 7 summarizes the contributions of the thesis work with respect to the specific problem it has set out to solve and with respect to the larger context of human factors research in cybersecurity. Chapter 8 concludes with the final take-home messages of the dissertation.

Chapter 2

2 Background

This chapter provides the background information needed to understand the work presented in this thesis. Definitions of cyberspace, cyber threat situations, and security operation centers are initially explained to provide a general understanding of what is meant by certain terms related to cyber environments. Human factors in cybersecurity are explained to provide a brief overview of why the field of human factors research exists to anchor the subsequent work presented in the thesis. Socio-technical systems theory is explained to provide an overview of one way in which researchers approach the interconnectedness between humans and technical environments. This will be followed by narrowing the focus on the cyber work-domain to provide some practical context related to the challenges complex information environments pose on cyber teams and how they navigate these challenges. This grounding in the cyber work-domain directly addresses the scope of the research presented in this thesis, as it mainly concerns the relationship between the downstream effects that navigating complex information environments have on communication. The use of visualization aids for establishing team mental models is briefly explained to relate the tools cyber teams use to understand the information environment to the specific interventions employed as part of the thesis research. The concepts of metacognition, cognitive agility, and cognitive control are explained to provide an overview of how an individual's awareness of their own cognitive processes has been related to the control of cognition and behavior, theoretically, which is related to the inherent abilities of cyber team members to navigate complex information environments. In other words, they constitute cognitive processes that may be related to relevant performance indicators.

2.1. Cyberspace, Cyber Threat Situations, and Security Operation Centers

Through the digitization of society and increased network coverage, "cyberspace" has emerged as an action space that has presented novel opportunities for communication, collaboration, and innovation across organizational and societal sectors. For example, in military contexts, cyberspace is considered a fifth domain alongside the four domains of land, sea, air, and outer space that humans can operate within through the aid of science and technology (Kuehl, 2009). Cyberspace has been defined as:

> "a *global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies*" (Kuehl, 2009, pp. 4).

Thus, cyberspace encompasses the communication that occurs between computing devices and networks, the content of communication, and the devices themselves. Cyberspace also includes the interconnection between machines, networks, and the physical world (cyber-physical systems; Gutzwiller et al., 2015). The emergence of cyberspace as an action space has presented new challenges for security. The proliferation of connected devices and the vast amount of data being generated and transmitted make it easier for (cyber-)criminals and state actors to exploit vulnerabilities in digital infrastructure and to launch attacks. As technology and digitization advances, so do the tactics and capabilities of cybercriminals (Monteith et al., 2021). Dealing with this evolving cyber threat landscape is the objective of cybersecurity. The specifics of what cybersecurity entails may vary depending on the sector and organization in question. In the broadest sense, cybersecurity refers to the protection of cyber assets from unauthorized access, theft, or damage. A cyber asset can be understood as a completely or partly digitized protected organizational resource, including (but not limited to), websites, data, information, tangible objects such as computers, computer systems and software, and other digital infrastructure (Whitman & Mattord, 2012). As such, cybersecurity can be used interchangeably with "information security" and entails the implementation of measures to safeguard cyber assets from cyber threats and attacks (Whitman & Mattord, 2012).

Security is considered to have three main goals (or pillars; Lundgren & Möller, 2019): confidentiality, meaning that only entities who are authorized should have access to the protected asset; integrity, meaning that structural aspects of the asset should be intact (e.g., information should be correct and not altered by unauthorized entities), and; availability, meaning that the asset should be accessible, available, and usable by authorized entities only. These three properties make up the pillars of the confidentiality, integrity, and availability (CIA) triad, and an asset is only considered secure if it retains these three properties (Lundgren & Möller, 2019). A cyberattack can be any passive, active, direct, indirect, intentional, or unintentional act that damages or compromises the CIA of information and the systems that support it (Whitman & Mattord, 2012). An intentional attack can for example be when a hacker

attempts to break into an information system such as a network and consists of a series of deliberate steps:

> "*The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment.*" (Hutchins et al., 2010, pp. 4).

A direct attack can for example entail using a personal computer to break into a computer network while an indirect attack can be when a system is compromised for the purpose of attacking another system (e.g., as a subunit in a botnet; Whitman & Mattord, 2012). The difference being that a direct attack originates from the threat itself. As cybercriminals develop new ways of targeting and exploiting security vulnerabilities, the rate (Clarke & Martin, 2024; Monteith et al., 2021) and global cost of cybercrime continues to grow and is estimated to exceed $10 trillion by 2025 (Morgan, 2020; Petrosyan, 2023). The growing cost of cybercrimes, combined with the growing interconnectedness and interdependence of non-critical and critical digital infrastructures, is putting an increasing pressure on organizations and governments to invest in measures that keep them resilient against cyber threats (Iftikhar, 2024). "Cyber resilience" includes an organization's ability to protect cyber assets against cyberattacks but also its ability to swiftly resume and maintain business operations after having suffered a successful attack, albeit without harmful effects (Sharkov, 2016). It is thus an organizational state that entails having a holistic and comprehensive response to cyber threats, where individuals at all levels of management need to properly understand the threat landscape. Only this holistic and comprehensive approach will fully ensure the effective implementation of procedures for limiting or absorbing the impact of cyber threat situations (Sharkov, 2016).

A cyber threat is any event or circumstance with the potential of have a harmful impact on a state or an organization, their operations, assets, or individuals, by either modifying, disclosing, or destroying information, through service unavailability, or via authorized access to information systems (Joint Task Force Transformation Initiative, 2012; Tinde, 2022). The potential for harmful effects is what distinguishes cyber threats from attacks (and smaller cyber incidents), which in the case of attacks already have taken place thus entailing less situational ambiguity than cyber threats do (Tinde, 2022). A cyber threat situation is a combination of events or circumstances indicating to an organization that they are being exposed to one or

more cyber threats that may disrupt, control, cause damage to, or steal (e.g., exfiltrate) a cyber asset. Cyber threat situations may vary in complexity depending on the sophistication of the cyber threat actor (Hutchins et al., 2010), which may vary from nation-state actors and cybercriminals with geopolitical or profit motives, respectively, all the way down to thrill-seekers and (unintentional) insider threats driven by self-gratification or lack of awareness (Canham et al., 2020; Canadian Centre for Cyber Security, 2021).

Organizations source their cyber operations to security operations centers (SOCs). SOCs are centralized locations inside or outside an organization, consisting of organizational units or teams of cybersecurity experts and technology working around the clock to prevent, detect, report on, and defend against cyber threats (Agyepong et al., 2019). They do this by collecting and analyzing cyber threat information (also encompassing cyber threat data and cyber threat intelligence in this thesis), which is any information that can assist an organization in identifying, understanding, and mitigating cyber threat situations (Johnson et al., 2016). In essence, SOCs provide organizations with an overview of cyber threat situations while assisting them with threat management and compliance issues (Schinagl et al., 2015). Twelve typical cybersecurity roles as identified by the European Union Agency for Cybersecurity (ENISA; European Union Agency for Cybersecurity, ENISA, 2022) can be found in Table 4.

Role	Responsibility
Chief Information Security Officer (CISO)	Manages an organization's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Cyber Incident Responder / SOC analyst	Monitor the organization's cybersecurity state, handle incidents during cyberattacks and assure the continued operations of information and communication technology (ICT) systems.
Cyber Legal, Policy & Compliance Officer	Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organization's strategy and legal requirements.
Cyber Threat Intelligence Specialist	Collect, process, analyze data and information to produce actionable intelligence reports and disseminate them to target stakeholders.
Cybersecurity Architect	Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.

Cybersecurity Auditor	Perform cybersecurity audits on the organization's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.
Cybersecurity Educator	Improves cybersecurity knowledge, skills and competencies of humans.
Cybersecurity Implementer	Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.
Cybersecurity Researcher	Research the cybersecurity domain and incorporate results in cybersecurity solutions.
Cybersecurity Risk Manager	Manage the organization's cybersecurity-related risks aligned to the organization's strategy. Develop, maintain and communicate the risk management processes and reports.
Digital Forensics Investigator	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.
Penetration Tester	Assess the effectiveness of security controls, reveals and utilize cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.
Notes. Taken from European Union Agency for Cybersecurity, ENISA (2022).	

Table 4. Twelve typical cybersecurity roles identified by ENISA.

Traditional SOCs are organized in an executive hierarchy where decision-making and analytical tasks are separated and distributed among different staff (Staheli et al., 2016). How to act on threat and incident reports are assigned to decision-making staff (decision-makers). Analytical tasks such as asset monitoring, threat detection, forensics, network security, intelligence, and communicating suggestions for cyber threat- and cyber incident response are assigned technical staff (cyber analysts or cyber operators) at the bottom of the executive hierarchy. The typical SOC organizational structure is therefore one where information is pushed up and decisions are being pushed down in the decision-making hierarchy (Staheli et al., 2016). Consequently, information goes from being raw and unfiltered at the level of the analyst, to more synthesized, high-level analyses at higher levels in the decision-making hierarchy (Staheli et al., 2016). This means that the process of detecting and acting on cyber threat information is an involved process that potentially includes several humans, thus, it is vulnerable to human error (Jøsok et al., 2017). As noted by Veksler and colleagues (2020), cyber analysts working with intrusion detection tend to have long working hours (typically 12-hour shifts), and errors are more likely to occur during hand-offs at the end of shifts. This

tendency is an established phenomenon known for example from studies on shiftwork in nurses and its effect on handoffs and burnout rates (Friesen et al., 2008; Stimpfel et al., 2012). Furthermore, the role of a cybersecurity analyst is diverse, encompassing a variety of essential responsibilities for safeguarding computer systems and networks (see Table 4; European Union Agency for Cybersecurity, ENISA, 2022). SOCs need people with a mix of technical skills, analytical skills, and the ability to work with others to protect information systems from cyber dangers which includes:

Security breach prevention: Cybersecurity analysts have a crucial responsibility in safeguarding an organization's information systems against cybersecurity threats and attacks. They are tasked with the duty of overseeing networks, detecting weaknesses, and executing measures to avert security breaches (Patel, 2014).

Security Threat Analysis and Response: These experts are accountable for examining security breaches and taking action in response to occurrences. They employ several tools and methodologies to identify, examine, and alleviate potential hazards (Leenen & Meyer, 2021).

To ensure effective cybersecurity, analysts must consistently maintain a heightened level of awareness concerning security incidents and their potential ramifications. This entails keeping abreast of the most current security developments and dangers (Ural & Acartürk, 2021).

Collaboration and communication are crucial for a cybersecurity analyst to effectively work with other specialists in the field. This is the act of exchanging information regarding security warnings and collaborating in order to address security concerns (Hui et al., 2010).

Making use of artificial intelligence and big data analytics has become essential for cybersecurity analysts. They depend on these technologies to effectively handle vast amounts of data, detect trends, and make well-informed conclusions regarding security threats (Leenen & Meyer, 2021).

Thus, in addition to working long hours, cyber analysts are faced with a complex working-environment where failure to perform can have consequences for detecting and responding to cyber threats. A review on the challenges faced by SOC team analysts (Agyepong et al., 2019) identified several threats to SOC analyst performance, including the volume of security alerts, false positive alarms, sophisticated attacks, incident management complexities, skills and experience shortage, tacit knowledge, manual and repetitive processes, workloads,

burnout, analyst turnover, false negatives/missing attacks, lacking performance metrics for analysts, and inadequate communication. Human error is, however, not a novel concept in cybersecurity. As early as 1992 it was concluded in a report by the National Institute of Standards and Technology (NIST) that human error was the primary factor contributing to information security incidents (NIST, 1992). This assessment still holds true three decades later (Alsharif et al., 2022; Chowdhury & Gkioulos, 2021) which clearly suggests that cybersecurity research should continue to include the human factor as part of its scope.

2.2. Human Factors in Cybersecurity

While the importance of human factors in cybersecurity have been acknowledged for as long as the internet has been publicly available (e.g., McCauley-Bell & Crumpton, 1998; NIST, 1992), it has not been sufficiently addressed in cybersecurity research which tends to be biased towards technical solutions (Gutzwiller et al., 2015). After noting that organizations which implement a high number of technical security solutions still experience a disproportionate number of security-related breaches, Schultz (2005) proposed that cybersecurity is primarily a people problem and not a technical problem. He writes:

> "*Despite the fact that a considerable amount of technology is designed to run without people in the loop, technology is designed to be managed and used by people. No matter how human-independent technology is supposed to be, people need to interface with it at various points in time*." (Schultz, 2005, pp. 425).

The realization that there is a security risk associated with the interaction between humans and security system technology has led to the concept of viewing humans as 'the weakest link' in cybersecurity (Schneier, 2002; although the weakest link concept predates cybersecurity, Mc Mahon, 2020). Adopting this view may be a security threat in itself if it leads to approaches to cybersecurity training that is based on a flawed view of the role played by humans (e.g., awareness training; European Union Agency for Cybersecurity, Drogkaris, & Bourka, 2018). One could argue that empowering approaches to human performance in cybersecurity rather than defeatist ones will lead to better outcomes (Mc Mahon, 2020) and should therefore not downplay how environmental factors and organizational culture influence human performance in cybersecurity (European Union Agency for Cybersecurity, Drogkaris, & Bourka, 2018; Gutzwiller et al., 2015). While the human factors research discussed thus far mostly addresses human errors as they relate to causes of security breaches, human factors

research also addresses the determinants of performance among individuals tasked with detecting and defending against cyber threats (Agyepong et al., 2019; Jøsok et al., 2016, 2017, 2019). To this end, there is a need for a more targeted focus in cybersecurity research aiming to increase our understanding of cyberspace and to push the boundaries of human factors science (Gutzwiller et al., 2015).

Because there is a need for understanding the environmental (e.g., cyberspace) and organizational challenges associated with human performance in cybersecurity (Gutzwiller et al., 2015; Jøsok et al., 2017), and because flawed base assumptions when taken for granted can lead to suboptimal solutions (European Union Agency for Cybersecurity, Drogkaris, & Bourka, 2018; Mc Mahon, 2020), an analysis of how these challenges are conceptualized in terms of the frameworks and ideas that have been used to understand them is warranted. As we have discussed, the technical and human factors of cybersecurity are interdependent and cannot be fully understood in isolation (Gutzwiller et al., 2015). Rather, they are interwoven social and organizational processes (European Union Agency for Cybersecurity, Drogkaris, & Bourka, 2018; Jøsok et al., 2017; Staheli et al., 2016). Thus, it is worth looking closer at research on human performance in cyber-physical systems, that is, research related to the interconnectedness between machines, networks, and the physical world (Gutzwiller et al., 2015) to understand the complex of challenges associated with working-environments that require proficiency in navigating (and understanding) interacting social and technical systems (Hui et al., 2010; Leenen & Meyer, 2021; Patel, 2014; Ural & Acartürk, 2021). The following subsections will first look at sociotechnical systems theory (Trist & Bamforth, 1951) and its relationship with current cybersecurity research, challenges faced by cyber teams and how they relate to situational awareness (Endsley, 1988) and communication of recognized cyber pictures.

2.3. Sociotechnical Systems Theory

Sociotechnical Systems (STS) theory was originally proposed after World War II to explain the disruptive effects of mechanization on the organization of work in British coal mines (Trist & Bamforth, 1951). It was suggested that a production system could not be sufficiently described as a technical system or a social system. Rather, it should be viewed as an interrelationship of both types of systems; a STS, where interaction between social and technical systems create psychological effects in workers that have consequences for productive outcomes. Thus, the observed disruption of what was referred to as ‘a psychologically effective mode of

organization' was attributed to a flawed view of the coal mine production system as purely technical (Trist & Bamforth, 1951). Subsequently, it was proposed that effective performance (e.g., productive output, morale, and so on) is a function of joint optimization of technical and social systems, and that maximizing one system at the expense of the other results in suboptimal performance (Trist & Bamforth, 1951; Trist et al., 1963).

While it may seem like a simple theoretical concept, STS theory includes a variety of concepts such as 'whole' tasks, organizational culture (the pattern of attitudes, values, and beliefs held by leaders and workers), open systems (organizations are not isolated from their environment), psychological needs and motivation, Marxist-inspired ideas of individuals being alienated from productive activity and fellow workers, group-based rather than individual-based job (re)design, and (responsible) autonomy in worker groups (Emery, 1959; Emery & Thorsrud, 1976; Kelly, 1978; Trist & Bamforth, 1951; Trist et al., 1963). Responsible autonomy refers to all workers having the skills to perform any task in the production process (multi-skilling), meaning that when they are done with a task, they can help others with their tasks, if necessary, thus facilitating work continuity and coordination (Kelly, 1978). This approach was proposed to increase the feeling of being connected with the productive outcome and connection with workers. Similar ideas of autonomy in the form of dynamic group organization and distributed leadership have been mentioned in the context of team performance in cybersecurity (Jøsok et al., 2017). The argument being that the complexity of defensive cyberspace operations requires an adaptive approach that "breaks with fixed goals and fixed roles and task paradigms" (Jøsok et al., 2017, pp. 492). This point was also raised by David Omand in Securing the State (Omand, 2011). He wrote that the further removed you are from the point of execution, the less likely you are to know all the facts. Thus, you should state what you wish to achieve, not what you wish people to do (Omand, 2011). The multi-skilling relevant for autonomy in the original STS research (Kelly, 1978; Stahl, 2007) have also been referenced in cybersecurity research as integral to the performance of cyber operators through observations that cybersecurity professionals often need to switch between different cyber defense tasks, and in suggestions that training should reflect this need (Gutzwiller et al., 2015). The group-focused STS approach seemed to have an edge over the then-favored scientific management approach in that organizations were able cut staff significantly and still achieve reasonable outcomes, sometimes increasing efficiency (Kelly, 1978).

The core assumptions of STS theory and the social bias of STS interventions (not being sociotechnical/joint optimization) have, however, been criticized historically (Kelly, 1978; Pasmore et al., 1982). For example, it has been argued that STS research does not at all address – let alone prove – that joint system optimization is the solution to STS-related challenges; the research suggests that group autonomy is the solution to human/group performance issues in STSs (Kelly, 1978). Furthermore, the socially biased and autonomy-dependent STS interventions have been criticized for being more applicable in Scandinavian countries where there is more cooperation (and less social distance) between organizational hierarchies (Stahl, 2007). In relatively recent years, however, the STS term has been used in cybersecurity research to convey that the cybersecurity working-environment is a cyber-physical complex that consists of both human-human and human-machine (or human-computer) interactions (e.g., Charitoudi & Blyth, 2013; Jøsok et al., 2016; Zoto et al., 2018). This research operates from a core assumption that building and maintaining cyber resilience requires one to consider these interactions as opposed to just considering technical solutions (Jøsok et al., 2016). Thus, the STS approach to cyber risk management and impact assessment is suggested as an alternative to asset-focused (and technology biased) approaches that are based on the CIA triad (Charitoudi & Blyth, 2013). In the context of cybersecurity, STS can refer to:

> "[...] *people (individuals, groups, roles and organizations), physical equipment (buildings, surroundings, etc.), hardware and software, laws and regulations that accompany the organizations (e.g. laws for the protection of privacy), data (what data are kept, in which formats, who has access to them, where they are kept) and procedures (official and unofficial processes, data flows, relationships, in general anything that describes how things work, or better should work in an organization)*" (Charitoudi & Blyth, 2013, pp. 33-34).

In other words, an STS as used in a cybersecurity context includes how people interact with each other and cyberspace (as defined in Kuehl, 2009 and Gutzwiller et al., 2015), each other through cyberspace, and the technology that mediates this interaction. In contrast to the original incarnation of STS theory (Trist & Bamforth, 1951; Trist et al., 1963; but, ironically, in line with how the actual research was conducted; Kelly, 1978; Pasmore et al., 1982), there is less explicit emphasis on joint system optimization in how STS theory is conceptualized and applied in cybersecurity research. The goal is to capture the complexities that cannot be captured by linear modeling (Charitoudi & Blyth, 2013), and the technological aspects of the

cybersecurity working-environment (including the methods for using the technology) appears to be somewhat taken for granted. Thus, the focus is on tasks and roles, responsibility flows and behavioral dependencies, human adaptive ability, and the concept of "agents" as something that encompass individuals, groups of people, and even technological systems (Charitoudi & Blyth, 2013; Jøsok et al., 2016, 2017, 2019; McNeese et al., 2021; Yufik & Malhotra, 2021). This latter notion of agents in cybersecurity being both human and technological is also partly reflected in questions cybersecurity researchers ask regarding how teams adapt and respond to cyber threat situations versus how teams solve problems in non-cybersecurity contexts:

> "[...] *how does this apply with the cyber world in which perception is limited to what a computer can convey through the monitor, where space is seemingly infinite, and comprehension is shared between the computer and analyst?*" (Champion et al., 2012, pp. 2018).

What is also implicated in the question cited above, is that detection and comprehension of threats in cyberspace is a complex issue where humans appear more reliant on machines than in non-cybersecurity contexts. To understand the extent of these challenges, we have to also understand the challenges associated with the complex information environments where these human-machine interactions occur and how they affect team performance in cyber operations.

2.4. Challenges to Team Performance in Cyber Operations

One example of cyber operative teams are cyber protection teams, which perform threat-oriented missions to defend critical military networks against adversaries (Trent et al., 2019). They perform three basic types of missions: survey missions, which consist of short duration assessments of network vulnerabilities and recommended mitigations. Secure missions, centered on the hardening and defending of cyber key terrain, and Protect missions, which are time-sensitive deployments that combine Survey and Secure tasks with providing support for organizations that have experienced a cyber intrusion. A cognitive task analysis of the cyber protection team workflow (Trent et al., 2019) identified an extensive collection of tasks, including information exchange activities, planning and logistical activities based on receiving a mission statement, monitoring and collection activities that involves the deployment of sensors and subsequent data collection, analysis and synthesis tasks such as integrating and evaluating information from network and forensic analyses, continuous sensemaking, risk

evaluations, and closure procedures such as reports and briefings. While it was stated that no team performed the full collection of tasks identified in (Trent et al., 2019), there was still a notion of teams needing to adapt their work to suit the constraints of their missions, which is achieved by teams leveraging their understanding of a given situation.

The complexity of the information environment poses several challenges to team performance in cyber operations, especially in the context of making sense of data streams to inform defensive decision-making. Some of these challenges relate to navigating the four dimensions (or 4Vs) of Big Data environments, which pertains to the increasing volume, velocity, and variety of information, and decreasing veracity. Variety refers to the amount of different data requiring different treatments, veracity refers to the quality and availability of data, velocity refers to the velocity at which data must be managed, and volume refers to the volume of data that must be handled. In a practical example, cyber operators tasked with analyzing intrusion detection system alerts to determine if they are truly suspicious (the triage analysis aspect of network analysis) and should be forwarded to an escalation analyst, often have a predefined amount of time to analyze each alert. The role of triage analyst is associated with high cognitive and temporal demand, increased distress, and reduced task engagement (Greenlee et al., 2016). To contend with the rapidly changing information environments associated with cyber operations, cyber teams must dedicate effort to continuously develop and adapt a shared situational awareness and understanding of recognized cyber threats, while also converting their understanding into key information elements that effectively communicate actionable information to support decision-making. It is understanding and influencing the relationship between how cyber teams navigate information in complex information environments and its subsequent influence on communication that constitute the contextual scope of this thesis.

While cyber teams build situation awareness (SA) to navigate the information complexity of cyberspace, the SA concept can be traced back to World War I fighter pilots' internal (or mental) model of the world around them at any point in time (Press, 1986; cited in Endsley, 1988). To ensure mission success, this internal model was achieved in steps where the pilot first had to be aware of their enemy's location before being aware of 'their own self' (Press, 1986; cited in Endsley, 1988). As more and more technologies were added to the aircraft systems, however, SA has become increasingly dependent on human-machine interactions

between the pilot and the aircraft systems used to monitor and navigate the environment. SA can be defined as:

> "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*" (Endsley, 1988, pp. 97).

According to the SA model proposed by Endsley (1988), SA is achieved in three contingent stages or levels (SA Level 1-3; Figure 2), where each level must be achieved in succession in order to have full SA for decision-making.

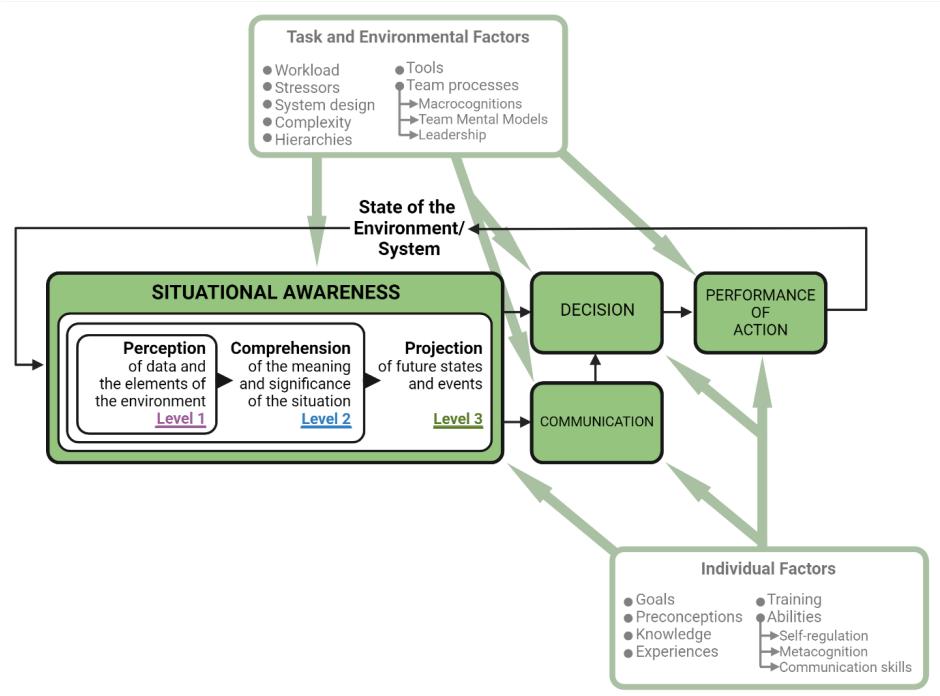

Figure 2. Endsley's (1988) Situational Awareness model.

Figure modified from (Lankton, 2007).

The first stage (SA Leve l) is the perception stage. It consists of the operator engaging in basic perceptual processes (i.e., monitoring displays, cue detection, recognition) that induce awareness of situational factors and their current state, and can include technical systems, other operators, and associated conditions such as their locations and the tasks in which they are

engaged. Raised awareness of situational factors then leads to the second stage (SA Level 2), which is the comprehensions stage. In SA Level 2 the operator integrates previous experiences with current perceptions to form an understanding of the factors that influence the current situation. This understanding then forms the basis for the third stage (SA Level 3). This is the prediction stage which allows for the operator to use their understanding of current situational factors to predict possible future states of the environment, including those following the action.

In *Securing the State*, David Omand (2011) writes that "*the most basic purpose of intelligence is to improve the quality of decision-making by reducing ignorance*". Cyber defense decision-making is dependent on good SA. Developing a SA that enables good decision-making during a cyber threat situation depends on having an accurate recognized cyber picture (RCP; also referred to as common operational picture or cyber common operational picture). SA in a cyber context entail having awareness of the underlying state of a specific cyber environment at any given point in time and the factors that will influence its future state. RCPs contribute to this awareness through the presentation of actively selected and actionable information that is used to describe the actual circumstances of an incident or threat (Knox et al., 2018). The information contained within an RCP can include the severity of known and unknown effects, the state of assets, and suggested courses of action, but may exclude details at the level of indicators of compromise (Knox et al., 2018; Tinde, 2022). A failure to generate effective RCPs may result in critical information being lost due to suboptimal communication flow and inadequate cyber defense (Rosen et al., 2008; Knox et al., 2018).

The RCP by itself does not constitute SA but is a visual or cognitive representation of cyber threat-related incidents and activities, serving as an important contributor toward establishing a shared SA (Alavizadeh et al., 2022). Because RCPs can consist of visual representations of cyber threat information, one way to facilitate the understanding of complex cyber threat information and subsequent RCP communication in cyber teams is through the use of visual aids (outside of the traditional Security Information and Event Management displays) that help build a shared mental model of the situation (Kullman et al., 2018). As one of the studies included in this thesis applied visualization in XR to optimize information processing and facilitate shared mental modeling of a cyber threat situation to improve communication in

cyber teams, the next section will address the use of visual aids to establish shared mental models of cyber threat situations.

2.5. Visualization Aids to Establish and Improve Shared Mental Models of Cyber Threat Situations in Cyber Teams

The purpose of RCP communication is to achieve a shared mental model of the cyber threat situation and to achieve shared SA. Mental models are cognitive knowledge structures of the causal relationships that govern world phenomena such as objects (humans, computers, footballs, buildings), events, and systems. Thus, mental models help individuals understand the behavior of phenomena which allows for predicting how they will respond when interacting with them. Shared mental models / team mental models concern the sharing of task-work, team-work, and temporal knowledge. In the context of crisis management, the goal of shared and team mental models is to distribute knowledge between team members to maximize overlap (Moon et al., 2020). Shared mental models in teams improve coordination and performance (Cannon-Bowers & Salas, 2001; Edgar et al., 2021). The mammalian brain, however, has evolved to understand events and information as they occur in time and space (Berggaard et al., 2018; Eichenbaum, 2014; Ray & Brecht, 2016). Achieving a shared mental model of events in cyberspace is fundamentally a challenging task when cyberspace cannot be sensed directly through the human sensory apparatus (Champion et al., 2012; Gutzwiller et al., 2015). Cyberspace is not a 3D environment where the relationship between the activity of agents in a given network and segments of the network can readily be reasoned about in terms of geographic proximity. Moreover, the speed of events is happening at a pace that makes it impossible for humans to infer causality without the aid of technology. Thus, the mental model of how a cyber threat situation relates to a given network and its associated assets may differ between individuals in ways that are not easy to establish due to the imperceptibility of cyberspace. Differences in how mental models are constructed may therefore mean having different understandings of causal relationships which can be challenging for agreeing on what to focus on during RCP communication, and for achieving a shared SA.

Shared mental models in teams can be achieved through the implementation of tools that facilitate efficient communication (Edgar et al., 2021). In the context of cybersecurity, this could for example entail the use of information sharing platforms. The effectiveness of information sharing platforms may depend on whether users know how to use them correctly (Brilingaitė et al., 2022). Other communication tools that help facilitate shared mental models

of events in cyber space could be indicating how an attacker got access to a protected network on 2D schematics/diagrams of the network topology (Kullman et al., 2019b). Such solutions, however, do not scale well with increased complexity and their static nature does not allow for exploration of interactions between nodes in the network. Additional communication tools that allow for exploration and increased complexity could for example be graph representations of the network traffic in packet capture (pcap) software or radial diagrams (Kullman et al., 2019b). Graph representations allow for visualization of the network and traffic volume in terms of number of sessions between hosts to help infer how potential attackers have moved within the network. During dyadic face-to-face communication, such solutions usually only allow for one individual exploring the topology at a time. Two individuals exploring the topology together would either entail one person watching the other person clicking on nodes if they wanted to orient together, or two individuals sitting on different computers thus not being able to see what the other person is doing. Furthermore, 2D schematics and graph representations in pcap software rely solely on the visual sensory system to encode information when orienting in the network. The visual system has limited attentional resources (Kanwisher & Wojciulik, 2000) and is therefore a major bottleneck for the information flow between the cyber operator and information from computer systems (Kullman et al., 2018). As mental models are formed by interacting with the phenomenon in question, how information is presented on the screen may therefore influence the mental model of the cyber operator and individuals communicating with each other. Current visualization methods may also not be true to the mental model of cyber operators, thus requiring more cognitive effort to fit the visualized information in their mental model. During face-to-face communication, this may require the cyber operator to rely on extra visualizations or explanations to relate what is being visualized to their mental model of the context. Other threats to performance when relying on the visual system are interactions between stress and display size (Hancock et al., 2015) and the role of stress on oculomotor control (Poth, 2021).

A recent review on the use of visualization for SA in cyber threat situations found that most visualizations targeted personnel at the operational level, while non-experts, managers, and decision-makers at higher organizational levels were rarely in the target user-group. Visualization tools were mostly designed for perceptual level SA and focused on visualizing threats, while few tools focused on visualizing impact information, response plans, or information shared within teams to facilitate higher levels of SA (Jiang et al., 2022). Although

there were many visualization approaches reported in the literature, immersive/extended reality (XR) approaches were rarely used (Jiang et al., 2022).

A meta-analysis (Kaplan et al., 2021) of extended reality methods for training enhancement assessed how effective training in extended reality was in the transfer of skills to real-world settings and without the aid of XR. While this latter criterion is incompatible with the purpose of the XR approach used in paper III in this thesis, it is still insightful to review the results of the meta-analysis. The authors (Kaplan et al., 2021) only included studies where participants were over the age of eighteen and the outcome measure was performance, which left them with a total number of twenty-five studies. Their findings suggested that while extended reality were time and cost effective, they were generally not more effective than traditional methods, unless they included physical tasks (Kaplan et al., 2021). The authors stated that limitations with respect to the available literature prevented granularity in analysis beyond dividing studies into cognitive, physical, mixed tasks. Thus, there are not enough studies to separate studies based on domain (e.g., surgery), those that assessed mixed reality (MR) from virtual reality (VR) and augmented reality (AR), nor were they able to separate studies based on how information was encoded (aside from immersiveness; Kaplan et al., 2021). For instance, 3D visualizations presented in MR/VR that allow for roaming around in the learning environment may leverage spatial-learning strategies similar to the method of loci (Kuhrt et al., 2021). The method of loci entails imagining a house (or palace; a memory palace), where the individual assigns information they want to remember in different rooms in the house, and then imagines walking from room to room to remember each piece of information. The method of loci is an effective memory technique (Dresler et al., 2017; McCabe, 2015) also for remembering 3D objects in VR settings (Reggente et al., 2019).

While visualization techniques may serve as technological aids to facilitate cyber team navigation of complex information environments, information processing and communication is also dependent on the cognitive processes cyber teams engage in to navigate the complexities inherent in their working-environments (Gutzwiller et al., 2015, 2020). The second study included in the thesis work is concerned with identifying neurocognitive performance metrics related to team performance in cyber operative contexts. Thus, the following three sections will address cognitive processes and abilities related to the goal-directed regulation of cognition. This will be followed by an introduction to the field of neuroergonomics and a summary of the chapter.

2.6. Metacognition

Metacognition is the ability to cognitively monitor, select, and control ongoing cognitive processes, and is typically referred to as cognition of cognition (or thinking about thinking; Efklides, 2008; Flavell, 1979). It is suggested to play an important role in the oral communication of information, as well as the cognitive and behavior modification involved in self-regulated, goal-directed behaviors and problem-solving (Efklides, 2008; Flavell, 1979). Based on the seminal work by Flavell on metacognitive knowledge (Flavell, 1979; Flavell & Wellman, 1975), a commonly accepted framework for metacognition was proposed (Nelson & Narens, 1990; Figure 3). Metacognition is divided into two main components, metacognitive knowledge (or monitoring) and metacognitive control (or regulation; Baird, 1986; Baker & Brown, 1984; Livingston, 2003). Metacognitive knowledge is the knowledge (or models) individuals have about their own cognitive processes, as well as their ability to monitor ongoing processes and reason about them (Fabricius & Schwanenflugel, 1994; Flavell, 1979). Metacognitive control consists of the cognitive ability to plan and adapt behaviors in a self-regulated manner (Baker & Brown, 1984; Efklides, 2008). As outlined in Figure 3, metacognitive knowledge is the bottom-up processing of object-level information to the meta level, while metacognitive control is the top-down flow from meta-level processing to the object level (Boldt & Gilbert, 2022; Nelson & Narens, 1990, 1994; Shimamura, 2008). The object level consists of all cognitive functions, while the meta level maps the relationship between cognitive functions and outcomes to exert control over object-level cognitive functions (although there might be some overlap between the two; Boldt & Gilbert, 2022).

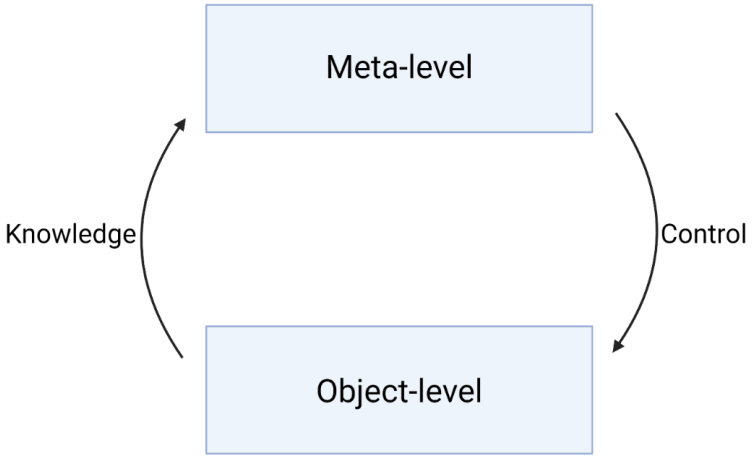

Figure 3. Metacognitive knowledge and control.

Bottom-up metacognitive knowledge of object-level cognitive processes and top-down metacognitive control of object-level cognitive processes from the meta level (adapted from Nelson & Narens, 1990).

Several metacognitive processes and constructs are discussed in the literature, some of which refer to the same or overlapping constructs (Efklides, 2008; Flavell, 1979; Fleur et al., 2021; Fleming & Lau, 2014). An overview of some of them can be found in Table 5. Metacognitive awareness (or monitoring) refers to the awareness of being engaged in a cognitive process and whether it will lead to a desired outcome (Flavell, 1979), linking metacognitive knowledge and self-regulated behaviors through metacognitive control (Efklides, 2008).

Component	Bottom-up (to meta-level)	Description
Metacognitive knowledge (Flavell, 1979; Nelson & Narens, 1990)	Metacognitive monitoring, Metacognitive experience, Metacognitive awareness (Flavell, 1979)	A form of brief or lengthy self-awareness where one is aware of being engaged in cognitive processes and the outcomes they will lead to.
	Metacognitive memory (Efklides, 2008; Flavell, 1979; Flavell & Wellman, 1975)	Knowledge of the contents of one's memory, goals, past experiences, and the abilities and skills one possesses. Mental models of conscious and unconscious object-level processes (own and other's).
	Metacognitive skills (Efklides, 2008), Metacognitive strategies (Flavell, 1979).	Knowing which object-level cognitive processes and behaviors that will lead to desired outcomes (procedural knowledge).
	Top-down (to object-level)	
Metacognitive control (Nelson & Narens, 1990)	Metacognitive judgment (Fleming & Lau, 2014), Offline metacognition (Fleur et al., 2021)	A current, prospective, or retrospective judgment of information or performance based on metacognitive memory or (conflict) monitoring.
	Metacognitive bias (Fleming & Lau, 2014)	Level of overconfidence or underconfidence in metacognitive judgments regardless of performance
	Metacognitive sensitivity, Metacognitive accuracy (Fleming & Lau, 2014)	The ability to correctly judge one's own performance and its relationship with bias. Affected by task difficulty (bias increases)
	Metacognitive efficiency (Fleming & Lau, 2014; Fleur et al., 2021)	Level of metacognitive sensitivity when controlling for actual performance

	Metacognitive skills (Efklides, 2008; Nelson & Narens, 1990; Veenman & Elshout, 1999)	Ability to select and deploy procedural knowledge and metacognitive strategies. Include strategies for learning, orientation, planning, regulation of cognitive processes, monitoring the execution of planned actions (e.g., knowledge acquisition), and for evaluating the outcome of task processing (e.g., retention, and retrieval). Based on knowledge about goals, what one knows and does not know, and knowledge about how to learn and perform optimally.
	Online metacognition (Fleur et al., 2021)	Tactical (stimulus-response) control over object-level cognition. Controlled response selection that can be based on monitoring but not based on metacognitive memory, strategies, or judgment).

Table 5. Metacognitive constructs

The contents of metacognitive awareness can serve as cues for changing the tasks one is engaged in, the goals one is pursuing, or the strategies one is employing when realizing that the activities one previously engaged in will not lead to desired outcomes (Flavell, 1979).

While this section has addressed individual-level metacognition, it is important to note metacognitive processes are also proposed to occur at the level of teams (team metacognition; Cooke et al., 2013). According to interactive team cognition theory, team-level cognitions are understood as a context dependent activity that should be studied at the level of the team (Cooke et al., 2013). While metacognitive abilities represent a general ability to monitor and control cognitive processes, and by extent, navigating information environment in a goal-directed manner, the agility with which an individual navigates a complex working-environment may require the identification of a specific set of cognitive abilities. The work included in this thesis is specifically concerned with identifying performance indicators that allow cyber team members to navigate information environments in a way that is flexible and conducive for efficient communication.

2.7. Cognitive Agility

The ability to engage in flexible decision-making in dynamic working environments is referred to as cognitive agility (Good, 2009; Good & Yeganeh, 2012). The cognitive agility construct is originally proposed to support decision-making in dynamic contexts through the engagement of cognitive processes and abilities related to cognitive openness, focused attention, and

cognitive flexibility (Good, 2009; Good & Yeganeh, 2012). Cognitive openness consists of perceptual attention that allows an individual to notice and search for new information that spans internal and external environments, and subsequently identify changing situational demands (Good & Yeganeh, 2012). Focused attention is the capacity to attend to task-relevant stimuli while ignoring task-irrelevant stimuli, and cognitive flexibility is the capacity to switch between cognitive and perceptual processes to adapt responses according to changing contextual demands (Friedman & Robbins, 2022). An example of cognitive agility in cyber operators could entail the capacity for flexible analytical pivoting when conducting intrusion analysis (as described in the diamond model of intrusion analysis; Caltagirone et al., 2013). Being aware of these processes in terms of knowing about them, when one is engaged in them, and also knowing when and how to engage in them, is dependent on metacognitive abilities (Efklides, 2008; Flavell, 1979; Fleur et al., 2021). Good and Yeganeh (2012) propose some metacognitive strategies to improve cognitive agility, thus drawing further connections between human performance in dynamic working-environments and metacognition.

2.8. Cognitive Control

Both metacognition and cognitive agility as described in the previous subsections are concerned with the goal-directed control of cognition and behavior. The cognitive flexibility, focused attention, and cognitive openness that are part of the cognitive agility construct (Good & Yeganeh, 2012), and metacognitive knowledge and control are facets of cognitive control (Boldt & Gilbert, 2022; Buckley et al., 2014; Desender et al., 2014; Fleur et al., 2021; Miyake et al., 2000; Questienne et al., 2018; Shimamura, 2008).

> "*Ultimately, cognitive control is grounded in behavior. This means that internally oriented aspects of control, such as those that plan for the future, must be integrated with externally oriented aspects of control, such as those that select appropriate sensory features for processing and action*" (Nee, 2021; pp. 1).

Cognitive control (often referred to as executive function in clinical literature) is a term derived from the perspectives of cybernetics and cognitive science (Friedman & Robbins, 2022; although cognitive control does not necessarily equate to control theory; Medaglia, 2019). It is usually associated with the healthy functioning of a brain area called the prefrontal cortex (Cohen, 2017), and is considered a core process in goal-directed behavioral regulation and in countering automatic, habitual, and inflexible responding. It involves the neurocognitive ability

to initiate, maintain, and monitor relevant neural activity to adapt to environmental challenges in support of goal-directed actions (Gratton et al., 2018; Botvinick et al., 2001). In other words, cognitive control enables humans "*to flexibly coordinate thoughts and behaviors in order to accomplish internal goals*" (Kim et al., 2011, pp. 130). Consequently, the absence of cognitive control produces automatic behavior that is not goal-directed, flexible, and adaptive (Friedman & Robbins, 2022). Higher cognitive demand, which is a function of task difficulty-factors such as the number of contextual rules and task variables, and rule complexity, requires a higher degree of cognitive control to be implemented (Tsaparlis, 2014).

Given that high stress and cognitive load are factors influencing cyber team communication and performance, cognitive control is a central construct to consider in the context of understanding and predicting cyber operative performance. Critical to the process of navigating complex and stressful information environments, especially as it relates to metacognitive processes underlying agile hybrid space movements and executing OLB-processes, is the cognitive control of attention. Whether it is flexible attentional processing during analytical pivoting or task shifting, alternating focus on internal or external stimuli or focusing on key elements during SA building and communication, the ability to allocate attentional resources to information that is in line with current priorities and goals precede the processing of that information.

The field of neuroscience has been instrumental in uncovering the mechanistic processes underlying cognitive control (Friedman & Robbins, 2022). Given the need for advancing our understanding of cognition in the context of cyber operator and cyber team performance (Gutzwiller et al., 2015), the following section will provide a general overview of how the field of neuroergonomics apply neuroscience to study human factors-related performance issues.

2.9. Neuroergonomics

Both neuroergonomics as a term and as a field was first proposed by the late Raja Parasuraman (2003) as a result of combining the knowledge gained from his numerous contributions to the fields of cognitive neuroscience (e.g., Parasuraman, 1990, 1998; Parasuraman et al., 2002) and human factors in human-computer interactions (e.g., Parasuraman & Riley, 1997; Parasuraman et al., 1996, 1999, 2000; Scerbo et al., 2001). The field has a broad scope with respect to improving human performance and its methods are utilized in both civilian and military sectors

(Ayaz & Dehais, 2019; Christensen et al., 2010). The term 'neuroergonomics' is a combination of the word 'neuro' from neuroscience, which refers to the scientific study of the brain and nervous system, and 'ergonomics' in reference to the study of humans at work (or human factors). Thus, the original definition of neuroergonomics was "the study of brain and behavior at work" (Parasuraman, 2003, pp. 5). The field of neuroergonomics has two major goals:

> "*(1) to use existing and emerging knowledge of human performance and brain function to design technologies and work environments for safer and more efficient operation; and (2) to advance understanding of brain function in relation to human performance in real-world tasks*." (Parasuraman, 2003, pp. 6).

Parasuraman (2003) argues that the added benefits of neuroergonomic approaches extend beyond traditional neuroscience and conventional ergonomics, suggesting that approaching complex ergonomic problems from a neuroscientific perspective will lead to refinement of ergonomic theories. Examples could be improved information presentation and task design (Parasuraman, 2003). One could argue that all ergonomic approaches aim to be neuroergonomic. All of human behavior is regulated by the nervous system and human performance is capped by its limitations. Thus, 'neuroergonomics' may in reality be a redundant term that will disappear when its goals are achieved (Christensen et al., 2010).

In the context of cyber team performance, the field of neuroergonomics has been concerned with improving SA processes since its inception. Improving monitor and display designs for SA was one of the areas where Parasuraman (2003) suggested that neuroergonomics could improve human-computer interactions. For instance, using neuroscientific knowledge about which colors and shapes are the most effective at triggering attention allocation in the nervous system, and how to limit information overload in the nervous system could be used to improve airplane displays (Parasuraman, 2003). This proposal could be extended to improving Security Information and Event Management displays in order to combat vigilance decrements in cyber operators (Guidetti et al., 2023). Research on visual display size has found that small display sizes may lead to operator performance decrements in contexts with high time pressures (Hancock et al., 2015). Optimizing information presentation based on neuroergonomic principles to facilitate adaptability (Parasuraman, 2003) links neuroergonomics to SA (Endsley, 1988). Neuroergonomics has received much interest in the US Air Force Research Laboratory and other agencies within the Department of Defense (Christensen et al., 2010).

> "[...] *the tremendous progress and investment in neuroscience can and should be focused on specific work environments in order to produce significant augmentation of human performance*" (Christensen et al., 2010, pp. 1).

Some topics that have been explored in the context of neuroergonomics for Defense are stress, hormones, resilience and hardiness, emotion and cognition, vigilance, trust, and neuromodulation (i.e., influencing brain activity; "neuroenhancement") through non-invasive brain stimulation and pharmacological substances (Brunyé et al., 2022; Christensen et al., 2010; Pobric et al., 2021). Given that stressful working conditions may have a detrimental impact on how cyber teams process and communicate cyber threat information, the work presented in this thesis have employed neuroergonomically informed approaches to 1) measure indicators of stress- and information processing-related cognitive activity through neurophysiological measurements and self-reports, and assess their association with communication demands, and 2) the visual presentation of network data and activity to facilitate shared mental modeling and communication of cyber threat information.

2.10. Chapter Summary

This chapter has provided the background information needed to understand the work conducted in this thesis. This has included an overview of what is included in terms related to cyberspace and cybersecurity, how SOCs are structured, how the complex information environments associated with cybersecurity pose challenges to cyber teams, and how cyber team must engage in processes such as building SA and communicating SA-related information in the form of RCPs. The potential for using visualization aid to facilitate RCP communication and shared mental models was discussed briefly, followed by an overview of cognitive constructs such as metacognition, cognitive agility, and cognitive control.

Chapter 3

3 The State-of-the-Art of Related Research

This chapter provides an overview of the state-of-the-art research that informed the studies on human-to-human communication in cyber threat situations in this thesis. This overview is provided to highlight the methodological considerations that went into subsequent research.

3.1. Cyber Situational Awareness

Establishing SA in the context of cybersecurity may be subject to pressures that are not found in other fields:

> "*Although to understand and act in the physical world is something humans are well-equipped to achieve, in the ethereal cyberspace, interfaces are the single point of connection used to extend human perception and action into the dense world of the network*" (Gutzwiller et al., 2015, pp. 322).

Endsley's SA model is commonly referred to in cybersecurity research (Ofte & Katsikas, 2023). However, as the human operator is dependent on technology to understand and navigate cyberspace (Gutzwiller et al., 2015), researchers have attempted to extend the SA concept to understand what it means in the context of cybersecurity (e.g., Barford et al., 2010; Franke & Brynielsson, 2014; Gutzwiller et al., 2016, 2020; Ofte & Katsikas, 2023). This has led to the cyber SA concept which is proposed to be a subset of SA that concerns the cyber environment (Franke & Brynielsson, 2014). An additional term, "cyber-cognitive SA" has been proposed to denote cyber SA in humans (Gutzwiller et al., 2016), however, in the work presented in this thesis, cyber SA in humans will just be referred to as cyber SA (acronym CSA in the empirical papers). In a very influential review, Franke and Brynielsson (2014) suggested that cyber SA can be achieved by feeding data from intrusion detection systems (IDSs) in data fusion processes or interpreted directly by decision-makers, but also be combined with information about plausible future attacks (e.g., intelligence reports). Later work has suggested that cyber SA in humans is a more involved process and should be differentiated from data fusion and what information is presented on screens (Gutzwiller et al., 2016). It has also been argued cyber SA should not be treated in isolation but should be considered as part of the overall SA and needs input from events occurring in the physical world (Franke & Brynielsson, 2014). Cyber SA needs to include the network, the world, and the organization or team (Gutzwiller et al.,

2016). What cyber SA entails, including what and how data should be processed to achieve cyber SA is highly dependent on the context (Franke & Brynielsson, 2014). Based on the assumption that human decision-makers were "indispensable" components in SA systems, Barford and colleagues (2010) suggested that building cyber SA for cyber defense at least consisted of the seven following steps listed in Table 6:

Step	Description
1. Awareness of the current situation (situation perception).	Situation recognition and identification. Identifying the type of attack (recognition is only recognizing that an attack is occurring), the source (who, what) of an attack, the target of an attack, etc. Situation perception is beyond intrusion detection.
2. Awareness of the impact of the attack.	There are two parts to impact assessment: 1) assessment of current impact (damage assessment) and 2) assessment of future impact (if the attacker continues on this path or more general if the activity of interest continues - what is the impact?).
3. Awareness of how situations evolve.	Situation tracking is a major component of this aspect.
4. Awareness of adversarial behavior.	Attack trend and intent analysis to understand behavior within the situation rather than the situation itself.
5. Awareness of why and how the current situation is caused.	Includes causality analysis (via back-tracking) and forensics.
6. Awareness of the quality and trustworthiness of the collected cyber SA information and derived decisions.	Quality metrics include truthfulness (or soundness), completeness, and freshness.
7. Assess plausible futures of the current situation.	Involves a multitude of technologies for projecting future possible actions/activities of an adversary, paths the adversary might take, and then constraining the possible futures into those that are plausible. Requires an understanding of adversary intent, opportunity, and capability, as well as own vulnerability.
Notes. Taken from (Barford et al., 2010).	

Table 6. The seven steps (or criteria) for building cyber SA for cyber defense

While cyber SA is relevant to any cyber threat situation and arguably important for individuals at all levels of management in affected organizations (Sharkov, 2016; Varga et al., 2018), albeit at varying degrees, Ofte and Katsikas (2023) conducted a systematic review to further

understand SA in the specific context of SOCs. They reported ongoing theoretical debate regarding how to understand SA within the context of SOCs, partly inferred from authors using several definitions for SA that included teams, systems, technology, mental states, and general consciousness (Ofte & Katsikas, 2023). Of important note was the notion that studies argued for the importance of SA in SOCs without defining how they understood SA. The largest issue, however, was the finding that there appear to be no standardized and reliable way of measuring SA in SOCs, thus, there is no reliable data to infer whether SA in SOCs is relevant for cyber defense decision-making (Gutzwiller et al., 2020; Ofte & Katsikas, 2023). These findings align with the reported lack of general performance metrics for SOC team analysts (Agyepong et al., 2019). Developing and validating questionnaires for measuring SA in SOC teams is subject to ongoing investigation (Gutzwiller et al., 2016; Lif et al., 2017, 2018, 2020).

3.2. Measuring Cyber Situational Awareness

Two notable efforts to develop measurements of cyber SA have been those by Gutzwiller and colleagues (2016) and Lif and Colleagues (2017, 2018, 2020). Gutzwiller and colleagues (2016) performed a cognitive task analysis to identify goals and abstract awareness elements that cyber analysts associated with network defense. This served as the foundation for planned experiments to establish a measure of cyber SA. Lif and Colleagues (2017) went further in developing a questionnaire to measure cyber SA in analysts and scouts. In subsequent research, they have shown that when teams incorporate answers to the questionnaire in their incident reports during CDXs, their reports receive higher independent quality ratings (Lif et al., 2018). The perceived relevance of the questionnaire, however, when rated by participants on a scale from 0 (low) to 7 (high) is 4.3 (Lif et al., 2018) and 4.1 (Lif et al., 2020). Thus, this cyber SA questionnaire is still being developed and validated (2017, 2018, 2020). Because there is a lack of performance metrics for cyber analysts (Agyepong et al., 2019), the work presented in this thesis uses the questionnaire developed by Lif and colleagues (2017) as a measure of cyber SA in paper II, while the measure of SA in paper III is partly inspired by the questionnaire by (Lif et al., 2017). Some of the questions in the questionnaire include high-level evaluation of situational elements (e.g., evaluating the impact of the attack), which is in line with the information needs of individuals higher up in the decision-making hierarchy (Staheli et al., 2016; Tinde, 2022).

Several methods have been proposed to measure subjective and objective SA in individuals and in teams (Endsley, 2020; Ofte & Katsikas, 2023; Salmon et al., 2008). The most

well-established method for measuring SA in research and education settings is the Situation Awareness Global Assessment Technique (SAGAT) proposed by Endsley (1995). The SAGAT is based on the freeze technique, which entails simulated tasks and scenarios being frozen and system displays being blanked at multiple random times, upon which participants are prompted to answer expert-formulated questions probing their situational perceptions (Endsley, 1995). A major strength of the SAGAT is that the multiple and random measurements allow for the direct measurement of SA under both high and low workloads and without biases related to having to rely on long-term memory at the end of a demanding exercise (Endsley, 2021). Another promising and direct measure of SA is the Situation Present Assessment Technique (SPAM; Durso et al., 1998). The SPAM method relies on real-time probing, where individuals are queried while carrying out ongoing operational tasks, and their time to respond is collected as an indicator of how available the situational information is (Durso et al., 1998). A recent meta-analysis (Endsley, 2021) compared the SAGAT and SPAM method, and while both methods performed equally well in predicting performance, the SAGAT method was considerably more sensitive with respect to detecting changes in SA following experimental manipulation (Endsley, 2021). Due to constraints related to the allotted time points for when we could carry out measurements during the cybersecurity exercise in paper II, and time constraints related to the execution of the experiment in paper III, including the SAGAT as a measure of SA in the thesis research was infeasible. Instead, the SA measures included in this thesis were based on the work of Lif and colleagues (2017). The cyber SA questionnaire does not employ real-time or direct probing, which means that any responses to the questionnaire items are biased by long-term memory processes.

3.3. Communication in Cyber Threat Situations

As noted in chapters 2.1, communication problems are one of the main challenges faced by SOC team analysts (Agyepong et al., 2019). At the individual and team level, SOC team analysts face several challenges that cannot be considered in isolation (Agyepong et al., 2019). When considering the SA model (Endsley, 1988), one can begin to speculate how dealing with a high number of alarms can influence communication of cyber threat information for shared SA (Agyepong et al., 2019). Findings from a small handful of studies go some way in answering these questions (Brilingaitė et al., 2022; Champion et al., 2012; Jariwala et al., 2012). The findings of these studies (with the exception of Brilingaitė et al., 2022) are addressed in Chapter 5.1. Some of the key findings will be summarized here albeit briefly to

avoid repetition. The studies either interviewed experts (Champion et al., 2012), observed cyber cadets and junior specialists participating in CDXs (Brilingaitė et al., 2022; Champion et al., 2012; Jariwala et al., 2012), or conducted studies assessing the relationship between cognitive load, communication, and SA (Champion et al., 2012).

Some of the main findings were that cyber operators experienced having to switch between several tasks thus not being able to focus on a single task (Brilingaitė et al., 2022). They experienced role ambiguity leading team members to work the same tasks such as monitoring same network without knowing. Intra-team communication issues were common (Brilingaitė et al., 2022; Champion et al., 2012) due to team communication and collaboration not being fostered (Champion et al., 2012; Jariwala et al., 2012). Communication breakdowns, for example due to cognitive load from a high number of security alerts, which appears to be related to reduced SA in teams (Champion et al., 2012) and a bias towards focusing on technical tasks rather than reporting activities (Brilingaitė et al., 2022). Efficient team communication and collaboration appeared to separate teams who performed well from those who did not despite using the same strategies at the technical level (Jariwala et al., 2012). Other issues included the challenges of team leaders having to collect pieces of SA information from several team members and not having adequate technical-level knowledge to fully understand cyber threat information (Brilingaitė et al., 2022).

This problem is expected to be more pronounced when communication occurs between individuals at various levels in a SOC (Knox et al., 2018; Jøsok et al., 2016). This can be problematic because individuals at lower levels performing the analytical work are the ones with the most technical competence, while individuals at higher levels are the ones making decisions based on what they understand from the information they receive from lower levels. Consequently, critical cyber threat information may be lost as information is relayed between individuals at ascending levels in an organization. Thus, the pieces of cyber threat information that is communicated must convey critical information but also be appropriate for the technical background of the recipient to create an accurate and meaningful picture of the recognized cyber threat.

The prioritized courses of actions of strategic-level management during a potential cyber threat situation includes more than those just directly dealing with the threat actor. Recent work indicates that strategic-level decision-makers are interested in information about organizational assets, cyber threat impact, implemented and required measures, and adversarial motivations

and objectives but not technical information (Tinde, 2022). In other words, high-level SA information, which is in line with the filtering processes described in (Jøsok et al., 2017; Staheli et al., 2016). Implicit and explicit knowledge about the relative weighting of these priorities may affect how information is presented to management but also how it is received (or processed). It may also be reflected in how (un)receptive executive management is to cyber threat information (Oltsik, 2019).

3.4. The Relationship Between Information Sharing and SA in Military Operations

Buchler and colleagues (2016) wanted to investigate the idea from Network-Enabled Operations framework that 'more is more' when it comes to information sharing for SA in military operations (Alberts & Garstka, 2004). During a 2-week military exercise, communication data was collected from an entire Coalition Joint Task Force organization, which consisted mostly of telephone and email communications. The initial dataset consisted of an email network of "213 mission command staff members and 19168 correspondences", and a telephone network of "3191 calls between 132 mission command staff members." (Buchler et al., 2016; pp. 4). They reduced this data to the email network of the three core units of the Coalition Joint Task Force organization, which was the Mission Command staff of a U.S. Division and two participating sub-ordinate Brigades. They performed social network analysis on the email data to visualize the network as nodes connected by directed and undirected edges and centralize hubs in the network (Buchler et al., 2016). They used the SAGAT (Endsley, 1995) to measure individual SA during the exercise. While the exercise did not have a specific focus on cybersecurity, SAGAT questions included at least one item asking about awareness of cyberattacks against Coalition operations. During the second week of the exercise, it was found that individuals whose connections with the network were characterized by higher propensity to receive emails, and a lower propensity to send emails, had higher SA (Buchler et al., 2016). In other words, "passive" recipients of emails had higher SA than those who actively communicated with other staff. They also found that individuals with large differences in SA were less likely to form connections with each other (Buchler et al., 2016). The authors offered some explanations for their results, for example that sending emails diverted attentional resources away from SA building or that the operational environment was incompatible with human cognitive abilities.

3.5. The Hybrid Space Framework and Team Coordination and Communication

Recognizing that military personnel face challenges spanning "social, cyber, and physical domains", the Hybrid Space framework (Figure 4a; Jøsok et al., 2016) was proposed to illustrate the cognitive agility required by the high demand for mental context shifting in defensive cyber operations (Knox et al., 2017; Figure 4b). The "hybrid" part of the framework is in reference to the interconnectedness between the cyber and the physical domains, juxtaposed along the horizontal axis in Figure 4a. This juxtaposition indicates how an individual may be focused on assets and actions in cyber or physical domains depending on where the orientation of their mental focus falls along the horizontal axis (Jøsok et al., 2016). Along the vertical axis, tactical, operational, and strategic military command levels are captured to convey "*the tension between tactical and strategic goals in decision making and action*" (Jøsok et al., 2016, pp. 180). Together, the horizontal and the vertical axes illustrate the converging complexities associated with the interrelatedness of assets and decision-making in cyber-physical systems, where each quadrant in the hybrid space represents a potential cognitive location (or mental focus), associated with their own sets of tasks and priorities, communication needs, and challenges (Jøsok et al., 2016).

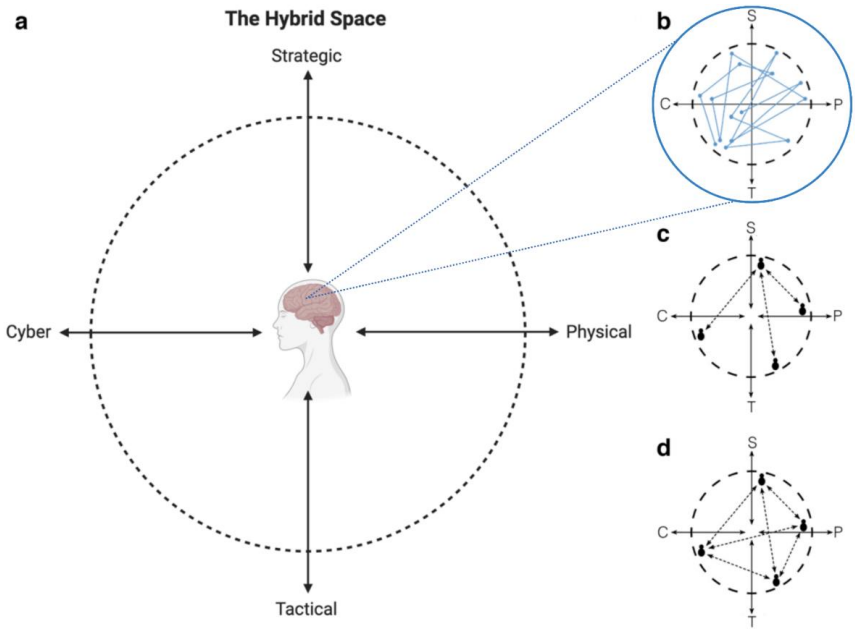

Figure 4. The Hybrid Space framework.

a The Hybrid Space framework (Jøsok et al., 2016, 2017). b Cognitive agility. c Hierarchical structure, complicated relations. d Hierarchical structure, complex relations. C = Cyber. S = Strategic. P = Physical. T = Tactical. Figure adapted from Ask et al. (2021).

Due to the interconnectedness between assets and decision-making agents in cyber and physical domains (Jøsok et al., 2016), team members are often located across the hybrid space to cover the entire operational context (Knox et al., 2018). This inevitably results in a need for team coordination and communication across hybrid space. In a team with individually distributed workloads and responsibility across the hybrid space, the individual holding the leader position establishes lines of communication to aggregate pieces of information into higher levels of understanding (McChrystal et al., 2016). Hierarchical organizational and communication structures are typical in SOCs (Staheli et al., 2016) but can have a negative impact on communication in cyber operative contexts when information is relayed between individuals across the hybrid space (Jøsok et al., 2017). In a large team where individual team members are allowed more singular focus, the leader has to readjust their mental focus each time they communicate with a new team member to ensure efficient communication (Jøsok et al., 2017). The more distributed the fragmented pieces of information are, the more challenging this communication process is (Brilingaitė et al., 2022).

In a small team, individuals often need to take on more roles than one, meaning constant mental context shifting due to shifting tasks and priorities, which is draining and detrimental to communication (Brilingaitė et al., 2022). Two communication partners can therefore have both different and shifting priorities according to their current roles, thus be in different quadrants of the hybrid (head) space each time they communicate with each other. This could potentially mean that they would have to spend cognitive resources shifting priorities away from the task they are currently engaged in and re-engage in the task they were previously engaged in during their last point of contact in order to adjust communication for efficient sharing of information (Knox et al., 2018). The complexity of the challenges associated with hierarchical communication, and communication between individuals changing positions in the hybrid space are depicted in Figure 4c and Figure 4d, respectively (Jøsok et al., 2017). Being explicitly aware of challenges associated with socio-cognitive distance in the hybrid space may thus be necessary to sufficiently manage the resulting socio-cognitive demands and to ensure effective communication.

3.6. The Role of Metacognition for Hybrid Space Movements and Cognitive Agility

It has been hypothesized that knowing where you are (where your mental focus is) in the hybrid space requires metacognition (Jøsok et al., 2016; Knox et al., 2018). When cyber operators have to switch between tasks in the cyber and physical domains (Brilingaitė et al., 2022; Gutzwiller et al., 2015), and it requires communication and coordination between individuals across the hybrid space (Jøsok et al., 2016, 2017), then noticing that communication issues are arising due to communication partners being located in different quadrants of the hybrid space is proposed to be achieved through metacognitive awareness (Knox et al., 2018). Hybrid space-related communication issues could manifest as discrepancies in technical understanding (e.g., between a cyber analyst and a decision-maker during RCP communication) or differing information needs due to having different priorities (Jøsok et al., 2016). Overcoming discrepancies requires exerting cognitive effort to calibrate communication style and content (Knox et al., 2018). If several individuals are communicating across hybrid space, it will require constant recalibration of style and content of communication to facilitate efficient sharing of information (Jøsok et al., 2017; Knox et al., 2018). This can be critical to performance during cyber threat situations with high stakes and high time-pressure.

It is cognitively demanding to move across the strategic-tactical and cyber-physical dimensions of hybrid space when adapting to the dynamics of cyber, social, and physical domains (Jøsok et al., 2016). To make these movements in a flexible and deliberate manner requires metacognitive skills (Jøsok et al., 2019; Knox et al., 2017, 2018). The ability to make skillful and flexible transitions between quadrants of the hybrid space by engaging in metacognitive knowledge and control processes is referred to as cognitive agility (Figure 4b; Knox et al., 2017). Because metacognitive awareness and metacognitive control is suggested to be required for flexible hybrid space movements, metacognition and self-regulation have been included in the cognitive agility construct in cyber operative contexts (Jøsok et al., 2019; Knox et al., 2017). There are few studies on cognitive agility as it relates to hybrid space movements in cybersecurity contexts and findings show mixed results.

A series of studies (Jøsok et al., 2019; Knox et al., 2017; Lugo et al., 2017) assessed the relationship between metacognitive awareness, metacognitive self-regulation (Jøsok et al., 2019; Knox et al., 2017), team workload demands (Lugo et al., 2017), and cognitive agility. The latter operationalized as self-reported movements in hybrid space during a CDX (Knox et

al., 2017). Metacognitive awareness and metacognitive self-regulation were indicated by scores on the metacognitive awareness inventory (Schraw & Dennison, 1994) and self-regulation questionnaire (Brown et al., 1999), respectively. Workload demands in team tasks were assessed with the team workload questionnaire (Sellers et al, 2014). Mostly zero findings were reported for metacognitive awareness and metacognitive self-regulation when measuring self-reported hybrid space movements during the last day of a CDX ($N = 31$; Knox et al., 2017). However, significant relationships were found for hybrid space movements and self-regulation when measuring hybrid space movements over four days of a CDX in a slightly smaller sample ($N = 23$; Jøsok et al., 2019). Hybrid space movements were also associated with communication and coordination demands but restricted by team dissatisfaction, demands for sharing time between tasks and teamwork, and by demands for monitoring own and team performance ($N = 31$; Lugo et al., 2017).

The relationship between metacognition and cyber SA in cybersecurity contexts is mostly unexplored. However, cyber SA generation and RCP communications necessarily start with detecting cyber threats. Individuals working in cybersecurity are more overconfident in their ability to detect deepfakes than non-professionals even though they are not better at detecting them (Sütterlin et al., 2022), suggesting a role for cognitive and perceptual processes in deepfake detection rather than professional background. Furthermore, a recent meta-analysis (Endsley, 2020) suggested that metacognitive judgements of one's own SA (measured as confidence ratings in SA) is partly responsible for the divergence between objective and subjective SA. Identifying that there is a need to communicate to improve, establish, or share SA may be dependent on how confident an individual is in their current understanding of the situation. This confidence may be reliant on an individual's "*insight into their ability to monitor and understand key information in a situation*" (Endsley, 2020; pp. 2).

Good and Yeganeh (2012) suggest that engaging in metacognitive processes will improve cognitive agility. As communication and coordination is necessary for SA building (Brilingaitė et al., 2022; Champion et al., 2012) and movements across the cyber-physical and strategic-tactical axes of the hybrid space (Lugo et al., 2017), engaging in metacognitive processes to facilitate efficient coordination and communication may improve cognitive agility for RCP communication and SA sharing (Knox et al., 2018).

3.7. Measuring Metacognition and Cognitive Agility

There are several ways of measuring metacognition and overconfidence (Fleur et al., 2021). Metacognition can be measured with self-report using the metacognitive awareness inventory (Schraw & Dennison, 1994) and behavioral measures where participants make prospective or retrospective performance judgements (Fleming & Lau, 2014; Fleur et al., 2021). For measuring metacognition with retrospective performance judgments, the most commonly used method is the receiver operating curve and meta-d′ (Fleming & Lau, 2014) derived from signal detection theory (Galvin et al., 2003). Such static measures do not account for the influence of dynamic situations that require evidence accumulation (Desender et al., 2022). Overconfidence is by definition an overestimation of knowledge and/or abilities, thus a product of poor metacognitive abilities and can therefore be measured using the same prospective and retrospective performance judgements used to measure metacognition. It can also be measured by overclaiming, which measures overconfidence by the extent to which individuals claim to have knowledge about bogus items on a questionnaire (Paulhus et al., 2003). There is, however, no standardized way of measuring metacognition and overconfidence in dynamic settings.

In paper II, metacognitive awareness was operationalized as prospective performance judgments controlled for actual performance using a formula described in (Meessen et al., 2018). The formula quantifies the deviation between expected performance (rated from 0 to 100%) and percentage of correct answers. To do this, the combined score on SA variables that were either correct (1) or incorrect (0) are converted to a scale ranging from 0 to 100. Prospective metacognitive judgments were selected based on their likely influence on how individuals perceive the need for planning, controlling, and monitoring behaviors (e.g., information processing, learning, communicating), the dependence on prospective metacognitive judgments on a part of the brain called the dorsolateral prefrontal cortex (Fleur et al., 2021; Vaccaro & Fleming, 2018), a brain area associated with vagal tone (Schmaußer et al., 2022), and previously reported associations between prospective metacognitive judgments and vagal tone (Meessen et al., 2018).

3.8. The Orient, Locate, and Bridge (OLB) Model

One of the challenges of communicating in cybersecurity is the distance in priorities and technical competencies between cyber operators and decision-makers in the SOC hierarchy. To combat communication difficulties resulting from individual differences, Knox and colleagues

(2018) proposed the Orient, Locate, and Bridge (OLB) model (Figure 5). The model is designed to be a pedagogical tool to teach cyber operators and other operative personnel science-based skills for efficient communication in safety-critical environments (Knox et al., 2018). By following the process outlined in the model, a bridging of communication between individuals located in different quadrants of the hybrid space is facilitated to reduce errors from miscommunication of critical information. In a cybersecurity context, this can mean successful communication of cyber threat information to achieve a shared SA. The OLB model consists of three inter-dependent and successive phases, each consisting of applying a set of metacognitive and socio-cognitive self-regulated processes (Knox et al., 2018).

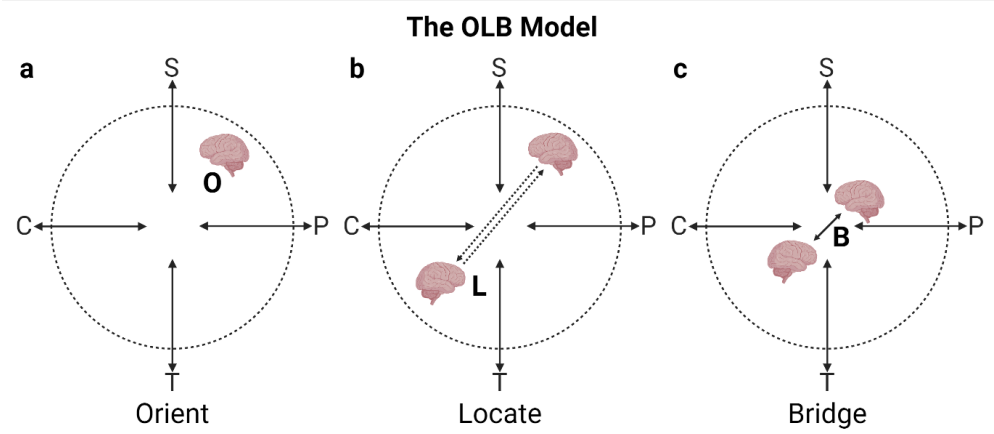

Figure 5. The Orient, Locate, and Bridge model (Knox et al., 2018).

a Orient. b Locate. c Bridge. C = Cyber. S = Strategic. P = Physical. T = Tactical. Figure adapted from Ask et al. (2021).

The first phase of the OLB process is the orienting phase (Figure 5a), which entails applying metacognitive awareness to get an overview of the "factors influencing one's momentary mental state and ongoing cognitive processes" (Knox et al., 2018; pp. 353). This includes determining one's own location in hybrid space, examining the content of one's own SA and how it is organized in knowledge structures. This can include (but is not limited to) assessing the quality or uncertainty of the evidence supporting the SA (knowing what you know or do not know; Endsley, 2020), and whether connections seen between situational elements are based on observable facts, gut-feelings, or previous experience. It may also include becoming aware of the (technical) knowledge that is prerequisite to understand the details of the SA or which pieces of information are the most salient or carry the most information (Knox et al.,

2018). Thus, orienting entails metacognitive processes for monitoring and controlling cognition along the cyber-physical and strategic-tactical dimensions of the hybrid space. Knox and colleagues (2018) provide an example of a cyber operator preparing an RCP brief for senior non-technical personnel.

> "*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*" (Knox et al., 2018; pp. 353).

The second phase of the OLB process is the locating phase (Figure 5b), which entails locating the communication partner in hybrid space and factors that can influence how they process information (Knox et al., 2018). This could include their expertise, information needs, workload, and goals. For instance, the level of technical or foundational knowledge of the communication partner may influence their ability to comprehend the communicated information. Similarly, a stressed communication partner that is operating with a hierarchy of priorities and is under a lot of time pressure, may not be receptive to the information if it is not a top priority. This could mean that they will forget it or dismiss it in order to not lose track of their main priorities. The locating phase is reliant on perspective taking (or theory of mind), which is the tendency and ability to adopt other people's point of view, reason about their mental states, and understand how they may differ from our own (Birch et al., 2017). This is crucial during communication as the context from which individuals are communicating will influence how they perceive and process language (Smirnov et al., 2014; Willems & Peelen, 2021). Thus, perspective taking during the locating phase allows the individual to notice if their communication partner's focus is in a different quadrant of the hybrid space than themselves (thus being in a different context mentally), and then use that information to make inferences about how they process information.

The third and final phase of the OLB model is the bridging phase (Figure 5c), which is where the content and style of communication is adapted to facilitate the co-construction of a shared situational model (Knox et al., 2018). After having used metacognition to locate their own position in hybrid space (orienting phase) and used perspective taking to locate the communication partner's position in hybrid space (locating phase), the process of bridging the gap can be initiated based on the perceived relative distance. This will entail establishing the

form that information should be presented in and at what level of detail, the tolerance for uncertainty, the openness to admit need for clarification and simplification, and so on (Knox et al., 2018). While the three phases are executed in succession, the dynamics of the situation may change resulting in communication partners changing their position along the tactical-strategic and cyber-physical axes according to changing goals and priorities. Thus, being able to flexibly transition between phases when noticing that one's own or the partner's context has changed, and to rapidly self-correct communication style during face-to-face communication is crucial to optimize OLB efficiency. In a sense, the OLB model applies the principles of cognitive agility in hybrid space in a practical and pedagogical framework for RCP communication.

3.9. Measuring OLB processes and RCP communication

The OLB model is a pedagogical framework for improving communication that has yet to be validated. Measuring the extent to which individuals spontaneously engage in OLB processes will necessarily require probing into their internal states during or after communication or make inferences based on observable communication behaviors. This thesis approached this through structured observations noting the frequency of verbal communication behaviors that explicit attempted to ground communication and engage in perspective taking.

RCPs are tailored to reflect the information that specific recipients require in order to make actionable judgments (Varga et al., 2018; Ahrend et al., 2016; Tinde, 2022). This thesis approached the measuring of RCPs by having participants provide short situational reports in response to an open-ended questionnaire used in paper III. The items were based on general knowledge about the information needs of non/less-technical decision-makers (Staheli et al., 2016; Tinde, 2022), which included instructions and questions such as "Describe the activity you saw (specific but not overly detailed), "What type of incident do you think it was?", and "If you could suggest anything, which actions should be done?".

In the following subsections, we will have a brief look at some neuroergonomic approaches that may have relevance for measuring and predicting information processing and communication in cyber teams.

3.10. Wearable Technology as an Approach to Neuroergonomics

Since Parasuraman's initial paper (2003), neuroergonomics has grown as a field and there are several methods that can be applied depending on the field and domain of study (Ayaz & Dehais, 2019). Some of the neuroergonomic methods that have received a lot of focus in the

literature are based on electromagnetic and hemodynamic neuroimaging techniques (Ayaz & Dehais, 2019; Parasuraman, 2011). While monitoring the brain activity of cyber operators in operational contexts would certainly make for an interesting proposition, applying neuroimaging techniques in the naturalistic setting of the cybersecurity exercise in paper II and the experiment in paper III was infeasible. Neuroimaging techniques usually put a lot of restrictions on participants with respect to test environment and movement. In the most restrictive cases (e.g., functional magnetic resonance imaging), participants are completely immobile, and the test environment is limited to what can be shown on a screen, heard through a speaker, or be visualized using XR. In the least restrictive cases (e.g., electroencephalography), the spatial resolution of the recordings is low, and the measurement systems are usually sensitive to movement artifacts which make them methodologically challenging to implement in operative contexts where there is a lot of movement. Furthermore, while applying neuroimaging techniques in research may provide actionable insight into performance-related brain dynamics during cyber operations, it still raises the question about how the use of neuroimaging systems is transferrable to the everyday contexts of cyber analysts. The implementation of the systems may be impracticable due to factors such as incompatibility with the working environment (e.g., imposing movement restrictions and need of physical space with respect to use and storage) or imposing a need for hiring a competent technician to operate the neuroimaging system. Thus, identifying other technologies that could be used to measure indicators of brain activity and where the findings are feasible to implement in a CDX, was of high importance for the thesis.

In the context of applied research and actionable contributions, *wearable technology* has increased in popularity in recent years as a type of technology with several performance-related use cases (Canali et al., 2022; Johnson & Picard, 2020). Wearable technologies constitute technologies such as sensor systems that can be worn on an individual's body to measure activities and parameters including biometrics related to neurophysiological activity (Canali et al., 2022; Johnson & Picard, 2020). The promise of these technologies is the relative ease to which they allow for combining contextual information (e.g., location) with multiple biosensor signals and analytics, thus allowing for a richer collection and interpretation of real-world data (Johnson & Picard, 2020). There is currently a lot of ongoing research on the use of wearable technology in military personnel and contexts (e.g., Hinde et al., 2021; Shi et al., 2019; Taylor et al., 2023, 2024), some of which include assessing the perceived comfort of wearing multiple sensors over multiple days of military training (Taylor et al., 2023), identifying devices suitable

for twenty-four-hour monitoring of autonomic nervous system activity (Hinde et al., 2021), fusing data from multiple wearable sensor sources (Shi et al., 2019), and using information from wearable sensors about operator fatigue to enhance personnel-directed decision-making (Taylor et al., 2024). Research where findings can be implemented through the use of wearable technology is therefore a promising area to focus neuroergonomic efforts, at least from the perspective of national cybersecurity, as there is already a trend towards adopting and implementing this group of technologies in military personnel. Furthermore, if research and findings are focused on analyzing sensor signals that are already being collected, it is simply a matter of performing an additional analysis on the signal at worst (if specific metrics need to be quantified), and at best, making decisions based on analyses that are already being conducted (if they relate to the interpretation of the output of transformations that are already being performed). Because the analytical and communicative performance of cyber analysts working in teams is influenced by the high stress and cognitive load associated with their working-environments (e.g., Champion et al., 2012; Greenlee et al., 2016), measuring peripheral signals related to how the brain regulates physiological arousal in stressful working-environments is likely to provide neurophysiological indicators of high relevance to cyber team performance. One such measure is vagally mediated heart rate variability (vmHRV), which is considered an indicator of an individual psychophysiological adaptive ability (Appelhans & Luecken, 2006).

3.11. Vagally Mediated Heart Rate Variability (vmHRV) as a Neuroergonomic Approach to Cyber Analyst Performance Metrics

Previous research has suggested that vmHRV is a relevant performance indicator for operative personnel in both military and civil contexts (Tomes et al., 2020). Assessing whether vmHRV is a relevant performance indicator for communication, SA, and metacognition in cybersecurity settings was unexplored prior to the work presented in this thesis. This possibility was, however, proposed in a previously published review with data article (Ask et al., 2021). The article highlighted how the relationship between physiological arousal and the neural substrates responsible for attentional control processes may be related to OLB-related processes, hybrid space movements, and cybersecurity-related analytical work, especially in emotionally demanding and stressful contexts (Ask et al., 2021).

On a neurological level, vmHRV reflects activity in one of the two main pathways through which cognitive and emotional stressors affect the organism which is via the

sympathetic branch of the autonomic nervous system (Marques et al., 2010). Thus, the ability of individuals to exert cognitive control at increasing levels of stress relates in part to the ability of the prefrontal cortex to modulate the level of arousal via the parasympathetic branch of the autonomic nervous system (Chand et al., 2020; Hansen et al., 2007, 2009; Hildebrandt et al., 2016; Kim et al., 2018; Magnon et al., 2022; Pu et al., 2010; Tomes et al., 2020). This is achieved through direct and indirect prefrontal influence on structures that constitute the central autonomic network (Schmaußer et al., 2022; Sklerov et al., 2019). The central autonomic network includes cortical, subcortical, and brainstem structures involved in adapting autonomic arousal to meet the demands of short-term and long-term stress (Benarroch, 1993; Gross, 1998).

During exposure to stress, the sympathetic branch of the autonomic nervous system increases activity in all organs including the heart, reflected in increased heart rate, while the parasympathetic branch of the autonomic nervous system decreases activity in organs (McCorry, 2007). The vagal branch of the parasympathetic nervous system (the vagus nerve) carries three quarters of all parasympathetic nerve fibers and is responsible for down-regulating activity in the organs of the abdomen and thorax such as the heart (McCorry, 2007). The excitatory influence of the sympathetic nervous system on heart rate is mediated by the neurotransmitter noradrenaline, while the inhibitory influence of the vagus nerve on the heart is mediated by the neurotransmitter acetylcholine. Due to the peak effect of acetylcholine on the heart arriving faster than that of noradrenaline, the resulting oscillations in heart rate following sympathetic and vagal input occur at different speeds (Berntson et al., 1997). Increased heart rate could result from increased sympathetic activity or vagal withdrawal, although in conscious animals these processes occur concomitantly (Pagani et al., 1982). Parasympathetic input to the heart is dominant at rest and keeps the heart beating at a pace that is lower than the intrinsic firing rate of the neurons of its pacemaker. Thus, an individual's ability to rapidly adapt arousal and emotional responses to changing contextual demands depends on the parasympathetic nervous system (Berntson et al., 1997) and the ability and capacity of the prefrontal cortex to exert influence on it via the central autonomic network (Appelhans & Luecken, 2006; Schmaußer et al., 2022; Thayer & Lane, 2009). A higher prefrontal capacity for exerting influence on the vagal branch of parasympathetic nervous systems translates to better psychophysiological adaptive ability and a higher capacity for initiating flexible responses to environmental stressors (Appelhans & Luecken, 2006).

Vagal activity and vagal influences on the heart is often referred to as vagal tone and can be quantified as vmHRV, which refers to the beat-to-beat variations in heart rate resulting from vagal input (Figure 6; Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology, 1996). When measured at rest, vmHRV is considered an index for an individual's psychophysiological adaptive ability (Appelhans & Luecken, 2006). High vmHRV at rest means low heart rate and high psychophysiological adaptive ability, while low vmHRV at rest means high heart rate and lower psychophysiological adaptive ability.

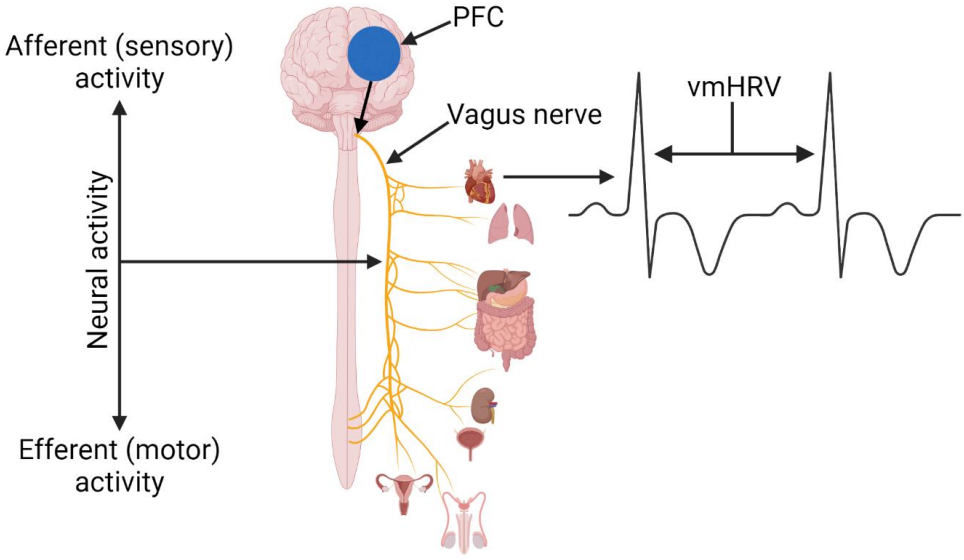

Figure 6. Prefrontal cortex and vmHRV.

Figure depicting the difference between afferent and efferent vagal activity, and the relationship between prefrontal input to the vagus nerve and the resulting influence on heart rate (figure adapted from Firth et al., 2022). PFC = Prefrontal cortex. vmHRV = vagally mediated heart rate variability.

A growing body of converging evidence links vagal tone to activity in neural structures and networks (Schmaußer et al., 2022; Chand et al., 2020) relevant for flexibly coordinating cognitive control processes (Badre & Nee, 2018; Cocchi et al., 2013, 2014; Cole et al., 2012; Duncan, 2013; Kim et al., 2011; Menon & D'Esposito, 2022; Nee, 2021; Nee & D'Esposito, 2016; Milardi et al., 2015; Panikratova et al., 2020; Torgerson et al., 2015), metacognition (Boldt & Gilbert, 2022; Fleur et al., 2012), self-regulation (Hare et al., 2009; Kelley et al.,

2019; Paschke et al., 2016; Schmidt et al., 2018), and connectivity between brain networks responsible for allocating attention towards external and internal processes (Chang & Glover, 2009; Chen et al., 2013; Fox et al., 2005; Liston et al., 2014; Raichle et al., 2001). Vagal tone has also been associated with attentional control (e.g, Blaser et al., 2023), metacognition (Meessen et al., 2018; Stuyck et al., 2023), and cognitive flexibility (Hildebrandt et al., 2016; Magnon et al., 2022). This data further suggests that vagal tone, indicated by vmHRV, could be a relevant indicator for cyber operator's ability to navigate the complexity of the information environment and subsequently efficiently communicate cyber threat information.

3.12. Measuring vmHRV

While the specific method for measuring the inter-beat-intervals used to quantify vmHRV in the present study was not a wearable technology, there are a number of wearable technologies that allow for quantification of vmHRV (Hinde et al., 2021). Thus, any findings related to the measurement of vmHRV in the present thesis are in a practical sense transferrable to wearable technologies. In study II where inter-beat-intervals were measured to quantify vmHRV, recordings were conducted two days prior to the CDX starting, thus, recordings were not directly influenced by the stress of the exercise. Consequently, associations between vmHRV and measures conducted during the exercise were more likely to reflect trait-related processes than situational dynamics of the exercise (if measures were influenced by anticipatory stress related to the exercise, then that is stress occurring while being removed from the situation which may indicate trait-level processes).

3.13. Mood-Congruent Processing

Performing well under stress depends on an individual's ability to handle task-dependent cognitive load under varying levels of stress. A practical example of this may include coordinating the engagement in analytical activities with effective communication and collaboration behaviors when the number of security alerts are increasing (Champion et al., 2012). The experience of stress can be positive or negative. Negative stress is an emotional experience, where the level of actual and perceived arousal induced in response to stress together with the level of perceived negative valence constitute the intensity of the emotional response (Goto & Schaefer, 2017).

Stress can have both short and long-lasting emotional influences on an individual, which in turn has consequences for how the brain perceives, interprets, interacts with, and remembers

information and other elements of the environment (Clore & Huntsinger, 2007; Faul & LaBar, 2023). Emotional responses can influence information processing through modulation of endogenous attention or shift towards exogenously (stimulus-) driven attention (Okon-Singer et al., 2015; Mohanty & Sussman, 2013). Endogenous attention refers to the top-down control of attentional processing and is more goal-directed compared to stimulus-driven attention, which is directed by bottom-up sensory processes (Okon-Singer et al., 2015).

One interesting information processing phenomenon resulting from emotional responses is mood-congruent processing, where stimuli are processed according to the current mood (Forgas, 2017; Tamir & Robinson, 2007). For instance, if an individual is in a good mood, they may focus on the positive aspects of a situation (e.g., what they have achieved) rather than the problems (e.g., unsolved tasks or unanswered questions), or downplay the likelihood of negative future outcomes (Dawson, 2023; Paul & Pourtois, 2017). Conversely, if an individual is in a negative mood, they may focus on problems rather than what is positive about the situation, resulting in less risky decision-making (Gambetti & Giusberti, 2012). Mood-congruent processing is a form of goal-directed information processing that is emotionally driven. The "correct" way to process stimuli is context-dependent, and if mood-congruent processing occurs in an inflexible manner that is hard to regulate, it becomes maladaptive (Koster et al., 2005). A mood-induced processing bias may result in allocating more attention to task-relevant emotional stimuli at the expense of task-relevant non-emotional stimuli or emotional stimuli corresponding to the opposite mood.

Reducing the impact of stressors on emotional processes depends on the capacity and ability of an individual to regulate their emotions. Emotion regulation ability can be understood as being able to select and deploy conscious and subconscious emotion regulation strategies and processes (Gross, 1998; Silvers & Guassi Moreira, 2019). Emotion regulation capacity can be understood as the volume (or level) of stress an individual can endure before they are unable to cope or adapt to the situation (Silvers & Guassi Moreira, 2019). There are several strategies for regulating emotions. Two of the most researched strategies are cognitive reappraisal and expressive suppression. Cognitive reappraisal is a flexible, goal-directed and antecedent-focused metacognitive strategy that modifies the emotional impact of a situation by changing how it is processed (Gross, 1998; Ochsner et al., 2004). Expressive suppression is a response-focused strategy that aims to modify emotional responses by inhibiting the expression of them (Butler et al., 2003; Gonzalez-Escamilla et al., 2022). Other emotion regulation strategies are

situation selection, situation modification, and attentional deployment (Gross, 1998; Livingstone & Isaacowitz, 2015).

There are several stressors that can elicit emotional responses in the cybersecurity working-environment, including the high information load that cyber operators are subjected to combined with long working-hours, high situational uncertainty, and time-pressure (Champion et al., 2012; Chappelle et al., 2013; Greenlee et al., 2016; Jøsok et al., 2017). Thus, capacity for emotion regulation may have consequences for cyber operator performance across a number of challenges (Lugo & Sütterlin, 2018). As previously mentioned, the role of triage analyst is associated with high cognitive and temporal demand, increased distress, and reduced task engagement (Greenlee et al., 2016). Preliminary data from a pilot study on cyber cadets participating in a five-day CDX found associations between self-reported affect and self-reported team workload demands (Ask et al., 2021). Higher self-reported arousal was associated with higher demands for team performance monitoring, while variability in self-reported mood, arousal, and control (indicators of regulated affect and flexible moods) during the exercise was negatively associated with perceived demands for team performance monitoring, sharing time between tasks and teamwork, and demand for team support (Ask et al., 2021). Interoceptive accuracy has been found to moderate the relationship between situational self-efficacy and counterintuitive decision-making in cyber cadets (Lugo et al., 2016). Counterintuitive decision-making abilities are associated with reduced propensity for heuristic and biased decision-making (Campitelli & Labollita, 2010; Toplak et al., 2011). Situational self-efficacy was measured by cyber cadets making prospective affective performance judgements related to how positive they were about the task, how aroused they were in anticipation of the task, and how confident they felt (Lugo et al., 2016). The results suggested that individuals with high situational self-efficacy but low interoceptive accuracy were better at counterintuitive decision-making than individuals with high situational self-efficacy and high interoceptive accuracy. For individuals with low situational self-efficacy, however, higher interoceptive accuracy indicated slightly better counterintuitive decision-making than individuals with low situational self-efficacy and low interoceptive accuracy (Lugo et al., 2016). In the context of mood-congruent processing, high situational self-efficacy and accurate interoceptive abilities may suggest a biasing effect of positive emotions on expectations and information processing ("I feel good so I think I will do good"). Low accuracy in interoceptive abilities but high situational self-efficacy may reflect a biasing effect of

analytical (or metacognitive) judgements on situational appraisals versus ("I think I will do good, so I feel good").

3.14. Measuring Moods and Emotion Regulation

In the context of assessing vmHRV as a performance indicator related to navigating information environments associated with cybersecurity, it was of interest to assess its relationship with mood- and emotion-related processes during the CDX in paper II, and to assess the association between measures of mood and emotion-related processes and measures of metacognition and SA. Some alternative approaches are to measure daily self-reports on the deployment of emotion regulation strategies (e.g., using a variant of the emotion regulation questionnaire to measure cognitive reappraisal and expressive suppression; Gouveia et al., 2018), or conversely, daily assessments of how individuals perceive their emotional states by using an instrument such as the self-assessment manikin (Bradley & Lang, 1994). A number of studies have been conducted on the association between vagal tone and various forms of emotional processing (e.g., De Witte et al., 2016; Geisler et al., 2010; Koval et al., 2013; Kwon et al., 2022; Lande et al., 2023; Min et al., 2023; Osnes et al., 2023; Pinna & Edwards, 2020; Sütterlin et al., 2011; Volokhov & Demaree, 2010; Watanabe et al., 2023; Williams et al., 2015). The relationship between resting vagal tone and emotion regulation depends on the measure used to indicate emotion regulation. For instance, there is some variation in findings when emotion regulation difficulties or emotion regulation strategies are measured using self-report questionnaires at rest, although studies generally report a lack of association with vagal tone (De Witte et al., 2016; Koval et al., 2013; Kwon et al., 2022; Lande et al., 2023; Watanabe et al., 2023). There do appear to be gender differences with significant associations between vagal tone and emotion regulation difficulties for females (Kwon et al., 2022) and Asian Americans at lower levels of vagal tone (Watanabe et al., 2023), and between vagal tone and social support seeking subscales (in adolescents; De Witte et al., 2016). Significant negative associations between scores on the difficulties in emotion regulation questionnaire and vagal tone have been found when controlling for trait anxiety and rumination (Williams et al., 2015).

In behavioral studies, however, resting vagal tone is positively associated with more frequently using cognitive reappraisal in response to negative stimuli (Volokhov & Demaree, 2010), negatively associated with avoidance of negative stimuli (Aldao et al., 2016), daily positive affect (Schwerdtfeger & Gerteis, 2014), and negatively associated with self-reported daily instability of positive (but not negative) affect (Koval et al., 2013). Studies on gender

differences in emotion regulation and vagal tone found significant gender differences for the regulation of positive valence (Min et al., 2023). Vagal tone is negatively associated with framing effects on decision-making (Sütterlin et al., 2011), suggesting that higher vagal tone may be a marker for resilience against the induction of emotional responses that lead to mood-congruent processing.

Due to the interest in assessing the effect of specific moods on processes such as metacognition and SA, and because the association between emotional outcomes and vmHRV appears to be more clear than self-reported use of emotion regulation strategies, the self-assessment manikin was chosen as a measure in study II.

3.15. Multi-Sensory Integration: Encoding of Visual and Spatial Information in Extended Reality for Shared Mental Modelling of Cyber Threat Situations

A neuroergonomic approach that is alternative to direct or indirect measurements of neural activity is to design tools based on previous knowledge about how information is presented in the specific working-environment and knowledge about how the brain processes information that has previously been explored with neuroimaging (Parasuraman, 2003). This can form the basis for neuroergonomic interventions.

As a solution to the problems of presenting data on standard computer screens, Kullman and colleagues (2018) proposed using extended reality to visualize 3D representations of network topology during a cyberattack. Visualizations in extended reality may have multiple use cases in cybersecurity settings, such as training and offering novel ways of understanding cyber threat information (Payer & Trossbach, 2015; Zehnder et al., 2024, in press). The authors suggested that the 3D visualizations should be designed to match the task-specific mental models of cyber analysts, acknowledging that mental models may vary depending on tasks (Kullman et al., 2018). To allow flexibility in the representation of network data, they developed the Virtual Data Explorer (VDE; [https://coda.ee/vde]), a dedicated 3D environment with a platform that allows creating interactive (motion controlled) 3D data and exporting rendered stereoscopic images to VR, MR, and AR headsets such as Oculus and Microsoft's HoloLens (Kullman et al., 2018). The VDE can visualize network data (network traffic, IP addresses, their relations, connections, sessions, as well as application logs and process memory usage logs, and so on) as structures with static relationships (forensic evidence within a volume of time) and as live-wire data where the relationships change over time (Kullman et

al., 2018). Importantly, the VDE has the capacity to visualize very large datasets and allows for on-site (MR) and remote (VR) collaborative exploration of the visualized data. The authors define the treatment of data in VDE as the following:

- Dataset: values collected from sensors, log files, and network traffic monitors
- Data-object: one instance from the dataset consisting of a set of event-related values that induced a log-line or an alert.
- Data-shape: the specific form of visualization that organizes the pixels that represent data-objects in positions according to a logical topology that matches the task-specific mental model of the cyber analyst.
- VDE scene: the meta-shape of the combined set of data-shapes that are spatially positioned to convey the relationship between them (Kullman et al., 2018).

Examples of how VDE can visualize data are shown in Figure 7

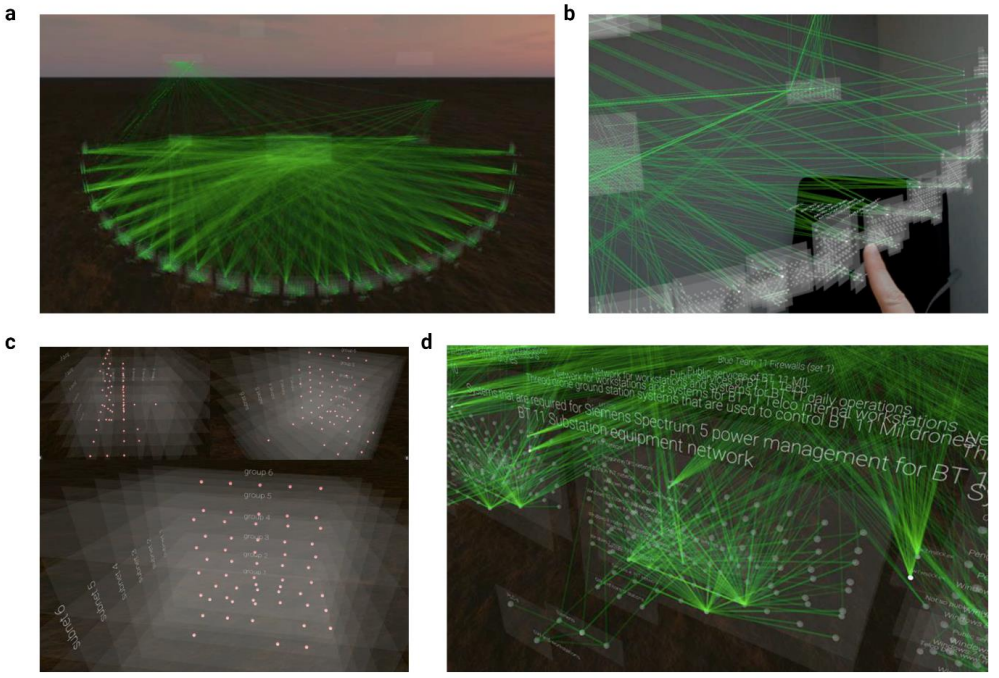

Figure 7. Visualization of network topography using the Virtual Data Explorer app.

a Full overview of the metashape of the actual network that was used during the NATO CCDCOE 2018 Locked Shields event as visualized in VR using the VDE app. b An individual interacting with the network topography in MR. c A close-up of nodes in the network from different angles and without the edges representing the connections between them. d A close-up of Blue Team nodes in the network with descriptive information and the edges that connect them. Adapted from (Kullman et al., 2019a).

Visualizing network data in AR and VR allows the organization of data values as visual real estate, where high-parameter data can be depicted as spatial structures (Kullman et al., 2018). Different variables are afforded different perceptual qualities thus allowing for inference of numerous relationships per unit of observation. This can include shapes and meta-shapes (the latter depicting the entire VDE scene or the hierarchical organization of a network into subnet segments such as organizations, departments, and so on), size, color, depth, distance, and brightness (Kullman et al., 2018). The spatial design allows the cyber analyst to explore the visualized data from different vantage points to better understand relationships, thus allowing for spatial reasoning about network intrusion data (Payer & Trossbach, 2015). For example, network entities can be positioned according to subnet and functional groups, in order of servers, network devices, and workstations that are distinguished by their operating system, allowing for intuitive inspection of suspicious activity in the network (Kullman et al., 2018). Motion controlled interaction with the data-shapes allows for intuitive manipulation of the visualization to explore the underlying dataset (Kullman et al., 2019a).

To investigate the perceived usefulness of VDE for cyber analysts, Kullman and colleagues (2019b) conducted semi-structured interviews with ten subject matter experts working as analysts (mean experience = 4.5 years) to sample their impressions. They used network traffic data from the 2018 NATO CCDCOE CDX Locked Shields to visualize forty minutes of network traffic in dynamic and interactive 2D and 3D representations (Kullman et al., 2019b). 2D visualizations were presented as radial diagrams of source addresses and destination addresses using Kibana [https://www.elastic.co/products/kibana] and as networks with nodes and edges in a force directed graph using Moloch (now known as Arkime; [https://arkime.com/]). 3D visualizations were presented using VDE and visualized in VR using the Oculus Rift headsets (Kullman et al., 2019b). Participants were first presented with a printed 2D diagram of the network, then asked which of the visualizations they would prefer to present the network, starting with the 2D visualizations and then the 3D visualization last. Seven of the participants stated using either Kibana or Excel to visualize network data (six were familiar with Kibana). There was a general preference among the participants for the 3D visualization, where most thought the visualizations made sense and found it useful for themselves and their teams (Kullman et al., 2019b). One participant explicitly expressed that the 3D visualizations matched how they would visualize “things”. Another participant

expressed that it would require adapting to not having to build this network representation in their mind, but that they could not understand why they still were using 2D representations with limited capability (Kullman et al., 2019b). Interestingly, one participant specifically addressed the VDE's potential usefulness in the transfer of knowledge (albeit in the context of training):

> "*Since I've been here for 4 years, I've trained about 80 people. I think if we'd have something like that from the start, it would change their whole perception of how to [think of networks] and jump start [their ability to work the networks].* [...]" (Kullman et al., 2019b; pp. 8).

The 3D visualizations should closely match the mental models of the individual end users and therefore not be developed independent of them (Kullman & Engel, 2022). To optimize the 3D visualizations for the analytical environment (e.g., malware analysis, network analysis, threat analysis) of the specific user, Kullman and colleagues (2020) suggest using semi-structured interviews to map the context-specific mental models of the analysts. The suggested interview is divided into two sessions. The first session is to understand the context in which the cyber analyst is working, what entities are part of the data they work with, and how they would organize those entities, procedural query processes and information needs, and so on. The second session would be the evaluation of the constructed 3D environment and its perceived usefulness (Kullman et al., 2020). It is important to note that the VDE is not a replacement for SIEMs, but an extra tool in the cyber operator's toolbox that is meant to aid them in developing their situational understanding and to facilitate communication of that understanding for shared SA.

The spatial navigation system is an intricate system that facilitates path integration through a combination of sensory and spatial memory processes (Moser et al., 2008). The spatial navigation system is involved in our procedural understanding of events as they occur in time and space via processes that facilitate episodic memory (Moser et al., 2015). Notable neural components of spatial navigation are place cells in the hippocampus (O'Keefe & Nadel, 1978) and grid cells in the entorhinal cortex (Fyhn et al., 2004; Hafting et al., 2005). The place cells in the hippocampus are individual cells that fire selectively for distinct environments (or places), hence their name (O'Keefe & Nadel, 1978). In essence, one place cell will fire for a specific football field when an individual enters that football field, thus contributing to its cognitive representation. Studies indicate that several non-spatial variables such as smells and

so on are encoded on top of place cells, suggesting how the brain may store event-related information according to where in space it happened (Moser et al., 2008). Grid cells in the entorhinal cortex consist of several cells whose firing pattern map the surface of a specific environment, and each cell will fire when the individual's position coincides with any vertex of a regular grid of equilateral triangles (hence their name), thus tracking an individual's movement across the environment (Doeller et al., 2010; Fyhn et al., 2004; Hafting et al., 2005). The entorhinal cortex is the major input structure to the hippocampus, serving as an interface between the hippocampus and neocortex (Witter et al., 2017). The entorhinal cortex is therefore the main candidate for integrating spatial (and non-spatial) multisensory information in navigation (Bilash et al., 2023; Hargreaves et al., 2005; Kerr et al., 2007; Witter et al., 2017). Grid fields persist after removal of prominent monuments, suggesting that the sensory input contributing to the maintenance and updating of grid fields is information about self-motion rather than visual cues related to stored knowledge about specific objects in the environment (Fyhn et al., 2007; Hafting et al., 2005). Signals of self-motion include optic flow, proprioception, and vestibular activity. Optic flow is the lawful (or predictable) movement of light reflected from objects in the environment across the retina as a result of self-motion (Niehorster et al., 2021). Proprioception is information from the position and movement of joints as well as the force exerted by muscles, signaling the body's position in space, as well as passive and active movement (Han et al., 2016). Vestibular activity comes from the vestibular organs, which are structures in the inner ear that generate signals in response to angular and linear acceleration. The vestibular organs provide information about head direction and speed of movement to the brain, thus serving as important contributor of non-visual cues to navigation (Jacob et al., 2014; Iggena et al., 2023; Yoder & Taube, 2014; Zwergal et al., 2024). In sum, these findings may suggest that 3D representations of network topology as outlined in (Kullman et al., 2018) may have an advantage over 2D representations by also leveraging neurocognitive mechanisms related to the encoding of spatial information in addition to visual encoding of objects.

Studies on VR navigation in humans have reported evidence of brain waves relevant for navigation, attention, learning, and memory (Bohbot et al., 2017; Ekstrom et al., 2005; Watrous et al., 2011, 2013). However, relatively recent findings show that brain waves are more similar to those during real-world navigation when participants are navigating in VR through self-ambulation (Bohbot et al., 2017) compared to stationary navigation in VR (Ekstrom et al., 2005; Watrous et al., 2011, 2013). This may suggest important contributions of self-motion

signals other than visual flow in extended reality-related navigation. How this relates to learning in healthy participants is not completely clear, however, and may be dependent on the specific environment (Iggena et al., 2023; Kuhrt et al., 2021). One study found that the availability of multisensory input during mobile VR navigation improved memory-guided navigation performance in both healthy humans and patients with hippocampal lesions when compared to stationary VR navigation (Iggena et al., 2023). The authors suggested that the multisensory input from the condition that included self-locomotion prevented the brain from having to devote resources to resolve conflicting sensory information. The ability of humans to generate mental representations of abstract space was assessed in a study where participants had to navigate an abstract environment consisting solely of a gradient of geometrical shapes (Kuhrt et al., 2021). Participants had to use their understanding of the space to decide the angle between two points, and to decide which of two positions were closest in space to a third position. Contrary to expectations, performance was not different between groups that did stationary versus mobile navigation (Kuhrt et al., 2021). The authors proposed that the lack of difference in performance between the groups could be due to the specific tasks being solvable by remembering the amount of specific geometrical shapes between points in the abstract space. Interestingly, participants were better at determining the angle between two points that were far away from each other rather than close, further suggesting that the amount of information between two points contributed to more accurate judgements of the relationship between them (Kuhrt et al., 2021).

In sum, 3D representations of network topology and activity may help in communication for shared cyber SA in several ways. It may solve scalability issues related to fitting large datasets in 2D representation by allowing for representing more network information, and more intuitive ways of understanding the relationships between the network information, than traditional methods for network traffic visualization (Kullman et al., 2019b). Generating a 3D environment may allow for spatial encoding of information and spatial reasoning about network information, which may provide an advantage over visually encoding information presented on a screen (Kuhrt et al., 2021; Kullman et al., 2018; Payer & Trossbach, 2015). If the visualized 3D environment is large enough to allow for self-ambulated roaming in between elements in the network, it may further enhance spatial encoding of information through mechanisms that leverage multisensory integration as opposed to stationary navigation (Bohbot et al., 2017; Iggena et al., 2023). If the visualized environment closely represents the mental models of cyber operators, it may reduce the effort needed to integrate cyber threat information

with how they understand the network (Kullman et al., 2018, 2020). Importantly, communication and shared mental models may be further influenced by the ability of cooperating dyads to point to object-shapes that encode relevant information, facilitating joint attention, which may help orienting and perspective taking processes outlined by the OLB model (Knox et al., 2018) or explain to each other what they are seeing.

In short, the VDE (Kullman et al., 2018) may serve as a potent tool for helping cooperating dyads build a shared mental model of how a cyber threat situation relates to their network and achieve shared cyber SA.

3.16. Chapter summary

The hybrid space framework (Jøsok et al., 2016) illustrates the interconnectedness between cyber and physical space, and the tensions between strategic and tactical priorities in decision-making and action. This furthers our understanding of the complex environment that cyber operators must navigate when investigating and communicating cyber threat information. While cognitive skills and processes involved in cognitive agility, including metacognition, attentional control, emotion regulation, and self-regulated behaviors have been suggested as important when navigating and communicating across this hybrid space (Jøsok et al., 2016, 2019; Knox et al., 2017, 2018), this remains to be validated against neurophysiological correlates and performance outcomes. This thesis addresses these previous limitations by utilizing vmHRV, a neurophysiological measure correlated with cognitive abilities relevant for cognitive agility to assess its relationship with measures of metacognition, communication, and cyber SA during a CDX. Emotional states and emotion regulation have also been suggested as relevant for information processing and collaboration in cyber teams (Ask et al., 2021; Lugo & Sütterlin, 2018) but this too have not been verified against performance outcomes during a CDX. Because the association between self-reported emotions appear to be more reliably associated with vmHRV than self-reported emotion regulation strategies, and because self-reported emotions provide more insight into what cyber operators are feeling, this thesis utilizes self-reported mood ratings (self-assessment manikin) during a CDX to assess the relationship between vmHRV and mood, and between mood, metacognition, and cyber SA. This allowed further assessing how mood influences information processing in cyber teams. Findings related to vmHRV will have implications for wearable sensor technology which can readily be utilized in cyber operative settings such as CDXs.

The research and technological development conducted by Kullman and colleagues (2018, 2019a, 2019b) allows for using XR platforms to visualize network topology and activity in 3D. Such visualizations may improve the efficiency of shared mental modelling during communication in cyber teams which may ultimately result in better cyber defense decision-making. Furthermore, if visualizations are at a scale where cooperating team members can walk around in the visualized network, it may also leverage spatial information encoding processes thus not only loading on visual senses. This could help facilitate multi-sensory integration, which could translate to more efficient processing of complex information which, in turn, may have downstream benefits on sensemaking and communication. This thesis investigates these potential benefits by comparing the effect of 3D visualizations of network topology against 2D visualizations on dyadic cyber team communication, cyber SA, and decision-making during a simulated cyberattack. To assess the effect of 3D visualizations on communication, we operationalized communication behaviors that had been suggested as relevant in observations of cyber teams or in proposed frameworks in previous research. These operationalizations consisted of noting the frequency of previously identified communication behaviors during structured observations, including OLB behaviors (2018), task resolution communication (Jariwala et al., 2012), and communication dysfunction behaviors (Champion et al., 2012; Henshel et al., 2016; Jariwala et al., 2012) such as prolonged silence (considered an indication of communication breakdown; Champion et al., 2012; Jariwala et al., 2012).

The following chapter discuss general methodological principles followed by a general overview of how data was collected for the thesis work. Detailed overviews of methods of analysis can be found in chapter 5.1-5.3. In general, I planned and conducted most of the planning of measurements, data collection, and subsequent analyses.

Chapter 4

4 Methodology

The work included in this thesis is a series of studies aimed at understanding and influencing the relationships between the neurocognitive processing of cyber threat information, the human-to-human communication of that cyber threat information, and decision-making in cyber threat situations. The overarching goal is to develop neuroergonomic approaches to understand and influence human-to-human communication of recognized cyber threat situations. The work relies on a number of methodologies including systematic literature review with qualitative synthesis, and quantitative studies including a study with correlational design applied in a naturalistic setting, and a randomized experiment with head-to-head design conducted in a semi-naturalistic setting. While the approaches are informed by neuroscience, the nature of the research is applied and, by necessity, ultimately interdisciplinary.

4.1. Applied Research

The core issues addressed by this work are the performance issues that cyber analysts working in teams face in situations where they have to communicate their understanding of cyber threat situations to team members and less technical personnel. The working-environments where this communication occurs are very dynamic and highly complex in ways that are hard to study in controlled laboratory settings. In other words, without capturing situational dynamics and complexity, it is difficult to determine the extent to which findings can be generalized to the real world. Because the ultimate goal is to solve a real-world problem, the research has sought out contexts with high fidelity to the environments where the behaviors of interest occur. The naturalistic studies were conducted in collaboration with the Norwegian Defense Cyber Academy (NDCA) and the NATO CCDCOE Locked Shields CDX. Including the work in this thesis, the NDCA has spent most of the past decade inquiring into the psychological and neurocognitive determinants of cyber operator performance to identify ways of improving and accelerating training of cyber cadets. The work presented in this thesis is a continuation of the research previously conducted at the NDCA.

It is difficult to exactly separate basic research from applied research without making inferences about the psychological state of researchers (e.g., motives) and the expected utility of research outcomes (Reagan, 1967). For instance, a scientist conducting basic research may

contextualize their findings by relating them to a practical problem without having the intention of solving that problem. However, applied research is generally considered to include research that aims to solve specific and practical problems faced by individuals or groups, while basic research can also include goals where the desired knowledge about a phenomenon is sought for the sake of knowing. Thus, for basic research, the potential utility of the knowledge is just a bonus regardless of the utility being explicitly acknowledged by the researcher. An example of a specific practical problem could be "how can we make it easier for cyber operators to explain the significance of complex technical information to an individual who does not have a fundamental understanding of the components of the environment that gives the technical information its relevance?". A basic research problem could be "where are the neuroanatomical gradients that determine the transition from internally directed problem-solving to externally directed problem-solving?". Knowledge previously derived from basic research can be transferred into applied research contexts to serve as theoretical frameworks guiding scientific inquiry (Parasuraman, 2003). This is exactly the approach adopted by the work in this thesis, where the neuroergonomic approaches applied in this work have been derived from neuroscientific findings reported in basic research.

4.2. Systematic Reviews

Developing neuroergonomic approaches for understanding and improving communication of recognized cyber threats requires understanding the contextual factors posing challenges to adequate communication. To understand these contextual factors, the work presented in this thesis started by systematically reviewing previous studies that have been published on the topic of human communication in cybersecurity. Literature reviews are conducted to assess existing knowledge on a specific topic of interest, where the topic is either broadly or narrowly defined. As such, literature reviews may serve several purposes, such as synthesizing state of the art knowledge within a given field. This synthesis may in turn be used to identify where and how to guide future research. Literature reviews may also address questions that require examination of converging and diverging evidence from multiple disciplines and model systems. Such examinations may be impossible to address in a single study. Literature reviews may also be used to provide an overview of methodological shortcomings and unanswered questions in primary research. This can help improve the quality and explanatory power of future research efforts. Literature reviews may also serve the purpose of generating and evaluating theories and frameworks.

Systematic reviews are literature reviews conducted with a systematic methodology that includes clearly stated aims procedure, a transparent literature search strategy that reduces sampling bias, explicit criteria for inclusion and exclusion, a series of review phases where literature collected from the initial searches are reduced to those eligible for inclusion, and a plan for how to treat and report relevant information in the reviewed literature. There are some recommended guidelines for how to conduct systematic literature reviews, one of them being the Preferred Reporting Items for Systematic Evaluations and Meta-Analyses (PRISMA) guidelines (Moher et al., 2009). Using PRISMA for literature evaluations provides substantial advantages. The PRISMA framework offers a methodical and clear-cut review protocol that improves the ability to replicate research findings (Moher et al., 2015; Tricco et al., 2018). It aids in the identification of significant discoveries and guarantees the excellence of research selection, which is vital due to the diverse quality of sources. PRISMA helps mitigate bias by employing a predetermined selection method and criteria.

The systematic framework developed by PRISMA is extensively utilized to establish research inquiries and criteria for the inclusion and exclusion of investigations. This facilitates a comprehensive examination of the literature, enabling the identification of deficiencies and providing direction for future investigations (Moher et al., 2015; Tricco et al., 2018). The PRISMA guidelines recommend authors to be explicit about any limitations to the publication year of the articles that were considered for inclusion in the search strategy, the date of the last database search, and the type of sources that were considered (Moher et al., 2009). This holds special significance in the swiftly growing domain of cyber operations where “academic literature is not the only relevant source [of information]” (Spring & Illari, 2021; pp. 2). Thus, it is important to clarify whether non-academic sources were considered for inclusion so that readers can make inferences about limitations arising from the omission of gray literature. The systematic literature review included in this work was part scoping in nature as it aimed to provide an overview of how human-to-human communication in cyber threat situations had been studied scientifically and therefore surveyed scholarly resources such as academic journals and conference papers.

It should be noted that an updated version of the PRISMA guidelines were published after the systematic review included in this thesis was accepted for publication (Page et al., 2021). The updated version includes a list of twenty-seven items with recommendations for preferred reporting and a new flow diagram to visualize the review process.

4.3. Quantitative Research

Developing neuroergonomic approaches for understanding and improving communication of recognized cyber threats implies relating internal (and in principle unobservable) processes to observable behaviors. To determine if and how they are related one must have some quantifiable way of measuring their relationships. Quantitative research is considered to be a deductive approach. Studies are conducted and analyzed within a reductionist framework where phenomena of interest are approximated through definitions allowing for objective quantifiable observations. These observations constitute data which can be reduced to smaller, more manageable processes. By favoring (reductive) specificity over richness, phenomena of interest are reduced to concrete operations and numbers, allowing for hypothesis testing and replication.

Reliability and validity in quantitative research concerns theoretical validity, measurement instrumentation, study design, and analysis. In behavioral research, concepts such as metacognition and SA are hypothetical constructs used to explain observable behavior. These hypothetical constructs (latent variables) are operationalized through the definition of observable activities in order to measure them (observed variable). Examples of operational definitions can be defining which responses on a multiple-item measure indicate anxiety, or defining how variation in the intervals between consecutive heartbeats indicate brain activity. Needless to say, valid operational definitions are particularly important in behavioral and naturalistic studies where the aim is to make conclusions about how unobservable mental phenomena influence behavior. For these operationalizations to be valid, the instruments must undergo several checks for reliability and validity. If an operational definition actually measures a real underlying construct the way it is intended, it is considered to have construct validity (addressing both the specificity of the measurement and the existence of the construct). As part of the purpose of the research conducted in this thesis is to identify performance metrics for cyber analysts working in teams, a handful of the measures employed in the work contributes towards establishing or falsifying the construct validity of the measures.

Reliability in quantitative research concerns whether a measurement has internal and external consistency. Internal consistency on a multiple-item measure refers to the consistency of people's responses across the items, which is expected if all the items reflect the same underlying construct. External consistency is how consistent the measure is across different testings on the same people (test-retest reliability). The cyber SA measure (Lif et al., 2017)

used in Chapter 5.2 is novel and still being validated. Thus, it was especially necessary to test the internal consistency of this measure.

Validity in quantitative research concerns whether a study has internal and external validity. Internal validity is determined by study design and refers to the extent one can make conclusions about the causal effects in a study, in other words, whether observed effects are a result of variable manipulation, chance, or confounding variables that have not been observed. External validity refers to whether (and the extent) an effect can be generalized from the participants of a study and the study setting to the whole population of interest, all settings of interest, and across time. The studies in Chapter 5.2 and 5.3 had small samples sizes, thus it is hard generalize the findings reported in these studies outside the study context.

4.4. Correlational Approaches

Part of the aim of the thesis work was to assess the relationship between measures such as mood, vagal tone, communication variables, metacognition, and cyber SA. Correlational research comprises a set of valuable methodological approaches utilized in studies aiming to explore and quantify relationships between variables without directly manipulating any of them. Applying a correlational approach can be suitable when conducting research on human behavior in naturalistic settings. An example could be when researchers have identified a set of variables they suspect to be related but want to study them in the context of naturally occurring behaviors to preserve ecological validity. In other words, correlational research is suitable when researchers want to observe the relationship between variables in a given system without interfering with the system. Correlation approaches are also suitable in situations when researchers want to assess the relationship between variables of interest but do not have the opportunity to manipulate any of them.

Correlational research focuses on determining the strength of the observed relationships and whether they are positive or negative but cannot infer causation due to the lack of a manipulated independent variable. This separates correlational approaches from experimental approaches where studied populations are randomly divided into two or more groups and where at least one group is subject to manipulation of an independent variable. Correlational approaches may include pseudo-experiments where participants are grouped according to naturally occurring characteristics (sex, level of expertise, high or low values on a test or measurement, access to healthcare) to assess differences between group membership and

outcomes. Causation can still not be inferred because group membership is predetermined and not manipulated by the experimenters. In essence, causal attribution is determined by how data is collected and not by how it is analyzed. Correlational methodology allows for the exploration of patterns and connections that can provide insightful findings that contribute to the depth of knowledge on a topic and inform future research.

Given representative samples, reliable measurements, and the research being conducted in a setting with high fidelity to the phenomenon that researchers want to make inferences about, correlational approaches can have high external validity. This means that they are generalizable to similar contexts outside the specific research setting. Correlational approaches do, however, have low internal validity because they do not allow for strong causal conclusions even when third variables are controlled for. As paper II in this work is correlational in nature, causation cannot be inferred from it.

4.5. Experimental Approaches

Improving communication through neuroergonomic approaches implies the application of an intervention that has a desired effect on communication. In Chapter 5.3, an intervention in the form of a 3D visualization of network topology and activity in MR was employed to see if it would affect dyadic cyber team communication and cyber SA. The only way to determine whether an intervention improves communication is to measure its effect on a relevant indicator of communication and compare it to how that indicator behaves in absence of intervention. This is the basic premise of an experiment. In this case, the intervention serves as a manipulation and its presence or absence quantifies the independent variable. The outcome that is dependent on the manipulation is the measured values of communication, which quantifies the dependent variable. If communication (dependent variable) is indeed better in the presence of the intervention (independent variable), it supports the conclusion that the intervention has caused an improvement in communication. Experimental research plays a crucial role in scientific inquiry, specifically in studies where the aim is to understand cause-and-effect relationships between variables of interest. When controlling for confounding variables, experiments have high internal validity which makes it possible to draw strong conclusions about cause and effect within the study.

Whether the observed effect in an experiment is generalizable depends on whether the sample is representative in size and demographics, the sampling and allocation to conditions

were random, and how well the study setting, and manipulation matches the real setting. Random sampling and getting representative sample sizes is difficult when studying cyber operators. Security personnel are likely targets of social engineering, so they are hard to recruit outside of contexts such as CDXs or classrooms where the validity of the researchers and the research project can be verified. The number of available participants in such settings can vary from very few to a few hundred, meaning that even if you are able to recruit everyone it is still not enough. CDXs are expensive and time consuming, and organizers are (quite understandably) reluctant to allow true experimentation. The best one can hope for in such cases is to recruit people to participate in an experiment outside the CDX, which often means when they have time off from a 12-hour shift and in a less naturalistic setting depending on access (to equipment, cyber ranges, and so on) and budget.

4.6. Research Ethics

The work presented in this thesis includes studies using human participants, necessitating several ethical considerations.

The ACDICOM project is funded by the Norwegian Research Council (NFR project #302941) and is registered with the Norwegian Centre for Research Data (NSD). All requirements were met to obtain ethical clearance from the Regional Ethics Committee (REK) and NSD prior to working with human participants and personal data. Institutional guidelines were followed when applying to NSD ethical guidelines for experimental studies. Approval was obtained by filling out the initial NSD online form. REK clearance was not required due to the nature of the studies falling outside the effective area specified in the definitions paragraph (§4) of Act on medical and health research (the Health Research Act; [Lov om medisinsk og helsefaglig forskning (helseforskningsloven)]). The purpose of the studies was not to generate new knowledge on health and disease, thus not qualifying as medical or health research. Personal identifiers were not collected in any of the studies, neither was information about an individual's physical and mental health.

The research methodology required the researcher to conduct studies with people (participants and collaborators) from various organizations involved in cybersecurity. The researcher observed and surveyed students at the NDCA. All data was handled with sensitivity and in line with national guidelines for handling research material of this kind. The project was based on unclassified and unrestricted data. The researcher ensured that participants signed

informed consent forms and that they understood their rights to withdraw from the research at any stage. All data was anonymized upon collection and no information that could be used to trace any data or results in the studies back to an individual participant (e.g. name, home addresses, emails, D.O.B, phone numbers) was collected. Instead, participants generated unique identifiers specifically for each study, consisting of numbers and letters, that they would use when they filled in forms. The subject of cybersecurity can raise sensitive issues among respondents. In cases where participants withdrew consent, they had been instructed to provide their unique identifiers to the researcher, upon which any already gathered data associated with that identifier was destroyed and no further data was collected.

During military CDXs and Cyber Engineering Exercises, responsible and authorized personnel from the Norwegian Defense may execute procedures that are illegal if they were to be conducted outside of a controlled environment. Such practices are well planned, prepared and rehearsed prior to implementation. One of the studies was conducted during an annual Cyber Engineering Exercise organized by the NDCA. This exercise is 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.

The study complies with the Declaration of Helsinki and is in line with the Recommendations for the Conduct, Reporting, Editing and Publication of Scholarly Work in Medical Journals.

4.7. Data Collection and Analysis

The data for paper I (chapter 5.1) was collected through literature searches on the databases Google Scholar, ScienceDirect, IEEE, and Taylor & Francis ($N = 17$). Results from individual studies were summarized in tables and written summaries, and methodological shortcomings were identified. A qualitative synthesis was conducted to provide a coherent picture of the field of research on human-to-human communication in cyber threat situations and suggestions for future research.

The data for paper II (chapter 5.2) was collected from cyber cadets ($N = 36$) participating in the Cyber Operations track of the NDCA's annual Cyber Engineering Exercise. The cyber cadets were tasked with investigating a network intrusion. Data was collected using neurophysiological measurements (inter-beat-intervals) and self-report measures of

prospective performance estimations, affect (perceived mood, arousal, and control), cyber SA, and team workload demand. The neurophysiological measurements were used to quantify vagal tone. The cyber SA self-report measures were scored by one of the organizers of the exercise. Prospective performance estimations controlling for scores on the cyber SA measurements were used to generate variables for metacognition.

The data for paper III (chapter 5.3) was collected from graduating cyber cadets ($N = 22$) recruited at NDCA. Participants were randomly paired in dyads and allocated to one of two groups that either used 3D visualizations of network topology and activity in MR, or 2D visualizations of network topology and activity in printed network diagrams and force directed graphs in Arkime. The comparison of 3D visualization in MR with 2D visualizations in Arkime constitutes a head-to-head design. Network topology and traffic was visualized using network data from the NATO CCDCOE CDX Locked Shields 2022. The dyads were given a series of tasks related to investigating suspicious activity during a simulated cyberattack and decision-making. Data was collected using self-report measures and structured observation. Self-report measures included a forced choice task where participants had to identify the correct network topology, cyber SA, communication demands, and forced-choice decision-making. Structured observations included noting the frequency of select communication behaviors.

Chapter 5

5 Empirical studies

This chapter contains the papers that were published as part of the thesis work. The following is the list of publications:

I. Ask, T. F., Lugo, R. G., Knox, B. J., & Sütterlin, S. (2021). Human-Human Communication in Cyber Threat Situations: A Systematic Review. In Stephanidis, C., et al. HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning, and Culture. HCII 2021 (pp. 21-43). *Lecture Notes in Computer Science*, *13096*. Springer, Cham.

II. Ask, T. F., Knox, B. J., Lugo, R. G., Helgetun, I., & Sütterlin, S. (2023). Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. *Frontiers in Human Neuroscience*, *16*, 1092056.

III. Ask, T. F., Kullman, K., Sütterlin, S., Knox, B. J., Engel, D., & Lugo, R. G. (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *Frontiers in Big Data*, *6*, 1042783.

5.1. Human-Human Communication in Cyber Threat Situations: A Systematic Review

Torvald F. Ask[1,2(*)], Ricardo G. Lugo[1,2], Benjamin J. Knox[1,2], and Stefan Sütterlin[2,3,4]

[1] Norwegian University of Science and Technology, Gjøvik, Norway

[2] Østfold University College, Halden, Norway

[3] Tallinn University of Technology, Tallinn, Estonia

[4] Albstadt-Sigmaringen University, Sigmaringen, Germany

Abstract. In cyber threat situations, decision-making processes within organizations and between the affected organization and external entities are high-stake. They require human communication entailing technical complexity, time pressure, interdisciplinary factors, and often an insufficient information basis. Communication in cyber threat situations can thus be challenging and has a variety of implications for decision-making. The cyber-physical system is a rapidly changing socio-technical system that is understudied in terms of how cyber events are communicated and acted upon to secure and maintain cyber resilience. The present study is the first to review human-to-human communication in cyber threat situations. Our aims are to outline how human-human communication performance in cybersecurity settings have been studied, to uncover areas where there is potential for developing common standards for information exchange in collaborative settings, and to provide guidance for future research efforts. The review was carried out according to the PRISMA guidelines and articles were searched for on scientific databases. Articles focusing on human-human communication in cyber threat situations published in peer reviewed journals or as conference papers were included. A total of 17 studies were included in the final review. Most of the studies were correlational and exploratory in nature. Very few studies characterize communication in useful goal-related terms. There is a need for more collaboration between cyber defense exercise-organizers and cognitive scientists. Future studies should assess how team mental model-development affects team communication and performance in cyber defense exercises.

Keywords: Cyber threat communication · Human factor · Systematic review

1 Introduction

A Cyber Threat Situation (CTS) is the potential occurrence of a cyber-attack aiming to damage, disrupt, or steal a cyber asset. A cyber asset can be understood as a completely or partly digitized protected organizational resource (Whitman and Mattord 2012). With the increased digitization of society and global network coverage, the cyber threat land- scape is evolving and so is the

need for research on the prevention and effective handling of cyber threats. Organizations often assign their cybersecurity operations to Security Operation Centers (SOCs). SOCs are teams and organizational units that cover multiple security activities such as preventing, detecting, assessing, and responding to cyber threats and incidents (Muniz et al. 2015). Within the SOC organizational structure, technical tasks such as asset monitoring, detection, analysis, forensics, network security, intelligence, and communicating suggestions for cyber threat- and cyber incident response are assigned to technical staff while subsequent decision-making tasks such as how to act on threat and incident reports are assigned to other individuals (decision- makers; Muniz et al. 2015). Consequently, there is a potential knowledge gap between technical personnel and decision-makers.

Cyber professionals, known as cyber operators in military sectors and cyber analysts in civil sectors (interchangeably referred to as COs), make up the technical personnel in SOCs and face a unique set of challenges spanning the cyber, physical, and social domain (Jøsok et al. 2016). This cyber-physical working environment of human-machine and human-human interaction creates a complex Socio-Technical System (STS) that is subject to high rates of innovation, increasing network interconnectedness, and rapid flow of information (Zanenga 2014). Decision-making in STSs has its own set of challenges. In cyberspace, the impact of decisions and actions on own- and third-party infrastructure is influenced by connectivity between different decision-making agents (Tikk-Ringas et al. 2014). In a cybersecurity setting, there is a persisting element of uncertainty regarding the presence, persistence, and consequences of adversarial behavior. This suggests that decision-makers need to prioritize multiple assets based on known and unknown risk and cognitively transition between cyber and physical contexts when estimating the impact of their decisions (Jøsok et al. 2016).

Due to the multiple impact-dimensions of cyber defense decisions, communication between human agents is at the core of good cyber defense decision-making (Knox et al. 2018). Strategic-level decision-making and tactical-level technical developments need simultaneous integration but are usually distributed over different roles, both vertically and horizontally within an organization. Since CO activity and decision-making is dis- tributed among different roles within the SOC (Muniz et al. 2015), there are multiple dyadic relationships that simultaneously influence the information requirements of cyber threat communication. The information communicated from a CO during a CTS must be available for interpretation by all dyads. This can be challenging when stakeholders belong to non-technical sectors or lack

technical skills. In a recent review, Agyepong et al. (2020) identified communication as one of the challenges facing SOCs. How cyber events are communicated and acted upon in the physical domain to secure and maintain cyber resilience is currently not well understood. In this paper, we systematically review the literature on human-human communication in CTSs.

1.1 An Accurate Recognized Cyber Picture is Critical for Effective Cyber Defense Decisions

Successful decision-making based on human interaction requires a shared situational awareness (SA) of the CTS. This includes a mutual understanding of what caused the situation, the current state of assets, potential adversaries, how the situation is evolving, and which actions to take to mitigate detrimental outcomes. An organization's Cyber Situational Awareness (CSA) influences whether an organization maintains control in its cyberspace (Franke and Brynielsson 2014). Seven requirements that need to be met to have full CSA for cyber defense have been suggested (Barford et al. 2009): (1) awareness of the current situation, (2) awareness of the impact of the attack, (3) awareness of how situations evolve, (4) awareness of adversarial behavior, (5) awareness of why and how the current situation is caused, (6) awareness of the quality and trustworthiness of the CSA information, and (7) assessment of plausible outcomes. Having an accurate Recognized Cyber Picture (RCP; or Cyber Common Operational Picture) is crucial to achieve CSA. While CSA can be understood as being aware of the underlying state of a specific cyber environment at any given moment (Franke and Brynielsson 2014), RCPs consist of actively selected and actionable information specifically pertaining to cyber threats (Cyber Threat Intelligence; CTI) and aim to update stakeholders CSA and support their decision-making. To achieve this goal, RCPs should contain the information suggested by Barford et al. (2009).

In the process of cyber threat communication, the CO must first investigate the threat to create the initial RCP, then it is shared (shared RCP; sRCP) across platforms, in differing modalities, and often across organizations, hierarchical layers, professional backgrounds, and societal sectors. When the CO shares the RCP, the CO must translate information that is often inherently complex and at times vague. The receiving partner may lack the expertise of the CO and have a mindset that is oriented towards action in the physical world (Knox et al. 2018). Thus, the cyber-to-physical relay of RCPs is subject to many challenges which may render the sRCP inaccurate, losing critical information. Consequently, the sociocognitive demands of the tasks

performed by COs are complex, demanding high cognitive load, and require both technical (e.g. digital forensic analysis) and non-technical skills (e.g. communication; Jøsok et al. 2017).

1.2 Cognitive Aspects of Cybersecurity Performance and Implications for Cyber Threat Communication

Through enhanced information flow, cyber increases human operative abilities (Buchler et al. 2016) while simultaneously creating an environment at odds with human cognition (Zachary et al. 2013). Due to high levels of social barriers, situational shift, and uncertainty, COs must understand and skillfully apply a variety of cognitive processes to adapt to complex and changing task demands (Jøsok et al. 2016, 2017, Knox et al. 2019a). Although these challenges are acknowledged by the adoption of science-based educational approaches to meet the cognitive demands of cyber (e.g. Knox et al. 2019a), common best practices to meet these demands currently do not exist.

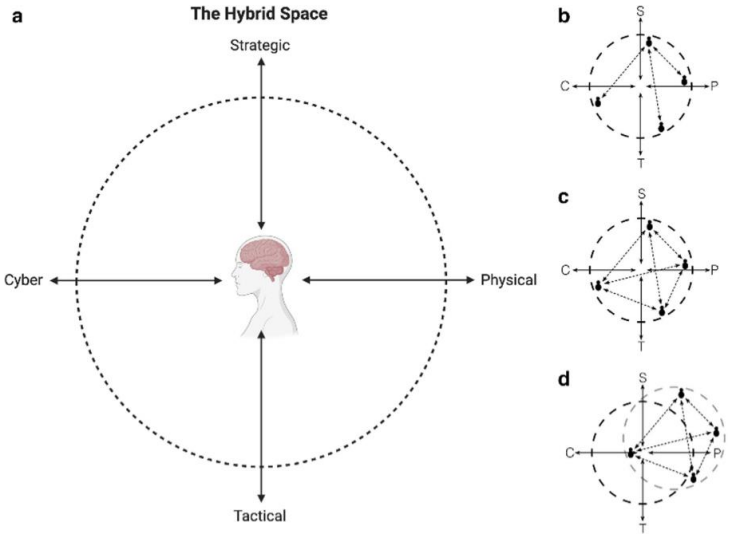

Fig. 1. a The Hybrid Space Framework (Jøsok et al. 2016, 2017) conceptualizing the cognitive landscape cyber operators must navigate. Created with BioRender.com b Hierarchical structure, complicated relations. c Hierarchical structure, complex relations. d Sliding space. C = Cyber. S = Strategic. P = Physical. T = Tactical.

Research conducted in collaboration with our lab put forward the Hybrid Space (HS; Fig. 1,a) framework (Jøsok et al. 2016) to conceptualize the cognitive landscape COs must navigate. The HS framework focuses on the interconnectedness between cyber- and physical space, and the tension between tactical and strategic goals in decision- making. If a CO is more oriented

towards cyber, communicative challenges may arise when the COs communicates with someone located in the strategic-physical quadrant who in turn must relay the information to an individual with orientation in another quadrant (Fig. 1,b; Jøsok et al. 2017). Further socio-cognitive complexity is added when a group of individuals in different hierarchical layers and different tasks all communicate with each other, requiring constant re-adjustment of communication style and message content (Fig. 1,c; Jøsok et al. 2017). From the perspective of the CO, locating your own current cognitive focus within the HS requires metacognitive awareness (Knox et al. 2017). When other individuals enter the HS, the CO needs to be aware of their presence in the space and adopt perspective taking to understand their CSA, their grasp of the RCP, and to communicate efficiently one's own RCP understanding. This helps facilitate that involved partners can develop and calibrate shared CSA so that decisions incorporate both tactical and strategic approaches in both the physical and cyber domain (Knox et al. 2018).

Good cyber defense relies on effective team coordination (Forsythe et al. 2013) and COs working in teams must actively engage in dynamic problem solving to acquire knowledge from each other and the environment (Jøsok et al. 2017). In line with the shifting task demands of the HS, the HS might move along its axis as the focus of the team changes (Fig. 1, d; Jøsok et al. 2017) thus changing communicational needs.

1.3 Current Approaches to Solving Communication Problems in the Hybrid Space: The Orienting, Bridging, Locating (OLB) Model

The process of communication from threat detection to the CO submitting the RCP to a decision-maker is subject to many iterative sub-processes and factors that affect the sRCP and decision-making. Building on the HS framework, our lab proposed the Orienting, Locating, Bridging (OLB) model (Fig. 2; Knox et al. 2018) as a tool to improve communication flow.

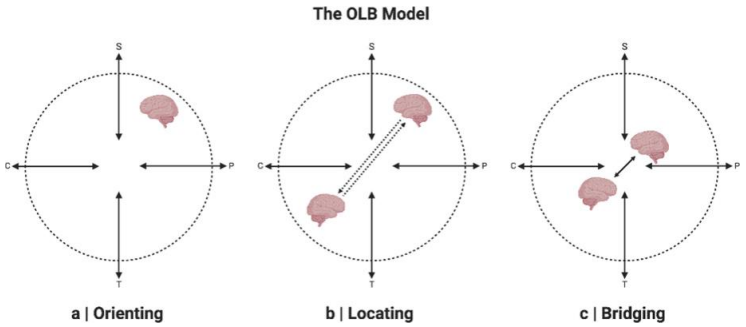

Fig. 2. Orienting, Bridging, Locating (OLB) model. The OLB model (Knox et al. 2018) is a three-stage pedagogical tool to ground communication between cyber operators and their communication partners. C = cyber. S = strategic. P = physical. T = tactical.

Although metacognitive awareness is associated with movements in the HS (Knox et al. 2017) and the OLB model provides guidelines for how to apply the HS framework to improve communication (Knox et al. 2018), more research on HS movements and subsequent communication efficiency is needed.

1.4 Aim

Given the lack of knowledge regarding human cyber threat communication, in this paper, we review the literature on communication in CTSs. Our aims are to (1) outline how human-human communication performance in cybersecurity settings has been studied, (2) to uncover areas where there is potential for developing common standards for information exchange in collaborative settings, and (3) to provide guidance for future research efforts. While laws and regulations can both be promoters and impediments to information sharing practices (see Pala and Zhuang 2019), reviewing laws are currently outside the scope of this article.

2 Methods

The systematic review was carried out according to the PRISMA guidelines (Moher et al. 2009). We wanted to review qualitative and quantitative original research articles and reviews that studied human-human communication of cyber threat information.

2.1 Review Procedure

1. Identify literature on human-human communication in CTSs through database searches.
2. Categorize the publications according to type and methodological approaches.
3. Provide a summary of the selected articles in order of methodological approaches and which aspect of communication that was studied.
4. Synthesis and discussion of findings followed by suggestions for future research.

2.2 Literature Collection Methodology

There was no limit to publication year. Only articles written in English were considered. Databases and search terms are listed in Table 1. Any peer reviewed conference papers and journal articles that either: (1) described characteristics of human communication of cyber threat information, (2) suggested ways to improve the relay of cyber threat information between humans, (3) assessed how aspects of human communication related to cybersecurity performance, or (4) assessed neuroscientific, cognitive, and psychological constructs related to

communication were considered for inclusion. Communication could either be the primary focus of the studies or part of a broader focus.

Table 1. Overview of databases, search terms, filters, hits, and date of last search

Database	Search terms	Filters	Hits	Date of last search
Google Scholar	“communication”, “cyber threat”, “human-interaction experiment”, “recognized cyber picture”, “cyber common operational picture”, “cyber threat communication”	None	590	Feb. 11. 2021
ScienceDirect	“communication”, “cyber threat”, “human-interaction experiment”, “recognized cyber picture”, “cyber common operational picture”, “cyber threat communication”	Reviews and research articles	1251	Feb. 11. 2021
IEEE	“communication”, “cyber threat”, “human-interaction experiment”, “recognized cyber picture”, “cyber common operational picture”, “cyber threat communication”	None	388	Feb. 11. 2021
Taylor & Francis	“communication”, “cyber threat”, “human-interaction experiment”, “recognized cyber picture”, “cyber common operational picture”, “cyber threat communication”	None	11	Feb. 13. 2021

2.2 Descriptive Information and Statistics

Characteristics of each study such as literature type and methodology, results and outcomes including statistics, and studied population were summarized and presented in tables.

3 Results

The phases of the review are depicted in the flow diagram in Fig. 3. Of studies assessed for eligibility, 13 were excluded due to: (1) proposing technical tools for improved CSA without assessing effects on human communication, (2) only focusing on organization- media communication after a security breach, (3) focusing on increasing the frequency of threat reporting without suggesting ways to organize cyber threat information or making human-to-

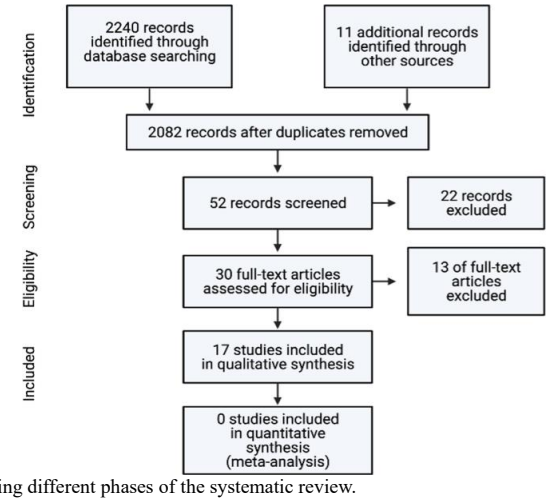

Fig. 3. Flow diagram depicting different phases of the systematic review.

human communication more effective, (4) not studying human-to-human relay of cyber threat information or associated human factors, (5) applying mathematical modeling of communication and collaboration without human subjects. A total of 17 studies were included in the final review. Twelve of the selected articles studied some aspect of cognition and its role in cybersecurity performance. Six of the studies were con- ducted on team-based cyber defense exercises (CDXs), Table Top Exercises (TTXs) or Cyber Defense Games (CDGs). There were not enough data to conduct a meta-analysis. None of the studies were published prior to 2012, average publication year was 2016. Overview of the identified publications according to type and methodology is provided in Table 2.

Table 2. Overview of the selected publications according to type and methodology

Type	Methodology			
	Qualitative	Quantitative	Mixed	Total
Conference paper	3	2	3	8
Journal article	6	3		9

Knowledge type				
Empirical	5	5	3	13
Theoretical	4			4
Total	9	5	3	17

3.1 Quantitative and Mixed Studies on Cyber Threat Communication

Five studies examined communication in cyber teams during CDXs, TTXs, or CDGs (Buchler et al. 2018, Champion et al. 2012, Finomore et al. 2013, Henshel et al. 2016, Lugo et al. 2017). One study assessed the role of expectations on security information sharing (Mermoud et al. 2018). One study assessed the role of beliefs on knowledge absorption of cyber threat information (Percia David et al. 2020). One study assessed the knowledge requirements of strategic level decision makers (Garcia-Granados and Bahsi 2020). Table 3 summarizes the selected quantitative/mixed articles.

The Role of Communication in Cyber Team Performance. To understand how to develop human cyber skill-sets in cyber operational environments, communication and collaboration (ComCol) among team members along with years of experience, and number of roles inhabited by team members were examined as predictors of maintain- service tasks, scenario-injects, performance against the red (attacker) team, and incident response (Buchler et al. 2018). ComCol scores strongly and positively predicted performance on maintain-service tasks and scenario-injects. ComCol scores also predicted performance against the red team, although negatively. ComCol scores did not strongly predict incident response scores (Buchler et al. 2018). Simultaneous analysis of all predictors showed that the ComCol factor was not a unique predictor of performance (Buchler et al. 2018).

As a follow-up to no-findings (Jøsok et al. 2019, Knox et al. 2017, 2019b) on individual traits associated with cyber tactical and strategic decision-making performance, Lugo et al. (2017) investigated the effects of team workload demands on performance in a CDX simulation for testing officer cadets' teamwork perceptions. Outcome measures were based on the HS framework (Jøsok et al. 2016). Previous studies (Jøsok et al. 2019, Knox et al. 2017, 2019b) showed that both cognitive and metacognitive factors could explain cyber-physical interactions, but could not explain any tactical-strategic decision- making during the CDX. ComCol performance demands showed increased involvement on tactical and strategic decision-making outcomes as well as facilitating cyber-physical transitions (Lugo et al. 2017).

Only dissatisfaction with team performance was identified as a negative team factor. The results suggested that situational and team factors need to be taken into consideration alongside individual factors to explain performance (Lugo et al. 2017).

Several factors influence cyber team SA (CTSA) among COs. Based on the observation that intra-team communication problems were fundamental challenges to CTSA among COs participating in CDXs (Champion et al. 2012), a TTX pilot study was conducted. Team performance dropped by 0.42% per security alert added, affecting perceived attack path, collaborative team report detailing the order and specifics of security breaches, and CTSA. Mental demands were somewhat high and CTSA was moderate to low and declined with increased information (Champion et al. 2012).

Table 3. Overview of quantitative and mixed studies included in the review

First author, year	Design	Effect sizes	Results	Outcome	Population (N; sex)	Comments
Buchler (2018)	Correlational; naturalistic: Survey, structured observation	ComCol on: Maintain services: R2 = 0.42 (−0.13, 1.00); Scenario injects: R2 = 0.54 (−0.03, 1.13); Red team: R2 = 0.27 (−0.23, 0.79)	Maintain services: β1 = 0.65 (−0.21, 1.54)*; Scenario injects: β1 = 0.74 (−0.04, 1.53)**; Red team: β0 = − 0.00 (−0.94, 0.90)*	ComCol joint positive predictor of maintain services, scenario injects, and joint negative predictor of scores against red team	Students in cyber defense competition (N = 64; sex not reported)	
Garcia-Granados (2020)	Correlational; Literature review, expert panel survey	Not applicable	43 topics identified. SLDM must know all of them. ART had highest average ranking	Overview of which topics SLDM must have knowledge about and ranked order of priority	CISOs (N = 10; sex not reported)	
Champion (2012)	Correlational: Unstructured interview, observation, TTX	Not reported	(F(1,15) = 4.584*); 60.17% correctly classified	Number of security alerts reduce team effectiveness and CTSA	Proprietary sample (N = 24; sex not reported)	Cognitive load = NASA-TLX
Finomore (2013)	Experiment; naturalistic, within-subjects design	Not reported	Correct: F(2, 11.06) = 9.00*; None (M = 87.5%), Medium (M = 87.5%), High (M = 37.5%). Time: F(2, 9.88) = 14.10*; Medium (M = 16 min, 30 s), None (M = 16 min, 54 s), High (M = 27 min, 48 s) inject	Untruthful statements diminish team performance	Paid participants (N = 24, m = 9)	

(*continued*)

Table 3. (*continued*)

First author, year	Design	Effect sizes	Results	Outcome	Population (N; sex)	Comments
Henshel (2016)	Correlational; naturalistic	Not reported	Average arguing 2.05 of 7; Average task redistribution 5.66 of 7	Arguing negatively correlated with TTP and Correct categorization of NIST event	US army's Computer Network Defense Teams (N = 446; M = 96%)	
Lugo (2017)	Correlational; naturalistic	X-axis: (R2 = .245**); Y-axis: (R2 = .124*)	Communication demands associated with cyber-physical actions (X) and tactical-strategic decision-making (Y)	Hybrid space performance movements operationalized (4 variables) as DV	Cyber defense cadets (N = 31; sex not reported)	IV: TWLS; DV: Hybrid space
Mermoud (2018)	Correlational survey	Spearman's p Frequency: .184–.244** Intensity: .169–.275**	Value of info, social reciprocity, institutional design, and trust associated with SIS	2 DV: Frequency & Intensity of information sharing	MELANI-net cybersecurity managers (N = 262; sex not reported)	6 hypotheses tested
Percia David (2020)	Correlational; questionnaire	Spearman's p: Resource = 0.2860; Usefulness = 0.2779; Reward = 0.0258; Reciprocity = 0.3543	Resource belief***, usefulness belief***, and reciprocity belief*** positively associated with knowledge absorption	Knowledge about which beliefs are associated with knowledge absorption of cyber threat information	MELANI-net cybersecurity managers (N = 262; sex not reported)	Follow-up of Mermoud (2018)

Notes. P < .05 = *, P < .01 = **, P < .001 = ***. ART = Advanced persistent threat. CDX = Cyber defense exercise. CISO = Chief information security officer. ComCol = Communication and Collaboration. CTSA = Cyber team situational awareness. DV = dependent variable. IV = independent variable. NIST = National Institute of Standards and Technology. SIS = Security information sharing. SLDM = Strategic level decision-maker. TTP = Time between start of inject to returned approval by team controller. TTX = Tabletop exercise. TWLS = Team workload scale

The authors suggested that information overload drive abnormalities in both team structure and team communication, and that team cyber defense processes must be restructured to facilitate sharing of workload and information. Lack of communication was suggested to be one of the most important contributors to the findings (Champion et al. 2012). The authors did not correlate mental fatigue scores with communication metrics.

In line with findings regarding the challenges associated with communication problems in cyber teams (Champion et al. 2012), detrimental effects of arguments on team performance were reported in initial findings from a study on predictors of cyber team proficiency in CDXs (Henshel et al. 2016). The effect of communication on the following Blue Team proficiency metrics were assessed: (1) Time-to-Detect: Time between start of inject and first validated detection report, (2) Time-to-apProval (TTP): Time between start of inject to returned approval by team controller, (3) Time-to-End (TTE): Time between start of inject to blue team filing close out report, and (4) Category Correct (CatCorrect): Percent of National Institute of Standards and Technology (NIST) category of inject correctly identified by the blue team. Frequent arguing was found to be significantly and negatively correlated with TTP as well as CatCorrect. Task redistribution when necessary was significantly and positively correlated with TTE and CatCorrect (Henshel et al. 2016). The authors did not report correlation coefficients or p-values but note that most of the data will be reported elsewhere (Henshel et al. 2016).

While other studies (Champion et al. 2012, Henshel et al. 2016) mainly looked at communication with respect to cyber-attacks aimed at assets, one study (Finomore et al. 2013) sought to study the influence of human-directed cyber-attacks on team communication and performance. Distributed team members in a CDG were exposed to misleading information and effects on team processes and decision-making were measured. They all received unique factoids and had to compare them to the factoids received by other team members through communication over a shared radio channel (Finomore et al. 2013). Within-subjects design was employed and divided in conditions None, Medium, and High. For the Medium condition, the inject was suggestive and contradicted supportive information. In the High condition the injects contradicted expert factoids and were phrased as facts. There were no injects in the None condition. Injects in the High condition had the most detrimental effect on team performance both on number of correct answers as well as time spent on completion. How the injects affected communication specifically was not assessed (Finomore et al. 2013).

Knowledge Requirements of Strategic-Level Decision-Makers (SLDMs). To tackle communication problems between SLDMs and their CO teams, a study (Garcia- Granados and Bahsi 2020) tried to identify topics of knowledge requirements that could serve as basis for training or CDXs for SLDMs without IT or security background. A literature search identified 43 topics of knowledge that were sorted based on incident rate to assess their emphasis in the literature. 10 chief security information officers from different industries rated the topics on the level of knowledge needed. A higher rank meant that the topics were attributed a higher knowledge priority (Garcia-Granados and Bahsi 2020). Although having a low incident rate in the literature, "Advanced Persis- tent Threat" had the highest average ranking. The lowest ranked topic was "Access control models". No topic was rated as 'no knowledge' meaning that the participants meant SLDMs needed some knowledge about all the topics that were identified (Garcia- Granados and Bahsi 2016). Topics associated with third party security attained a lower average rank.

The Role of Expectations on Sharing of Cyber Threat Information. The role of incentives for Security Information Sharing (SIS) between human agents working in institutions were assessed to see if expectations of usefulness, reciprocity, institutional barriers, reputation, and trust would affect SIS (Mermoud et al. 2018). A questionnaire was administered to participants of the closed user group of the Swiss Reporting and Analysis Center for Information Assurance (MELANI) which is a government organization that provides a platform to facilitate SIS between Critical Infrastructures (Mermoud et al. 2018). Six hypotheses were tested regarding the effect of expectations on frequency and intensity of SIS, and the moderating role of trust. They found that the value of information a human agent expects to receive from SIS significantly increases the intensity of SIS, but not frequency. Expectancy of social reciprocity significantly increased both intensity and frequency of SIS, as did expectations that SIS would be facilitated by their institution. Both transactional reciprocity and trust between human agents significantly increased frequency of SIS but not intensity. Reputation was not a significant predictor of SIS. They found partial support for their hypothesis regarding the moderating role of trust. It negatively and significantly moderated the relationship between value and the intensity, but not the frequency of SIS. Trust negatively and significantly moderated the relationship between transactional reciprocity and SIS (Mermoud et al. 2018). Education was negatively associated with the frequency of SIS. Gender, age, length of membership in MELANI, and industry affiliation were not significant predictors of SIS.

The Role of Beliefs on Knowledge Absorption of Cyber Threat Information. Building on the previous findings of Mermoud et al. (2018) regarding the role of incentives on SIS, Percia David et al. (2020) assessed the relationship between various resource beliefs and tacit cybersecurity knowledge absorption in a study of cybersecurity man- agers participating in MELANI (the same closed user-group as in Mermoud et al. 2018). Knowledge absorption was not tested directly, but measured through participants rat- ing the amount of exclusive information they received through SIS. They found that the belief that valuable knowledge could be acquired (resource belief), expectations of augmenting efficiency of cybersecurity production (usefulness belief), and willing- ness to reciprocate when receiving valuable information (reciprocity belief) were all positively associated with cybersecurity knowledge absorption. The belief that participation in knowledge-transfer processes would result in reward (reward belief) was not associated with knowledge absorption. Neither were any control variables except prior participations in ISAC events (Percia David et al. 2020).

3.2 Qualitative Studies on Cyber Threat Communication

Three studies examined the collaborative and information sharing practices of COs and made suggestions for how to improve the information sharing practice (Ahrend et al. 2016, Skopik et al. 2018, Staheli et al. 2016). One study examined the information requirements different stakeholders had to find an RCP useful (Varga et al. 2018). Two studies researched the role of team mental models (TMMs) in team communication (Hámornik and Krasznay 2018, Steinke et al. 2015). One study assessed the role various aspects of communication had on performance during CDXs (Jariwala et al. 2012). One study examined how communication impacts the level of trust given to individuals and how it affects cybersecurity risk assessment (Henshel et al. 2015). One study surveyed the literature on Technical Threat Intelligence (TTI) to define what it entails (Tounsi and Rais 2018). Table 4 summarizes the selected qualitative articles.

Table 4. Overview of qualitative studies included in the review

First author, year	Design	Results	Outcome	Population (N, sex)	Comments
Ahrend (2016)	Exploratory: semi-structured interview, user diary, thematic analysis	6 themes, 5 subthemes	Knowledge about how COs collaborate to organize threat and defense information and tailor it to the needs of the client	Threat intelligence service providers (N = 5; m = 4)	Supports Staheli (2016)
Hámornik (2018)	Exploratory: semi-structured interviews	TMM is developed and updated by both internal and external communication	Good TMMs may reduce need for communication during high-risk incident responses and under high time pressure	Industry experts operating SOCs or performing SOC related activities (N = 13; sex not reported)	Similar communication methods as reported by Ahrend (2016)
Henshel (2015)	Exploratory: review and synthesis	Trust framework with four subcategories of communication: 'accuracy', 'thoroughness or completeness', 'timeliness', and 'honesty'	Trust framework for risk assessment related to human factors in the cyber domain	Not applicable	
Jariwala (2012)	Exploratory: observation, questionnaires, focus group	Distributed leadership, open task communication, active feedback, asking for help, offering aid crucial in cyber team performance	Communication aspects relevant for cyber team performance	Computer security students (N = 20; m = 18)	

Skopik (2016)	Exploratory: review/survey	Suggestions to increase and optimize information sharing among COs and stakeholders	Structural overview of the dimensions of cyber threat information sharing	Not applicable	
Staheli (2016)	Exploratory; semi-structured interviews	COs collaborate and communicate more with each other than decision-makers. COs are dis-incentivized to share CTI	A user-centered collaborative system for COs called Cyber Analyst Real-Time Integrated Notebook Application	Cybersecurity personnel spanning several job junctions and 8 sectors (N = 37; sex not reported)	Supports Ahrend et al. (2016)
Steinke (2015)	Exploratory: review	Methods for improving communication and developing TMMs for CERTs	Suggestions for enhancement of CERT communication	EMS teams, MR teams, NPPO teams	
Tounsi (2018)	Exploratory: review	Trust is an important factor for successful sharing of threat intelligence	Identification of factors when sharing threat intelligence	Not applicable	Supports Henshel (2015) and Steinke (2015)

First author, year	Design	Results	Outcome	Population (N, sex)	Comments
Varga (2018)	Exploratory: open-ended survey	Enriched, non-speculative information about an event and how to mitigate it in the short- and long-term. No one requested information on adversarial behavior	RCP Information elements that are useful for stakeholder's CSA	National government agencies, regional county administrative boards, county council, local municipal actors, commercial companies that mainly operate nation-wide infrastructure (N = 28; Sex not	

				reported)	

Notes. CERT = Cyber emergency response team. CO = Cyber operator. CSA = Cyber situational awareness. EMS = Emergency medical systems. MR = Military response. NPPO = Nuclear power plant operating. RCP = Recognized cyber picture. SOC = Security operation center. TMM = Team mental model.

Interviews on the SIS Practices of COs. Analyst level COs engage in several informal collaborative and coordination practices when gathering CTI (Ahrend et al. 2016, Staheli et al. 2016). The information needed about a threat differ between clients, thus, RCPs need to be enriched with client-specific information (Ahrend et al. 2016, Staheli et al. 2016). COs communicate through email and phone calls with clients to identify their CTI needs, which is done through onboarding procedures and ongoing communication centered around CTI reports (Ahrend et al. 2016). Gathering information on similar threats that occurred in the past is called gathering Threat and Defense Knowledge (TDK). If a CO was not the one investigating the original cyber threat, COs communicate with the CO who did to gather TDK (Ahrend et al. 2016). This is done by requesting artifacts and information either by face-to-face communication or over email. COs learn about who have encountered similar threats through team meetings, conferences, blogs, and eavesdropping on conversations in and around the office (Ahrend et al. 2016). If COs cannot find information about threats they often assume it does not exist. Existing databases for SIS is circumvented due to not meeting the needs of the COs (Ahrend et al. 2016). COs are often de-incentivized to share data or interim analyses as their reputation as experts is built upon being the one to uncover cyber threats (Staheli et al. 2016) and not sharing information is common (Skopik et al. 2018).

The collaborative ecosystem may involve many organizations with CSA being dis- tributed across COs but the collaborative practices are less common higher up in the SOC hierarchy (Staheli et al. 2016). A typical decision-making hierarchy can be structured with analyst level COs at the bottom, then further up you have supervisors, managers, and then directors at the top (Staheli et al. 2016). While analyst level COs make decisions about what information to include in the RCP, strategic level COs make decisions about whether to send or revise RCPs. Interaction is often unidimensional with information being 'pushed up' and decisions being 'pushed down' the hierarchy (Staheli et al. 2016). A centralized system that incentivizes documenting, SIS and that allows for organizing files to avoid 'cluttering' is needed to facilitate communication of CTI between COs (Ahrend et al. 2016, Staheli et al. 2016). Staheli et al. (2016) proposed a user-centered collaborative system for COs but it needs testing.

Review on the SIS Practices of COs. In their extensive survey, Skopik et al. (2016) identify five primary dimensions of information sharing: (1) Efficient cooperation and coordination, (2) Legal and regulatory landscape, (3) Standardization efforts, (4) Regional and International implementations, and (5) Technology integration into organizations (Skopik et al. 2016). The authors discuss two taxonomies for information and note that TS-CERT taxonomy (Kácha 2014) is more convenient due to the main categories being universal while sub-categories being part of the description rather than a classification schema. The authors also identify 4 scenarios where cybersecurity information is shared; (1) SIS about recent or ongoing incidents; (2) SIS about service dependencies; (3) SIS about the technical service status, and; (4) when requesting assistance of organizations (Skopik et al. 2016). Shortcomings regarding SIS practices concern Cyber Emergency Response Teams (CERTs) not sharing incident data with other CERTs (ENISA 2011). Recommendations were made to enrich incident information with additional metadata to provide insights into observed events (ENISA 2011) and to develop verification methods and criteria for assessing the quality of the data sources. There was demand for establishment of SIS communities with defined scopes (ISO 2012). A CTI exchange (ITU-T 2012) model was proposed.

Interview on Stakeholder's RCP Information Requirements. Most of the reviewed studies approach RCPs from the perspective of SOCs. To address the limited research on stakeholder's RCP needs, one study examined the information elements an RCP must contain to be perceived as relevant for the stakeholder's CSA (Varga et al. 2018). Respondents said RCPs needed non-speculative factual descriptions of the events leading up to an incident and that information came from multiple trustworthy sources; otherwise the quality of the information had to be explicitly stated (Varga et al. 2018). The RCP needed information on the internal state of one's own organization, correct time stamps of events, affected location, size of event, up-to-date picture of organizational stance, all taken and planned actions, explicit view of one's own information requirements, communication plan with approved messages, whom to coordinate responses with, and list of available resources. Difficulties regarding information sharing such as adaptation of information to the situation and receivers were mentioned. The information needed in a RCP depended on the situation but included operational information (Varga et al. 2018). Most wanted information on the consequences an incident had to one's own organization and how it would evolve; few wanted to know the impact on other organizations. Differences were seen between regional and service-specific actors, where regional actors need RCPs to facilitate crisis management collaboration while service-specific actors use RCPs to maintain

continuity in a service (e.g. electricity) provided to customers and to inform governments agencies with information for a broader perspective. No one asked for information about adversarial behavior (Varga et al. 2018).

Interview on the Role of TMMs in SOC Team Communication. Due to the known role of TMMs on team performance, Hámornik and Krasznay (2018) explored the role of team communication on TMMs in SOC teams. Communication facilitating team-level cognitive processes needs to be explicit and is more effective prior to security events. When security events occur, cognitive load is high, capacity for effective communication is low, and coordination is implicit (Hámornik and Krasznay 2018). 13 industry experts who are operating a SOC or performing tasks related to SOCs were interviewed using a semi-structured approach. They reported that local team members communicate within the team verbally or by using email, chat, or ticketing systems. Remote teams communicate via computer-mediated channels, phone calls, and occasional but rare face-to-face meetings (Hámornik and Krasznay 2018). The TMMs are developed and updated by both internal and external communication. If the mental models are well functioning, explicit communication and coordination activities may not be required during high-risk incident responses and under high time pressure. The authors propose that team cognitions such as constructing and updating TMMs via communication is key in SOC team performance and suggest that research should be focused on measuring the effect of communication on TMMs (Hámornik and Krasznay 2018).

Review on the Role of TMMs in Team Communication. CERTs are composed of two or more individuals who prepare for and respond to cybersecurity incidents. By examining other emergency response team's methods of adaptation to incidents, Steinke et al. (2015) identified 5 areas that could be improved to increase CERTs effectiveness. One area concerned enhancement of communication. Information richness and reduction in complexity of interaction was important for effective communication; more one-way communication and less two-way exchanges of information. All necessary information should be communicated at once. The authors (Steinke et al. 2015) propose that CERTs can develop TMMs and transactive memory through cross-training, guided team self- correction training, role identification behaviors, pre-mission communication briefings, individual and team after-action reviews and debriefings pointing to where communication broke down, where interactions and coordination did not occur where they should have, and by making electronic knowledge maps displaying team member roles and expertise (Steinke et al. 2015). The authors note that the dynamic and

evolving nature of cyber can make it hard to adopt strategies from other incident response teams and must therefore be experimentally tested on CERTs.

Observation and Focus Group on the Role of Communication on Team Performance During CDXs. Among all the studies on cyber team communication, only one detailed the goal of communication within teams (Jariwala et al. 2012). Two cybersecurity teams, Team A and Team B were observed to assess the influence of team communication and coordination on performance. Team A outperformed Team B. Team A had distributed leadership among three members which facilitated sharing of completed tasks and information. Team B had one leader who at times was uncertain about what the team was working on. Team A openly discussed each other's tasks and provided feedback. When Team A members needed help with a task, the team adjusted and assisted the team member until they could resume independence. Team A members asked for and offered aid more than they planned and assigned roles. When a task could not be completed, leaders would instruct members to pick up another task where completion was feasible. Team B had members that never spoke during the length of the CDX, partly attributed to cultural and language barriers (Jariwala et al. 2012).

Review on the Impacts of Communication on the Level of Trust Given to COs and How It Affects Cybersecurity Risk Assessment. In their review of trust as a human factor in cybersecurity risk assessment, Henshel et al. (2015) describes how their 'trust framework' relates to communication in cyber defense situations. According to their framework, trust is increased by a CO who can effectively communicate with superiors and other COs, log incident reports with minimal false negatives and false positives, communicate information in a timely manner, and employ competency when applying cyber defense tools (Henshel et al. 2015). Communication is efficient when there is common ground and it is built on shared mental models. Based on the concept of defender trust, they divide communication in four subcategories; 'accuracy', 'thoroughness or completeness', 'timeliness', and 'honesty' (Henshel et al. 2015). Effective communication for cyber defenders requires timeliness as any amount of wasted time will increase the window for attackers to do damage or go undetected. Honesty is integral to trust whilst dishonest communication harms both team effectiveness and the accuracy of defensive efforts in the cyber domain (Henshel et al. 2015).

Review on Subdivisions of Technical Threat Intelligence. In response to the diversity of CTI research and subsequent lack of consensus of what CTI is, Tounsi and Rais (2018) reviewed the literature on TTI, a subset of CTI, and its multiple sources, the gathering methods,

information lifespan, and intended receivers. The authors found that fast shar- ing of CTI alone was not sufficient to avoid targeted attacks (Tounsi and Rais 2018). In support of the framework suggested by Henshel et al. (2015), trust was identified to be an important factor for successful SIS; trusted environments and anonymous sharing were listed as possible solutions when organizations engage in SIS (Tounsi and Rais 2018). The interconnectedness of organizational SIS is increased through the recent use of portals and blogs to exchange semi-automatic threat information. When the quantity of threat information is large, security teams must contextualize the threat data they collect with the specific vulnerabilities and weaknesses they have internally (Tounsi and Rais 2018). As in the reports of Ahrend et al. (2016) and Staheli et al. (2016), a need for common standards for information sharing were expressed (Tounsi and Rais 2018).

4 Discussion

The aim of this paper was to: (1) outline how human-human communication performance in cybersecurity settings have been studied, (2) uncover areas where there is potential for developing common standards for information exchange, and (3) provide guidance for future research efforts. We found that very little research has been done on human-human communication in CTSs and most of the current studies are correlational and exploratory in nature. One study assessed what kind of information that was deemed useful for stakeholders' RCP (Varga et al. 2018). None of the stakeholders interviewed listed adversarial behavior as useful. This could indicate that stakeholders are more oriented towards action in the physical world than in cyber. This can be useful knowledge for COs and suggest use cases for the HS framework (Jøsok et al. 2016, 2017) and the OLB model (Knox et al. 2018) which address these potential problems at both a theoretical- conceptual and practical level, respectfully. The HS framework might be a useful tool for stakeholders to become aware of their own cognitive 'blind spots', while the OLB model can be used by COs to enrich CTI with information on adversarial behavior and make salient how this behavior contributes to the evolution of the CTS.

Steinke et al. (2015) suggested that enriched, one-way communication of cyber threat information where all necessary information is communicated once would enhance CERTs cybersecurity performance. The relevance of these findings is addressed in the HS framework (Fig. 1, a–d; Jøsok et al. 2016, 2017) which illustrates how communication between individuals located across the HS gets increasingly complex when information is relayed across the space and individuals. When cyber threats occur, timely responses are often key, especially during

cyber threat incidents with high time pressure. For one-way communication to be effective, updated and effective TMMs are necessary (Hámornik and Krasznay 2018, Steinke et al. 2015). Cyber TMMs that are updated through communication and coordination prior to the occurrence of cyber incidents may allow for less communication during high-risk incidents with high time pressure (Hámornik and Krasznay 2018, Steinke et al. 2015). Cyber teams perform better in CDXs when they spend more of their time communicating help needs and aid-offerings than planning and role-assigning (Jariwala et al. 2012). Based on these findings, longitudinal studies on cyber TMMs and how they relate to the evolution of communication practices could provide novel insights into how and when cyber threat communication can be optimized for performance.

Support for the notion that too much communication during cyber threat incidents can be detrimental to performance is seen in naturalistic studies showing that ComCol negatively predict scores against attacker teams (Buchler et al. 2018). This, however, might depend on the quality and type of communication, the aspect of performance that is in question (Buchler et al. 2018, Champion et al. 2012, Henshel et al. 2016, Jariwala et al. 2012), and level of expertise (Lugo et al. 2017, Buchler et al. 2018). For example, communication positively predicts handling of both maintenance tasks and scenario injects (Buchler et al. 2018) and productive communication regarding task progress- updates and stating the need of help can enhance incident handling (Jariwala et al. 2012). Under-communication can also be detrimental to team performance by leading to team members working on the same tasks without knowing (Champion et al. 2012). Distributed team leadership might mitigate these issues if individuals holding leadership positions also spend time communicating with team members to know which tasks they are working on (Jariwala et al. 2012). Indeed, the dynamic and evolving nature of cyber and the broad demands of expertise might favor distributed leadership (Jøsok et al. 2017). ComCol performance demands influence tactical and strategic decision-making outcomes and cyber-physical transitions in the HS (Lugo et al. 2017). As opposed to the Buchler et al. (2018) study on CO experts, these cadets were novices. ComCol demands might be necessary in training and development, but may become less relevant with experience.

To update their own and clients CSA, COs enrich RCPs with useful TDK by communicating with both team members and COs from other organizations as well as their clients when investigating a cyber incident (Ahrend et al. 2016, Staheli et al. 2016). This practice is most common for analyst level COs but less and less common higher up in the decision-making

hierarchy (Staheli et al. 2016). Albeit making decision-making more effective, these structural inefficiencies can be detrimental to CSA and shared mental models in the organization, cause communication and coordination problems, and potentially reduce creativity among COs (Staheli et al. 2016). This can be illustrated with the HS framework (Jøsok et al. 2016) when COs and SLDMs are in different quadrants of the HS without knowing where the other organizational members are. Studies assessing or manipulating the RCP-related resource-beliefs of COs and SLDMs (Mermoud et al. 2018, Percia David et al. 2020) may be useful in determining the effect of shared mental models on the resulting RCP.

The reviewed literature has several limitations. Most of the studies were the first to assess the relationships they studied and have thus not been replicated, although they seem to converge on some common principles. Half of quantitative studies (Buchler et al. 2018, Lugo et al. 2017, Mermoud et al. 2018, Percia David et al. 2020) report effect sizes and one study did not report effect sizes nor p-values (Henshel et al. 2016). Sensitivity issues might be the reason why few studies report participant characteristics such as which sector respondents belong to. The Varga et al. (2018) study was con- ducted exclusively on Swedish participants with a large disproportion of respondents belonging to national agencies and critical infrastructure operators, meaning that the robustness of the findings may vary according to which sector provided the answers. This issue is discussed by the authors (Varga et al. 2018). In general, cybersecurity personnel are hard to access, and naturalistic studies are tricky to conduct because con- textual variables are hard to manipulate partly due to restricted collaboration with CDX organizers. This is apparent in the reviewed literature and is a barrier that needs to be overcome. Few studies (Jariwala et al. 2012, Steinke et al. 2015) elaborate on the quality and characteristics of communication. A focused effort is needed to develop quantitative measures of communication that can be readily applied in CDXs in addition to measures of TMM development. Moreover, only two studies assessed individual and team measures (Champion et al. 2012, Lugo et al. 2017) although only one study assessed the relationship between these measures (Lugo et al., 2017). Thus, there is also a need for studies simultaneously assessing individual and team factors related to communication and performance.

4.1 Conclusion

Communication in CTSs has not received much attention and the nature and quality of studies vary. Studies assessing both team factors and individual factors simultaneously are almost non-existent. We found only one study where variables were manipulated to see their effects on

communication and more basic and experimental studies are needed. CDX organizers could benefit from collaborating with cognitive scientists to experimentally manipulate aspects of the CDX such that new insights can be achieved.

It would be useful to manipulate and quantify TMM development prior to and during a CDX or TTX to measure the effect on communication. Standards for characterizing and assessing cyber team communication need to be developed and implemented in studies.

Funding. This study was conducted as part of the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM; project number 302941) project. ACDICOM is funded by the Norwegian Research Council.

References

Agyepong, E., et al.: Challenges and performance metrics for security operations center analysts: a systematic review. J. Cyber Secur. Technol. 4(3), 1–28 (2020). https://doi.org/10.1080/237 42917.2019.1698178

Ahrend, J.M., et al.: On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In: 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (2016). https://doi.org/10. 1109/cybersa.2016.7503279

Barford, P., et al.: Cyber SA: situational awareness for cyber defense. In: Cyber Situational Awareness, pp. 3–13. Springer, Cham (2009). https://doi.org/10.1007/978-1-4419-0140-8_1

Buchler, N., et al.: Cyber Teaming and Role Specialization in a Cyber Security Defense Competition. Front. Psychol. 9 (2018)

Champion, M.A., et al.: Team-based cyber defense analysis. In: 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (2012). https://doi.org/10.1109/cogsima.2012.6188386

ENISA: Proactive detection of network security incidents (2011). https://www.enisa.europa.eu/activities/cert/support/proactive-detection/survey-analysis. Accessed 20 Mar 2021

Finomore, V., et al.: Effects of cyber disruption in a distributed team decision making task. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 57, no. 1,pp. 394–398 (2013)

Forsythe, C., Silva, A., Stevens-Adams, S., Bradshaw, J.: Human dimension in cyber operations research and development priorities. In: Schmorrow, D.D., Fidopiastis, C.M. (eds.) AC 2013. LNCS (LNAI), vol. 8027, pp. 418–422. Springer, Heidelberg (2013). https://doi.org/10.1007/ 978-3-642-39454-6_44

Franke, U., Brynielsson, J.: Cyber situational awareness – a systematic review of the literature. Comput. Secur. 46, 18–31 (2014). https://doi.org/10.1016/j.cose.2014.06.008

Garcia-Granados, F. Bahsi, H.: Cybersecurity knowledge requirements for strategic level decision makers. In: International Conference on Cyber Warfare and Security 2020 (2020). https://doi. org/10.34190/ICCWS.20.102

Hámornik, B.P., Krasznay, C.: A team-level perspective of human factors in cyber security: security operations centers. In: Nicholson, D. (ed.) AHFE 2017. AISC, vol. 593, pp. 224–236. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60585-2_21

Henshel, D., et al.: Trust as a human factor in holistic cyber security risk assessment. Procedia Manuf. 3, 1117–1124 (2015)

Henshel, D.S., et al.: Predicting proficiency in cyber defense team exercises. In: MILCOM 2016- 2016 IEEE Military Communications Conference (2016). https://doi.org/10.1109/milcom. 2016.7795423

ISO: ISO/IEC27010: Information technology – security techniques –information security man- agement for inter-sector and interorganizational communications (2012)

ITU-T: Recommendation ITU-T x.1500 cybersecurity information exchange techniques (2012)

Jariwala, S., et al.: Influence of team communication and coordination on the performance of teams at the iCTF Competition. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 56, no. 1, pp. 458–462 (2012)

Jøsok, Ø., Knox, B.J., Helkala, K., Lugo, R.G., Sütterlin, S., Ward, P.: Exploring the hybrid space. In: Schmorrow, D.D.D., Fidopiastis, C.M.M. (eds.) AC 2016. LNCS (LNAI), vol. 9744,

pp. 178–188. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39952-2_18

Jøsok, Ø., Knox, B.J., Helkala, K., Wilson, K., Sütterlin, S., Lugo, R.G., Ødegaard, T.: Macrocog- nition applied to the hybrid space: team environment, functions and processes in cyber oper- ations. In: Schmorrow, D.D., Fidopiastis, C.M. (eds.) AC 2017. LNCS (LNAI), vol. 10285, pp. 486–500. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58625-0_35

Jøsok, Ø., et al.: Self-regulation and cognitive agility in cyber operations. Front. Psychol. 10, 875 (2019)

Kácha, P.: Idea: security event taxonomy mapping. In: 18th International Conference on Circuits, Systems, Communications and Computers, 2014 (2014)

Knox, B.J., et al.: Socio-technical communication: the hybrid space and the OLB model for science-based cyber education. Mil. Psychol. 30(4), 350–359 (2018)

Knox, B.J., Lugo, R.G., Jøsok, Ø., Helkala, K., Sütterlin, S.: Towards a cognitive agility index: the role of metacognition in human computer interaction. In: Stephanidis, C. (ed.) HCI 2017. CCIS, vol. 713, pp. 330–338. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58750-9_46

Knox, B.J., et al.: Cognisance as a human factor in military cyber defence education. IFAC-PapersOnLine 52(19), 163–168 (2019)

Knox, B.J., et al.: Slow education and cognitive agility: improving military cyber cadet cognitive performance for better governance of cyberpower. Int. J. Cyber Warfare Terrorism (IJCWT) 9(1), 48–66 (2019)

Lugo, R., et al.: Team workload demands influence on cyber detection performance. In: 13th International Conference on Naturalistic Decision Making 2017, pp. 223–225 (2017)

Mermoud, A., et al.: Incentives for human agents to share security information: a model and an empirical test. In: 2018 Workshop on the Economics of Information Security (WEIS), Innsbruck (2018)

Moher, D., et al.: Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. J. Clin. Epidemiol. 62(10), 1006–1012 (2009). https://doi.org/10.1016/j.jclinepi.2009.06.005

Muniz, J., et al.: Security Operations Center: Building, Operating, and Maintaining Your SOC. Cisco Press, Indianapolis (2015)

Pala, A., Zhuang, J.: Information sharing in cybersecurity: a review. Decis. Anal. (2019). https:// doi.org/10.1287/deca.2018.0387

Percia David, D., et al.: Knowledge absorption for cyber-security: the role of human beliefs. Comput. Hum. Behav. 106, 106255 (2020). https://doi.org/10.1016/j.chb.2020.106255

Skopik, F., et al.: A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput. Secur. 60, 154–176 (2016). https:// doi.org/10.1016/j.cose.2016.04.003

Staheli, D., et al.: Collaborative data analysis and discovery for cyber security. In: SOUPS 2016: Twelfth Symposium on Usable Privacy and Security (2016)

Steinke, J., et al.: Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Secur. Priv. 13(4), 20–29 (2015). https://doi.org/10.1109/msp.2015.71

Tikk-Ringas, E., et al.: Cyber security as a field of military education and study. Joint Forces Q.75(4), 57–60 (2014)

Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. 72, 212–233 (2018)

Varga, S., et al.: Information requirements for national level cyber situational awareness. In: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (2018)

Whitman, M.E., Mattord, H.J.: Principles of Information Security, 4th edn. Course Technology, Boston (2012)

Zachary, W., et al.: Context as a cognitive process: an integrative framework for supporting deci- sion making. In: The 8th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2013) (2013)

Zanenga, P.: Knowledge eyes: Nature and emergence in society, culture, and economy. In: 2014 International Conference on Engineering, Technology and Innovation (ICE) (2014)

5.2. Neurophysiological and Emotional Influences on Team Communication and Metacognitive Cyber Situational Awareness During a Cyber Engineering Exercise

Torvald F. Ask[1,2*], Benjamin J. Knox[1,2,3], Ricardo G. Lugo[1,2], Ivar Helgetun[4] and Stefan Sütterlin[2,5,6]

[1]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway, [2]Faculty for Health, Welfare and Organization, Østfold University College, Halden, Norway, [3]Norwegian Armed Forces Cyber Defense, Lillehammer, Norway, 4Norwegian Defense University College, Cyber Academy, Lillehammer, Norway, [5]Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany, [6]Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Tallinn, Estonia

Background: Cyber operations unfold at superhuman speeds where cyber defense decisions are based on human-to-human communication aiming to achieve a shared cyber situational awareness. The recently proposed Orient, Locate, Bridge (OLB) model suggests a three-phase metacognitive approach for successful communication of cyber situational awareness for good cyber defense decision-making. Successful OLB execution implies applying cognitive control to coordinate self-referential and externally directed cognitive processes. In the brain, this is dependent on the frontoparietal control network and its connectivity to the default mode network. Emotional reactions may increase default mode network activity and reduce attention allocation to analytical processes resulting in sub-optimal decision-making. Vagal tone is an indicator of activity in the dorsolateral prefrontal node of the frontoparietal control network and is associated with functional connectivity between the frontoparietal control network and the default mode network. Aim: The aim of the present study was to assess whether indicators of neural activity relevant to the processes outlined by the OLB model were related to outcomes hypothesized by the model.

Methods: Cyber cadets (N = 36) enrolled in a 3-day cyber engineering exercise organized by the Norwegian Defense Cyber Academy participated in the study. Differences in prospective

metacognitive judgments of cyber situational awareness, communication demands, and mood were compared between cyber cadets with high and low vagal tone. Vagal tone was measured at rest prior to the exercise. Affective states, communication demands, cyber situational awareness, and metacognitive accuracy were measured on each day of the exercise. Results: We found that cyber cadets with higher vagal tone had better metacognitive judgments of cyber situational awareness, imposed fewer communication demands on their teams, and had more neutral moods compared to cyber cadets with lower vagal tone.

Conclusion: These findings provide neuroergonomic support for the OLB model and suggest that it may be useful in education and training. Future studies should assess the effect of OLB-ing as an intervention on communication and performance.

KEYWORDS

vagal tone, cognitive control, cyber operations, neuroergonomics, metacognition, cyber situational awareness, emotion, cyber team communication

1 Introduction

Cyber operations unfold at superhuman speeds, which pose high demands on human cyber operators. Due to the growing global network coverage and increasing interconnectedness between cyber and physical domains, cyber operations are conducted in a complex socio-technical system consisting of diverse human-machine and human-human interactions. Performance in this socio-technical system is influenced by several factors across multiple contexts including unique challenges spanning cyber, physical, cognitive, and social domains (Jøsok et al., 2016, 2017; Agyepong et al., 2019). The resulting working-environment poses a complex selective pressure requiring a seemingly unique but currently understudied competency profile (Jøsok et al., 2017, 2019; Knox et al., 2017, 2018; Lugo and Sütterlin, 2018).

Organizations source their cyber operations to Security Operation Centers (SOCs) consisting of teams and organizational units that work around the clock to detect, assess, and respond to cyber threats. SOCs are usually hierarchically organized where analyst-level responsibilities such as detecting, investigating, and reporting on cyber threats are assigned to technical personnel (cyber operators), while decision-making responsibilities are assigned to other individuals higher up in the SOC hierarchy (Staheli et al., 2016). Thus, cyber operators are

responsible for establishing situational awareness (SA) during cyber threat situations and communicating their SA to decision-makers. According to the SA model (Endsley, 1995), establishing SA for decision-making in a socio-technical system is achieved in three levels (Figure 1A), where all levels must be achieved in order to have full SA. SA Level 1 entails perceiving the elements of the situation, SA Level 2 entails comprehending the relationship between these elements, and SA Level 3 entails using the comprehension to predict possible future situational states (Endsley, 1995).

Seven requirements for achieving cyber SA (CSA) for decision-making during cyber threat situations have been proposed (Barford et al., 2009). These requirements can be arranged under the SA model (Figure 1B) where the establishment of SA Level 1 starts with having perceived indicators of compromise (Barford et al., 2009). Establishing shared CSA during a cyber threat situation depends on both technical expertise and socio-cognitive abilities (Franke and Brynielsson, 2014; Jøsok et al., 2016, 2019). The outcome of cyber defense decision-making is based on how well the cyber operators can communicate their CSA to decision-makers that are often less technically competent (Knox et al., 2018; Ask et al., 2021a). Cyber operators must therefore be capable of flexibly transitioning between cyber-oriented analytical processes and socially oriented processes such as adjusting communication to the needs of the recipient. This makes communication for shared CSA a dynamic and challenging process where the same complex information is communicated in different ways depending on the recipient's background (Ahrend et al., 2016; Staheli et al., 2016). The Hybrid Space framework (Figure 2A) was developed to illustrate the interconnectedness between the cyber and physical (cyber-physical) domains, and the tension between strategic and tactical goals in decision-making and action, thus outlining the cognitive landscape that cyber operators must navigate (Jøsok et al., 2016).

Transitioning between quadrants in the Hybrid Space to relay technical information to non-technical individuals, will in theory require the cyber operator to switch between mindsets (Jøsok et al., 2016; Knox et al., 2018). Doing this effectively depends on the cyber operator's ability to monitor and regulate their cognitions. Metacognition is the ability to direct attention internally to observe one's own cognitions, emotions, and behaviors, and assess if they align with goals, and consciously regulate them if needed (Flavell, 1979; Efklides, 2008). Metacognition is required for establishing accurate SA (Endsley, 2020). Previous studies on cyber cadets have shown that self-location and movements in the Hybrid Space is predicted by

metacognition and self-regulation (Figure 2B; Knox et al., 2017, 2019; Jøsok et al., 2019) and team communication measurements (Lugo et al., 2017a). When individuals are processing information in different domains, their cognitive focus is in different quadrants of the Hybrid Space. Communicating across quadrants of the Hybrid Space (Figure 2C) requires constant re-adjustment of communication flow and message content (Jøsok et al., 2017; Knox et al., 2018).

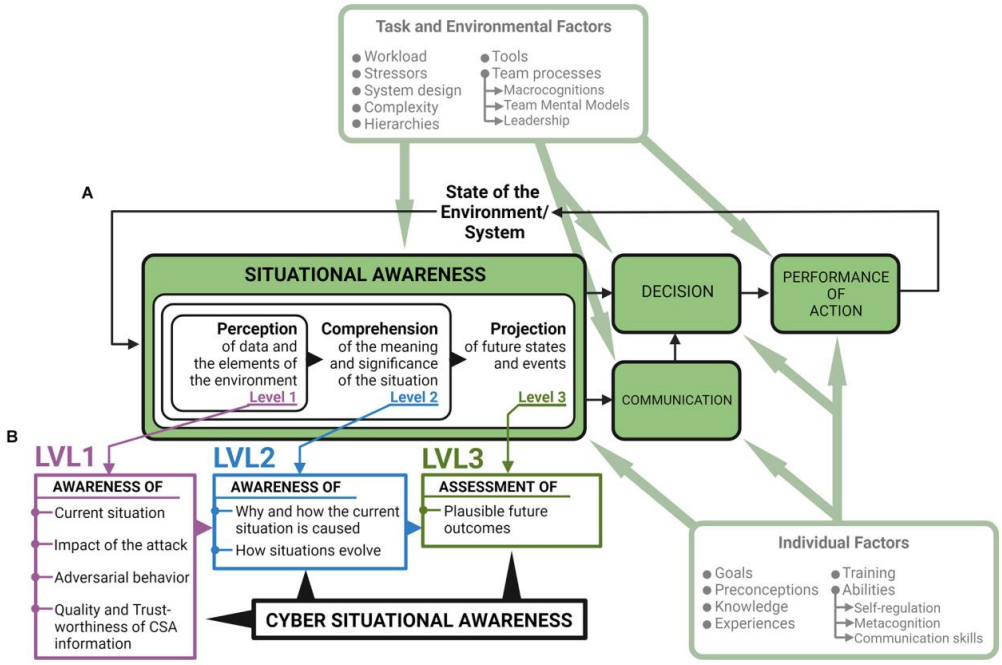

FIGURE 1

Situational Awareness (SA) model with suggested requirements for achieving Cyber Situational Awareness (CSA). (A) The SA model (Endsley, 1995). Communication has been added to the model due to its role in Security Operation Center (SOC) team decision-making (Knox et al., 2018; Ask et al., 2021a). (B) Seven requirements for achieving CSA during cyber threat situations (Barford et al., 2009). CSA generation, CSA sharing, and subsequent decision-making is affected by individual factors such as metacognition, self-regulation, and communication skills (Jøsok et al., 2016, 2019; Knox et al., 2017, 2018, 2019; Sütterlin et al., 2022) and task and environmental factors such as team-processes including macrocognitions, team mental models, and leadership (Jøsok et al., 2017; Lugo et al., 2017a; Ask et al., 2021a,b). Modified from Lankton (2007).

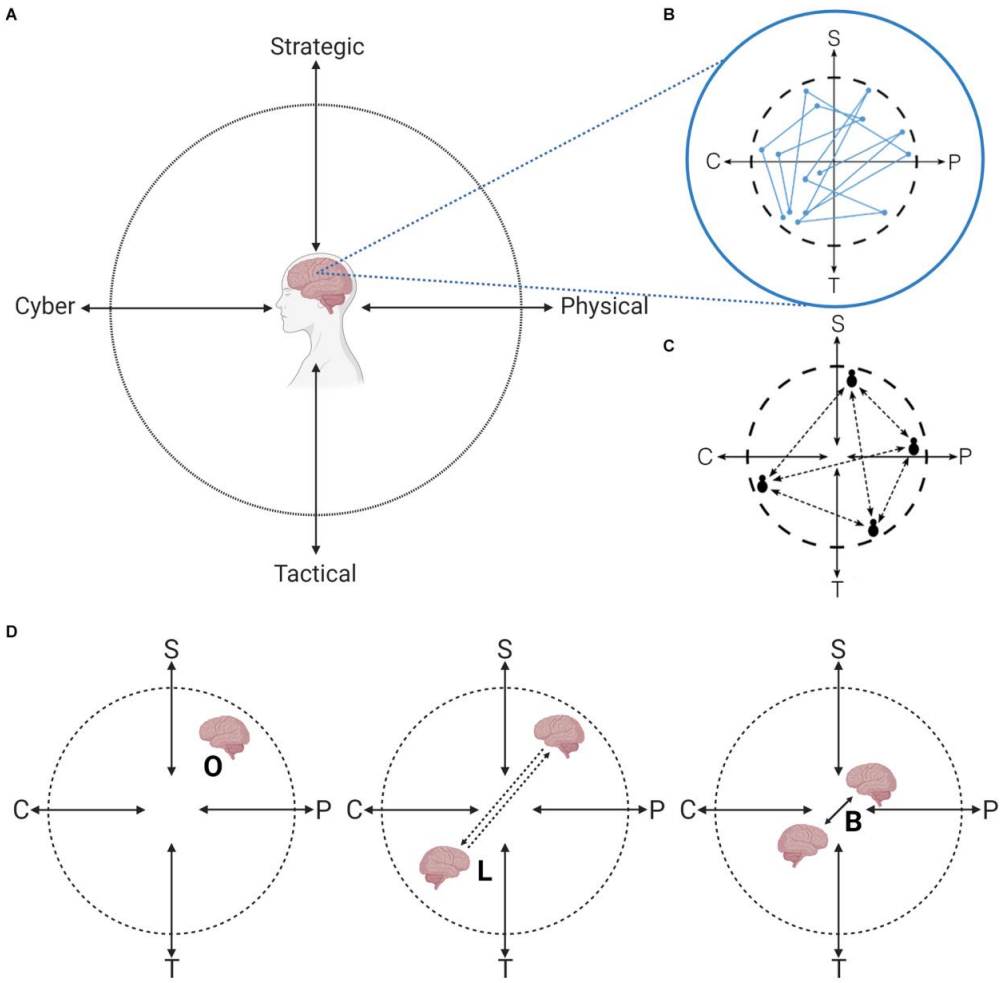

FIGURE 2

The Hybrid Space (HS) framework and the OLB model. (A) The Hybrid Space (HS; Jøsok et al., 2016). (B) Self-location and movement in the HS require metacognition and self-regulation (Knox et al., 2017, 2019; Jøsok et al., 2019). (C) Communication between individuals located in different quadrants of the HS. (D) The OLB model. S, Strategic; P, Physical; T, Tactical; C, Cyber; OLB, Orient, Locate, Bridge. Figure adapted from Jøsok et al. (2016) and Ask et al. (2021b, 2022). Created with BioRender.com

Recent reviews suggest that there is a lack of research on individual- and team-level SOC team communication and performance indicators (Agyepong et al., 2019; Ask et al., 2021a). The Orient, Locate, Bridge (OLB) model (Figure 2D; Knox et al., 2018) was developed based on the Hybrid Space framework to serve as a metacognitive tool supporting communication and sharing of CSA between individuals located in different quadrants of the Hybrid Space. The OLB model is a three- phase model where each phase builds on the previous phase to facilitate

efficient communication (Knox et al., 2018). In the orienting phase, the cyber operator applies metacognition to self-locate in the Hybrid Space to get a grasp of their current mindset (e.g., where their focus is, if they are stressed, etc.) and their CSA. In the locating phase, the cyber operator applies perspective taking to understand the specific information and communication needs of the recipient based on their location in the Hybrid Space. In the bridging phase, the cyber operator uses the insights from the orienting and locating phases as a guide for adapting communication style and content. This last phase ensures that communication can be grounded and CSA can be shared and calibrated between the cyber operator and the communication partner.

In more general terms, OLB-ing can be understood as a stepwise cognitive control process involving the deliberate (endogenously controlled) and flexible transition between attention to internal and self-referential states (e.g., Hybrid Space location, stress levels) and externally oriented cognitive processes. Cognitive control is the goal-directed coordination of task-relevant cognitive processes while inhibiting task-irrelevant automatic processes (Friedman and Robbins, 2022). In the brain, goal-directed cognitive processes are organized by a network of brain areas called the frontoparietal control network (FPN; Duncan, 2010; Menon and D'Esposito, 2022). This includes integrating attention to information from the external- present task environment and attention to internal-future goal-representations to coordinate externally directed cognitive processes and behaviors towards goal attainment (Nee and D'Esposito, 2016; Nee, 2021). On the other hand, attention to internal and self-referential information such as thoughts or the intensity and significance of one's emotional state is processed and maintained by the default mode network (DMN; Raichle et al., 2001; Raichle, 2015).

Both the FPN and DMN have anatomical hubs in the prefrontal cortex (PFC; Raichle, 2015; Menon and D'Esposito, 2022). The dorsolateral PFC (DLPFC) is one of the main hubs in the FPN (Menon and D'Esposito, 2022), while medial PFC structures (MPFC) constitute one of the main hubs of the DMN (Raichle, 2015). Activity in the FPN and DMN is often anticorrelated (Raichle et al., 2001; Fox et al., 2005; Chang and Glover, 2009), and DLPFC and MPFC activity is often anti-correlated during FPN-related tasks (Chen et al., 2013; Liston et al., 2014).

Both the DLPFC and MPFC are involved in metacognitive processes (Fleur et al., 2021). The DLPFC is specifically involved in metacognitive decision-making, while both DLPFC and MPFC are involved in prospective metacognitive judgments (Vaccaro and Fleming, 2018;

Fleur et al., 2021). Cognitive processes can go from being metacognitively controlled (Shimamura, 2008; Friedman and Robbins, 2022) to reactive (stimulus-driven) when individuals are subjected to stress or under emotional influence (Baek and Falk, 2018; Poth, 2021). Previous studies on cyber operators identified several emotional processes that may have differing effects on teamwork and communication (Lugo et al., 2016, 2017b, 2021; Ask et al., 2021b). Emotions can be interpreted according to intensity (arousal) and whether they are positive, negative, or neutral (valence; or mood), and are processed differently by DMN and FPN structures (Golkar et al., 2012; Terasawa et al., 2013; Fujimoto et al., 2021; Nejati et al., 2021). Stress reduces connectivity between the DMN and FPN (Chand et al., 2020), suggesting ways for how environmental pressures can disturb the flexible transition between self-referential and analytical processing.

From a neuroergonomics perspective, when faced with a challenging environment, the brain will find something akin to "the path of least resistance" to optimal performance (Botvinick, 2007; Wickens et al., 2015; Hagura et al., 2017; Khalil et al., 2019). This means initiating the cognitive processes and behaviors that are the least taxing to apply in order to reach a goal, given the environmental demands. If resulting in goal-attainment, they become part of a strategy for reaching the same goals under similar circumstances. The precision, combination, and order of the cognitions and behaviors, or trying new strategies to compare efficiency with older successful ones, are deliberately or unconsciously adjusted with experience via metacognitive and cognitive control processes (Flavell, 1979; Efklides, 2008; Khalil et al., 2019). Because the cybersecurity working-environment places such a heavy cognitive load on cyber operators (Jøsok et al., 2016; Agyepong et al., 2019), strategies for improved communication must not only be successful, but they must also be neuroergonomic to be sustainable. If the processes outlined by the OLB model are both successful and neuroergonomic in a cybersecurity working-environment, then they should be selected through evolutionary processes by the individuals working in those environments. If so, correlates of the neurocognitive processes underlying OLB-ing should be related to the outcomes predicted by the model (Knox et al., 2018).

Expert cyber incident response teams impose less communication demands on their teams compared to novices (Buchler et al., 2016; Lugo et al., 2017a). Because experts have spent more time in cybersecurity working-environments, they have also had more time to go through evolutionary cycles for selecting neuroergonomic approaches to make communication more

efficient. If the OLB model is neuroergonomic, the discrepancy in imposed communication demands between novices and experts may suggest that expert teams have a higher conscious or unconscious adoption rate of OLB-related cognitive processes for communication.

The main aim of this study is to assess some of the neurocognitive assumptions of the OLB model (Knox et al., 2018) to begin validating its potential as a neuroergonomic approach for CSA communication in cyber threat situations. This is done using peripheral proxies for DLPFC activity and FPN-DMN connectivity, and measurements of CSA, metacognition, and team communication. Prefrontally modulated vagal tone, quantified as vagally mediated heart rate variability (vmHRV), represents the beat to beat variations in heart rate that are influenced by the vagus nerve and modulated by the PFC (Appelhans and Luecken, 2006; Thayer et al., 2012). Vagal tone is an indicator of DLPFC activity (Brunoni et al., 2013a; Nikolin et al., 2017) and functional connectivity between the FPN and the DMN at rest (Chand et al., 2020). Associations have been found between metacognition and vagal tone in non-cyber tasks (Meessen et al., 2018). Vagal tone may therefore serve as a potential marker for the FPN-DMN interactions relevant for OLB-ing during cyber operations. Thus, we hypothesize that individuals with higher vagal tone have higher metacognitive accuracy and impose lower communication demands on their teams than individuals with lower vagal tone (hypothesis 1: H1).

The processing of emotional stimuli may influence cyber team performance (Lugo et al., 2016, 2017b, 2021; Ask et al., 2021b) for example by diverting attention away from externally directed and endogenously controlled cognitive processing and more towards stimulus-driven external (Poth, 2021) or internally directed self-referential processing (Baek and Falk, 2018). The DLPFC is involved in the self-report of valence (Nejati et al., 2021) and can be distinguished from other prefrontal structures based on this function (Terasawa et al., 2013; Fujimoto et al., 2021; Nejati et al., 2021). Higher vagal tone is associated with stress resilience (Hildebrandt et al., 2016) and endogenous control over attention during emotional distractors (Geisler and Kubiak, 2009; Park et al., 2012, 2013) known to elicit DMN processing (Winston et al., 2003; Zhou et al., 2020). Thus, we hypothesize that individuals with higher vagal tone, which reflects DLPFC function, will have different self-reported mood ratings than individuals with lower vagal tone (H2).

Metacognition is required for establishing accurate SA (Endsley, 2020). The Hybrid Space framework and the OLB model suggest that metacognition is required for efficient

communication of CSA with other individuals in the Hybrid Space (Jøsok et al., 2016; Knox et al., 2018). Metacognitive accuracy, how correctly an individual is in evaluating their own performance, can manifest as correctly judging performance as bad or good. Because both establishing SA and sharing CSA through communication is reliant on metacognition (Jøsok et al., 2016; Knox et al., 2018; Endsley, 2020), we hypothesize that individuals with more correct CSA ratings have higher metacognitive accuracy than individuals with less correct CSA ratings (H3).

2 Methods

2.1 Participants and setting

Cyber cadets (N = 36) that participated in the Norwegian Defense University College, Cyber Academy (NDCA) annual Cyber Engineering Exercise (CEX) were recruited for the study. The CEX is conducted during the fifth semester for graduating students at the NDCA. By this stage in their bachelor degree education, they have chosen and begun their specialized training. The specializations are military Information Communication Technology (ICT) systems and Cyber Operations. The specialization split was eleven (11) cadets pursuing Cyber Operations and the remaining twenty-five (25) military ICT. The CEX is intended to provide cyber cadets with a deeper understanding and appreciation for the breadth of a cyber engineer's profession and tasks in a military operative context. In particular, they develop more advanced technical skills in the domain of cyber operations and gain insight into how incidents occurring in the military cyber domain may influence and be influenced by operations in other military and non-military domains. The cadets learn how to make good judgments, give honest recommendations through clear communication, and make good decisions that result in the effective use of cyber tools and technologies to achieve operational goals. The CEX was divided into two independent operations: military ICT Operations and Cyber Operations. Both operations lasted for 5 days (see Figure 3 for an overview of the CEX and study).

For the CEX, the cadets were divided into two platoons, with each platoon consisting of three teams. One platoon participated in military ICT Operations for 5 days, while the other platoon participated in Cyber Operations for 5 days. Each team consisted of six individuals that were composed of a mix of military ICT and Cyber Operations cadets. The first 2 days involved orders, preparation, and training. This was followed by 3 days of mission execution. On day 6, there was a rotation where the platoons switched operations so that the platoon that started out

in the military ICT operations track switched to the Cyber Operations track, and vice versa. Participants per rotation (n = 16).

The present study took measurements when each platoon was undertaking the Cyber Operations track of the CEX. The defensive Cyber Operations involved scenario-based investigations of a network intrusion where the cadets experienced technical and operational uncertainty and complexity related to exploitation of their military cyber domain. After the initial preparation and training phase, the cadets deployed to a notional area of operations. For the CEX, this took the form of teams being assigned separate rooms, where the cadets deployed network sensor capabilities into their infrastructure and began targeted network surveillance based on their operational assessment and plans. The scenario developed allowing cadets to conduct different analytical tasks and investigate specific types and instances of network traffic. The cadets advanced through the exercise by solving these analytical and investigative missions. Each day the exercise would begin at 8:00 a.m. and end at 10:00 p.m., with the level of intensity (operational uncertainty and technical complexity) imposed upon the cadets gradually increasing each day. There were organized regular breaks for eating three times per day, once in the morning, once around noon, and once in the evening, where all the cadets participating in the Cyber Operations track could eat simultaneously. If any of the teams operated in shifts, this was organized within the teams, but usually meant that someone would bring with them food from the cafeteria to the individual(s) that did not join the common breaks.

Data from four participants were excluded from the analysis. Data from one participant were excluded for only providing baseline HRV data and not filling out daily questionnaires. A second participant was excluded due to measurement error during the recording of inter-beat intervals. Lastly, two participants were excluded due to not filling out relevant questionnaires for most of the exercise.

2.2 Materials and procedure

On the first day of the study, 2 days before the start of the CEX all participants answered a battery of questionnaires followed by recording of cardiac activity for quantification of vmHRV. Affective state, performance rating, team, and CSA measurements were collected on each day of the exercise. On the morning of each day of the exercise (approx. 7:30 a.m.), participants answered questionnaires pertaining to their affective state and judgments about

how well they think they would perform. At the end of each day (approx. 9:00 p.m.), participants answered questionnaires pertaining to judgments about how well they thought they had performed, team-workload demands, and CSA.

2.2.1 Vagally mediated heart rate variability

Cardiac activity was recorded at rest for 7 min 2 days prior to the start of the exercise using the Alive Software (AliveTM by Somatic Vision, Inc., Encinitas, CA, United States) biofeedback system. Alive measures heart rate through photoplethysmography. The recordings were conducted one at a time in a separate room that was secluded from other activities. Participants were seated in comfortable chairs.

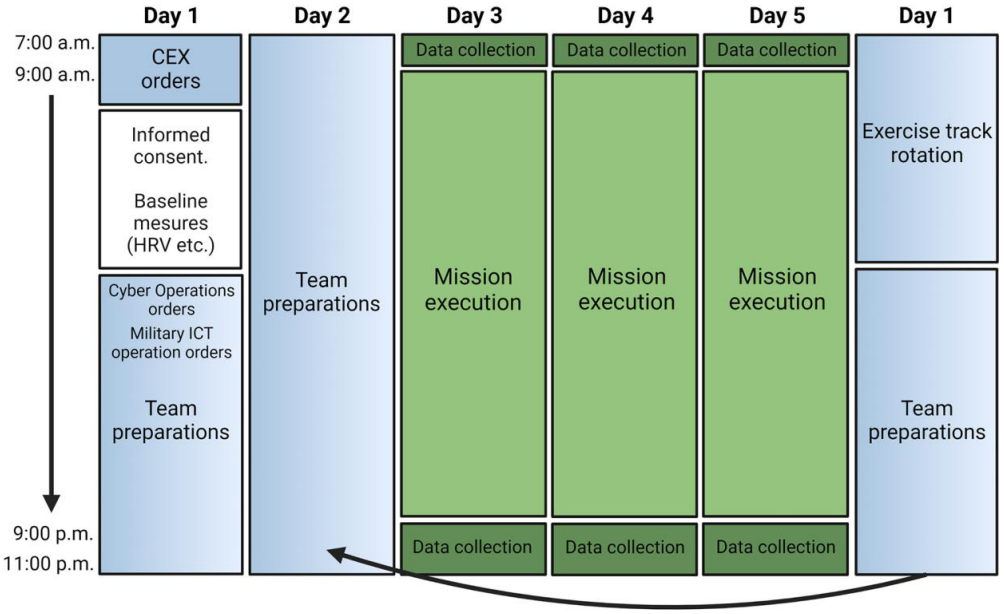

FIGURE 3

Overview of the study and the cyber engineering exercise. CEX, Cyber engineering exercise; HRV, Heart rate variability.

Three finger sensors were placed on the participant's non-dominant hand, after which they were told to rest for some minutes by themselves. After giving the instructions, the researcher left the room for the entirety of the 7-min recording period.

Five minutes in the middle of the recordings were used for quantification of vmHRV. Inter-beat intervals were extracted via R-peak detection and HRV was analyzed using ARTiiFACT software (Kaufmann et al., 2011). Artifacts were detected and corrected according to established methods (Berntson and Stowell, 1998). The high frequency component of HRV (HFHRV: 0.15–0.40 Hz, ms2) and the time-domain measure of HRV, root-mean-squares of successive NN differences (RMSSD), were extracted following recommendations by the Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology (1996). Both indices are commonly used as indicators of vagal tone. We were mainly interested in HFHRV as RMSSD is suggested to also be influenced by sympathetic input (Berntson et al., 2005; Williams et al., 2019) and evidence relating transcranial stimulation over DLPFC to prefrontally modulated vagal tone used HFHRV as an indicator (Brunoni et al., 2013a; Nikolin et al., 2017). HFHRV and RMSSD are usually highly correlated (Goedhart et al., 2007), thus we included RMSSD in the initial analysis to check for this correlation as an indicator of vmHRV index quality.

2.2.2 Self-assessment manikin

The self-assessment manikin (SAM) is a non-verbal assessment of affective states (Bradley and Lang, 1994). It consists of three pictorial items: Valence (mood; ranging from very negative to very positive), arousal (activation; ranging from very low to very high), and dominance (control; ranging from very low to very high) that are each measured on a 9-point scale, where participants indicate what they feel in the moment for each item. The SAM was administered at the beginning of each day during the exercise. The mean for mood, activation, and control scores were computed for each individual for all 3 days.

2.2.3 Judgment of performance

A prospective judgment of performance (JOP) questionnaire was used to assess the participants' prospective estimations of how well they would perform. The JOP questionnaire is used to assess how confident participants are about their future performance (e.g., Sütterlin et al., 2022). The questionnaire consisted of six items that were handed out at the beginning and at the end of each day, and included questions such as "How well do you think you will do?", and "How well will my team do?". The prospective JOP questionnaires were handed out at the beginning of each day. On each item, participants indicated their performance on a scale ranging from 0% to 100%.

For this study, daily perspective JOP at the individual and team level were z-transformed before averaging to generate prospective self-assessment (JOP) and team assessment (JOP team) JOP scores.

2.2.3 Team workload questionnaire

Establishing CSA is a team effort (McNeese et al., 2011; Champion et al., 2012; Jøsok et al., 2017). The team workload questionnaire (Sellers et al., 2014) was administered at the end of each day to assess how participants experienced workload demands on team tasks during the exercise. The items are scored on an 11-point Likert scale ranging from very low to very high. High scores indicate higher levels of subjective workload. The team workload questionnaire consists of six subscales divided into two dimensions, the Teamwork component (communication, coordination, team performance monitoring) and Task-Team component (time-share, team emotion, team support). Average scores for all 3 days were generated based on these subscales. The team workload questionnaire shows good reliability (Sellers et al., 2014). Reliability was also good in the present study (Cronbach's $\alpha = 0.839$). The perceived team success item from the NASA Task Load Index assesses retrospective confidence judgments of team performance (Hart and Staveland, 1988) and was also included in the daily team workload questionnaire.

2.2.4 Cyber situational awareness questionnaire for analysts

To assess CSA among participants, the CSA questionnaire for analysts (Lif et al., 2017) was administered at the end of each day. The questionnaire consists of a combination of qualitative and quantitative questions. Among the questions included in the CSA questionnaire, the following four were used for the purpose of study 1: "Where in the Kill Chain is attack 1?" (Kill chain), "How critical is the system?" (System critical), "How Severe is the Attack?" (Attack severity), "How urgent is it to take action?" (Action urgency).

For all CSA items, participants had to indicate which estimate they thought was correct on a Likert scale from 1 to 7. For the Kill chain item, participants had to indicate on a Kill chain flow chart where the attack was (seven options). Their answers were converted to a score from 1 to 7 depending on where in the kill chain they indicated that the attack was, with 7 corresponding to "Action on objectives", which is the last step in the kill chain.

Participants were instructed to leave items they did not know what to answer blank, but to write their participant ID on the front page, in which case those items were coded as 0 (thus making

CSA items range from 0 to 7). Responses were coded as missing if the entire form was left empty. Reliability for CSA items was good (Cronbach's $\alpha = 0.771$).

The correct answer for the kill chain item was 7. The correct answer for attack severity was 7. The correct answer for action urgency was 7. The correct answers for system critical was 6. CSA scores for the participants were generated by scoring correct assessments on the questionnaires for each day as 1 and erroneous assessments as 0. The scores for each day were z-transformed before averaging to generate CSA scores. Kill chain estimations could in theory be inferred from exercise instructions thus being too easy to tax metacognitive abilities. Metacognitive estimations for easy tasks are less subject to bias than for harder tasks (Fleur et al., 2021). Accounting for this possible confounder, a second CSA score was generated through the same steps as for the initial CSA variable except kill chain scores were excluded, resulting in a CSA2 variable.

The same procedure was done at the team level, where team CSA scores were generated based on the averaged correct CSA estimations for the entire team, and a team CSA2 variable was generated by excluding kill chain scores.

Due to the structure of the exercise, participants would only be able to make informed judgments on the attack severity item on days 4 and 5, while informed judgments on the kill chain, how critical the system was, and action urgency were possible on all 3 days. There was a very low number of correct CSA answers on day one which was likely due to participants spending time on sensor deployment and only starting to establish CSA during the tail end of the day.

2.2.5 Metacognitive accuracy

The individual and team CSA scores for each day, and the personal and team JOP scores for each day were used to generate the metacognitive accuracy (MCA) scores. CSA scores were range converted to a 0–100 scale. MCA scores were calculated as a deviation score using the approach described by Meessen et al. (2018). Briefly, scores were generated by squaring the product from subtracting the daily JOP scores (ranging from 0 to 100) for each day from the daily CSA scores (ranging from 0 to 100) for each day. This was followed by dividing by 100, using the following formula:

$$MCA = \frac{(Daily\ CSA\ score - daily\ JOP)^2}{100}$$

Because JOP scores are subtracted from the accuracy scores, CSA performance that matches performance estimations will give a score of zero, while performance estimations that are below or above CSA performance will give a score that deviates from zero. Squaring the product returns an equal positive value for all negative and positive equivalent deviations from zero. Thus, a low MCA score indicates high metacognitive accuracy, and a high MCA score indicates low metacognitive accuracy regardless of inaccuracy resulting from overconfidence or underconfidence. At the team level, a high metacognitive accuracy means having high accuracy when judging team-level CSA.

The z-transformed MCA scores for each day were averaged to generate two sets of MCA variables, MCA and team MCA. While the DLPFC is needed for making prospective metacognitive judgments about performance (Vaccaro and Fleming, 2018), metacognition for team processes is suggested to rely on different neural systems than those for individual metacognitions (Shea et al., 2014). Following the rationale for generating the CSA variables, two separate MCA variables were generated for each set: MCA and team MCA, and MCA2, and team MCA2, where the MCA2 variables excluded Kill chain scores.

2.3 Statistical analysis

Descriptive statistics were generated for all variables and presented in tables as mean, standard deviation (SD), minimum (min), and maximum (max) values for continuous and numerical variables, and frequencies and percentages (%) for ordinal variables.

Inspecting box-and-whisker plots of variables identified one outlier (value > 1.5 times the interquartile range above the upper quartile) for HFHRV. After re-inspection of inter-beat interval recording and artifact analysis for the HFHRV outlier, it was concluded that measurement error was unlikely, thus, HFHRV was log-transformed to pull in the outlier. Follow-up inspecting box-and-whisker plots confirmed that the log-transformed variable no longer contained extreme values. All subsequent analyses were performed on the log-transformed HFHRV variable.

For the purpose of the present study, we were mainly interested in the communication demand item of the team workload questionnaire due to reported differences between expert and novice teams (Buchler et al., 2016; Lugo et al., 2017a), and because the OLB model aims to reduce communication demands by making communication more efficient (Knox et al., 2018).

Because establishing CSA is a team effort (McNeese et al., 2011; Champion et al., 2012; Jøsok et al., 2017), all team workload questionnaire items were included in the analysis to assess the relationship between team workloads and team-level CSA and MCA. All variables were z-transformed for analysis. Shapiro-Wilk test of normality and confirmatory visual inspection of bar-graph distribution plots revealed that many of the variables were not normally distributed. Subsequent correlational analyses were parametric for relationships between normally distributed variables (SAM, HFHRV, MCA2, team MCA, team performance monitoring, team support demand), and nonparametric for all other relationships including between normally and not normally distributed variables.

Pearson and Spearman correlation analyses (2-tailed) was performed simultaneously for all variables and results were presented in a heat map as Spearman correlation coefficients (ρ) for nonparametric associations and Pearson's correlation coefficients (r) for parametric associations. RMSSD was included in the correlation analysis to check for associations with HFHRV but was not included in the heat map. Separate linear regression analyses were performed for significant correlations. All regressions were checked for violation of assumptions regarding homoscedasticity, normality, linearity, and multicollinearity.

2.3.1 Analysis of group differences

The differences between high and low HFHRV groups were assessed using Pillai's MANOVA and ANOVA for parametric comparisons and Kruskal-Wallis H tests for nonparametric comparisons. Results for the Pillai test were reported as Pillai's Trace ($Trace_{Pillai}$), approximate F(degrees of freedom 1, degrees of freedom 2; $F_{(df1,\ df2)}$), and p-values. Results for ANOVA were reported as F statistic(df), p-values, and effect size. Kruskal-Wallis H test was reported as H statistic(df), p-values, and effect size.

Effect size (η^2) for the Kruskal-Wallis H test was calculated as ($H-k$ + df)/($n-k$); where H was the Kruskal-Wallis statistic, k was the number of groups, and n was the total number of observations (32). Effect size (ω^2) for ANOVA was calculated as (sum of squares between − (k − 1) mean square within)/(sum of squares total + mean square within). Dunn's post-hoc test was used to assess significant relationships for non-parametric variables between groups and was reported as z-statistic and Bonferroni adjusted p-values (p_{bonf}). Tukey's post-hoc test was used to assess significant relationships for parametric variables between groups and was reported as mean difference (MD) and pbonf.

Violation of assumptions for MANOVA analyses were assessed with Box's M-test for homogeneity and Shapiro-Wilk test for multivariate normality. Violation of assumptions for ANOVA analyses were assessed with Levene's test for equality of variance and by inspecting Q-Q plots of residuals. There were no violations at any time.

2.3.2 Comparisons between low and high vagal tone groups

A median split was performed on the HFHRV variable to divide the sample into high HFHRV (HFHRV > median) and low HFHRV (HFHRV ≤ median) groups according to whether they had values above or below the median. This method is commonly used in studies aiming to assess vagal tone-related group differences in cognitive performance (Hansen et al., 2003, 2009; Pu et al., 2010; Williams et al., 2017). To test the hypotheses that individuals with higher vagal tone have higher metacognitive accuracy and impose lower communication demands on their teams than individuals with lower vagal tone (H1), and that individuals with higher vagal tone have different self-reported mood ratings than individuals with lower vagal tone (H2), ANOVAs were performed using vagal tone groups as fixed factors and mood, communication demand, and MCA variables as dependent variables. Metacognition has been suggested to be required for SA (Endsley, 2020) so CSA variables were also included in the analysis.

2.3.3 Comparisons between low and high metacognitive accuracy groups

Both vagal tone and prospective metacognitive judgments are influenced by DLPFC activity (Brunoni et al., 2013a; Nikolin et al., 2017; Vaccaro and Fleming, 2018; Chand et al., 2020). However, vagal tone can be influenced by processes other than DLPFC activity (Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology, 1996), but prospective metacognitive judgments are dependent on DLPFC activity (Fleur et al., 2021). Thus, a median split was performed on MCA and team MCA to assess whether the vagal tone was different between individuals with high and low MCA and team MCA. Due to low MCA scores meaning high accuracy, individuals below the median had high accuracy, and individuals above the median had low accuracy.

2.3.4 Comparisons of MCA between CSA accuracy groups

In the present study, high metacognitive accuracy (indicated by low MCA scores) could be due to accurately judging good or bad performance (e.g., having 0% correct answers and judging performance at 0%, and having 100% correct answers and judging performance at 100% would both give a score of 0). A median split was performed on the summed total of correct CSA

ratings for both days to divide the sample into two groups (CSA accuracy) according to whether they were less accurate or more accurate in their CSA ratings. To test the hypothesis that individuals with higher metacognitive accuracy have more correct CSA ratings than individuals with lower metacognitive accuracy (H3), two separate analyses were performed using MCA or MCA2 as a dependent variable and CSA accuracy as the fixed factor. This procedure was repeated for team MCA variables also, where the median split was performed on the summed total of correct team CSA ratings after averaging for the number of team members.

Alpha levels for hypothesis testing were set at the 0.05 level for all analyses. All data were analyzed using JASP version 0.15 (JASP Team, 2021).

3 Results

3.1 Descriptive statistics

Descriptive statistics for HRV indices, SAM, team workload questionnaire, JOP, CSA, and MCA variables are presented in Table 1.

3.2 Correlations between HFHRV, SAM, team workload questionnaire, JOP, CSA, and MCA scores

HFHRV was significantly associated with RMSSD ($\rho = 0.928$, $p < 0.001$), indicating that the indices were of good quality. Spearman and Pearson correlations between HFHRV, SAM, team workload questionnaire, JOP, CSA, and MCA variables are presented in Figure 4.

HFHRV was significantly and negatively associated with mood ($p = 0.003$). There were no significant relationships between HFHRV and activation ($p = 0.841$), or control ($p = 0.457$). There were no significant correlations between mood and activation ($p = 0.602$) or control ($p = 0.382$), or between activation and control ($p = 0.759$).

HFHRV was significantly and negatively associated with perceived team success ($p = 0.017$). Mood was significantly and positively associated with perceived team success ($p = 0.029$). Neither HFHRV ($p = 0.142$), mood ($p = 0.086$), activation ($p = 0.214$), nor control ($p = 0.091$) were associated with communication demand. Neither HFHRV, mood, nor activation was associated with any other team workload variables. Control was significantly and negatively associated with time-share demand ($p = 0.043$) but not any other team workload questionnaire items.

HFHRV was not significantly associated with JOP ($p = 0.122$) or JOP team ($p = 0.106$). The mood was significantly and positively associated with JOP ($p = 0.004$) and the JOP team ($p < 0.001$). JOP was not significantly associated with activation ($p = 0.457$), nor control ($p = 0.135$). JOP team was not significantly associated with activation ($p = 0.567$), nor control ($p = 0.505$).

HFHRV was significantly and positively associated with team CSA2 ($p = 0.035$). HFHRV was not significantly associated with CSA ($p = 0.597$), CSA2 ($p = 0.238$), nor team CSA ($p = 0.516$). The mood was significantly and negatively associated with team CSA2 ($p = 0.029$). Mood was not significantly associated with CSA ($p = 0.706$), CSA2 ($p = 0.384$), and nor team CSA ($p = 0.342$). No other significant associations between SAM variables and CSA variables.

Perceived team success was significantly and negatively associated with team CSA2 ($p = 0.033$). No other significant associations between team workload questionnaire scores and CSA scores.

TABLE 1 Descriptive statistics for HRV, SAM, TWLQ, JOP, CSA, and MCA variables (N = 32).

					High HFHRV		Low HFHRV	
Variables	Mean	SD	Min	Max	Mean	SD	Mean	SD
Mean RR	935.73	174.06	677.63	1,342.76	1,023.57	175.60	847.89	123.78
HFHRV	1,473.19	1,501.76	124.82	5,079.73	2,547.50	1,471.22	398.88	185.10
HFHRV_log	6.75	1.09	4.82	1.62	7.65	0.68	5.86	0.54
RMSSD	60.92	28.38	32.08	136.95	82.05	26.03	39.80	5.87
CSA	0.23	0.17	0.00	0.75	0.26	0.19	0.20	0.14
CSA2	0.18	0.17	0.00	0.66	0.22	0.19	0.14	0.15
Team CSA	0.23	0.67	0.18	0.36	0.24	0.07	0.22	0.05
Team CSA2	0.18	0.84	0.74	0.33	0.21	0.07	0.15	0.08
Z-Transformed variables								
HFHRV	−0.00	1.00	−1.76	1.62	0.81	0.62	−0.81	0.50
RMSSD	0.00	1.00	−1.01	2.67	0.74	0.91	−0.74	0.20
Mood	0.00	1.00	−2.02	1.84	−0.47	0.90	0.47	0.87
Activation	−0.00	1.00	−2.20	1.90	−0.17	1.01	0.17	0.98
Control	−0.00	1.00	−2.08	2.44	−0.21	0.97	0.21	1.01
Judgment of performance	−0.00	1.00	−1.91	2.36	−0.16	0.91	0.16	1.08
Judgment of performance team	−0.00	1.00	−1.69	2.21	−0.25	1.08	0.25	0.86
Communication	0.00	1.00	−2.53	1.32	−0.49	1.06	0.49	0.63

demand								
Coordination demand	0.00	1.00	−2.08	2.08	−0.26	0.98	0.26	0.97
Team performance monitoring	0.00	1.00	−1.79	2.07	−0.17	0.94	0.16	1.05
Time-share demand	0.00	1.00	−1.32	2.33	−0.01	0.94	0.01	1.08
Team support demand	0.00	1.00	−1.90	2.09	0.04	0.83	−0.04	1.15
Team emotion demand	0.00	1.00	−2.43	1.94	0.05	1.14	−0.05	0.87
Perceived team success	−0.00	1.00	−2.00	1.72	−0.54	0.79	0.50	0.91
CSA	0.00	1.00	−1.36	3.04	0.16	1.14	−0.16	0.83
CSA2	−0.00	1.00	−1.07	2.73	0.23	1.09	−0.23	0.85
Team CSA	0.00	1.00	−0.76	1.92	0.17	1.11	−0.17	0.87
Team CSA2	−0.00	1.00	−1.34	1.75	0.35	0.09	−0.35	0.99
Metacognitive accuracy	−0.00	0.663	−0.79	1.95	−0.08	0.75	0.08	0.56
Metacognitive accuracy2	0.00	0.703	−1.07	1.58	−0.17	0.69	0.17	0.69
Team metacognitive accuracy	0.00	2.168	−4.52	4.55	−0.89	1.15	0.89	2.5
Team metacognitive accuracy2	−0.00	0.800	−1.44	1.35	−0.38	0.46	0.38	0.89

Notes. HRV, Heart rate variability; SAM, self-assessment manikin; TWLQ, Team workload questionnaire; JOP, judgment of performance; RR, R-to-R peak interval; HFHRV, High frequency component heart rate variability; _log, log-transformed; RMSSD, Root mean square of successive RR differences; CSA, Cyber situational awareness; CSA2 and Metacognitive accuracy2, CSA and Metacognitive accuracy without Kill chain scores.

HFHRV was significantly and negatively associated with MCA2 ($p = 0.031$), team MCA ($p = 0.032$), and team MCA2 ($p = 0.012$). HFHRV was not significantly associated with MCA ($p = 0.156$). Mood was significantly and positively associated with MCA ($p = 0.004$), MCA2 ($p = 0.003$), team MCA ($p < 0.001$), and team MCA2 ($p = 0.004$). No other SAM variables were associated with MCA variables. Perceived team success was significantly and positively

associated with team MCA ($p < 0.001$) and team MCA2 ($p < 0.001$). No other associations between team workload questionnaire and MCA variables were significant.

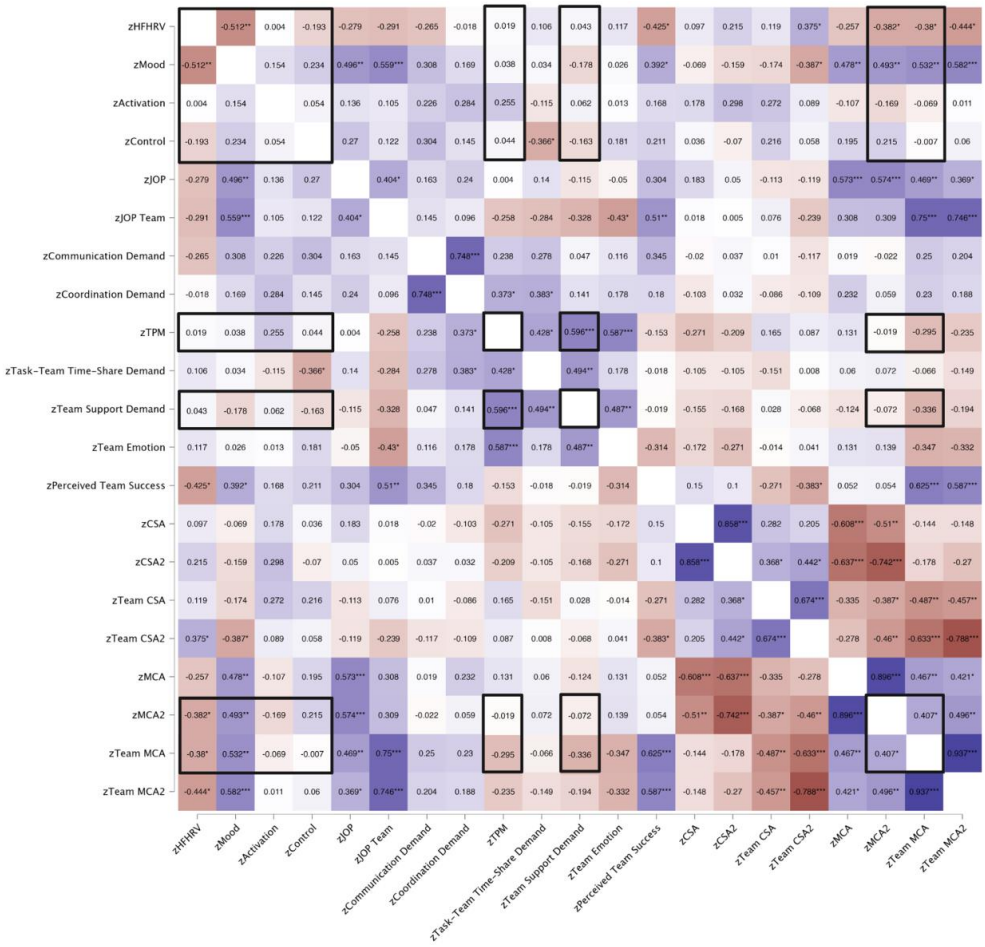

FIGURE 4

Correlation heat map for HRV, SAM, team workload questionnaire, JOP, CSA, and MCA variables. 2-tailed. *$p < 0.050$, **$p < 0.010$, ***$p < 0.001$. Matrix numbers are Pearson correlation coefficients (r) and Spearman's correlation coefficients (ρ). Pearson's r is indicated with black frames. Red, Negative correlation; Blue, Positive correlation. Color intensity indicates the strength of correlation. HFHRV, High frequency component heart rate variability; JOP, Judgment of performance; TPM, Team performance monitoring; CSA, Cyber situational awareness; MCA, Metacognitive accuracy; CSA2 and MCA2, CSA and MCA without Kill chain scores.

Separate linear regression analysis was performed for significant relationships. Table 2 shows the results for the regression analyses.

HFHRV was a significant negative predictor of mood ($p = 0.003$), perceived team success ($p = 0.034$), MCA2 ($p = 0.031$), team MCA ($p = 0.032$), and team MCA2 ($p = 0.012$). HFHRV was not a significant predictor of team CSA2 ($p = 0.064$). Figure 5 shows regressions for HFHRV and mood, MCA2, team MCA, and team MCA2.

TABLE 2 Results for linear regression analyses ($N = 32$).

Predictor	Dependent variable	β	*p*	R^2_{Adj}	$F(1)$
HFHRV	Mood	−0.512	0.003	0.237	10.644
HFHRV	Perceived team success	−0.382	0.034	0.116	4.949
HFHRV	MCA2	−0.382	0.031	0.117	5.122
HFHRV	Team MCA	−0.380	0.032	0.116	5.049
HFHRV	Team MCA2	−0.441	0.012	0.167	7.223
HFHRV	Team CSA2	0.331	0.064	0.080	3.702
Mood	JOP	0.481	0.005	0.206	9.020
Mood	JOP team	0.518	0.002	0.244	10.999
Mood	Perceived team success	0.384	0.033	0.118	5.018
Mood	MCA	0.424	0.016	0.152	6.575
Mood	MCA2	0.493	0.004	0.217	9.609
Mood	Team MCA	0.532	0.002	0.259	11.858
Mood	Team MCA2	0.569	<0.001	0.302	14.394
Mood	Team CSA2	−0.310	0.085	0.066	3.180
Perceived team success	Team MCA2	0.571	<0.001	0.303	14.058
Perceived team success	Team MCA	0.567	<0.001	0.298	13.760
Perceived team success	Team CSA2	−0.299	0.102	0.058	2.853

Notes. HFHRV, High frequency component heart rate variability; MCA, Metacognitive accuracy; CSA, Cyber situational awareness; JOP, Judgments of performance; CSA2 and MCA2, CSA and MCA without Kill chain scores.

Mood was a significant positive predictor of JOP ($p = 0.005$), JOP team ($p = 0.002$), perceived team success ($p = 0.033$), MCA ($p = 0.016$), MCA2 ($p = 0.004$), team MCA ($p = 0.002$), and team MCA2 ($p < 0.001$). Mood was not a significant negative predictor of team CSA2 ($p = 0.085$).

Perceived team success was a significant positive predictor of team MCA ($p < 0.001$) and team MCA2 ($p < 0.001$). Perceived team success was not a significant predictor of team CSA2 ($p = 0.102$).

3.3 Between-group comparisons

Table 3 shows the results from all the comparisons.

3.3.1 H1: Individuals with higher vagal tone have higher metacognitive accuracy and impose lower communication demands on their teams than individuals with lower vagal tone

Pillai's MANOVA was performed using mood, MCA2, and team MCA as dependent variables and vagal tone groups as fixed factor; the Kruskal-Wallis H tests were performed using MCA, team MCA2, CSA, CSA2, team CSA, team CSA2, and communication demand as dependent variables and vagal tone groups as fixed factor. The Pillai test for vagal tone groups was significant ($Trace_{Pillai} = 0.269$, $F(3,28) = 5.863$, $p = 0.030$). Figures 6A–D shows interval plots for differences between high and low HFHRV groups for MCA, CSA, and communication demand variables.

Communication demand was significantly different between low and high HFHRV groups ($p = 0.006$). Dunn's post- hoc test revealed that individuals with low HFHRV posed significantly more communication demands on their team compared to individuals with high HFHRV ($z = 2.748$, $p_{bonf} = 0.003$).

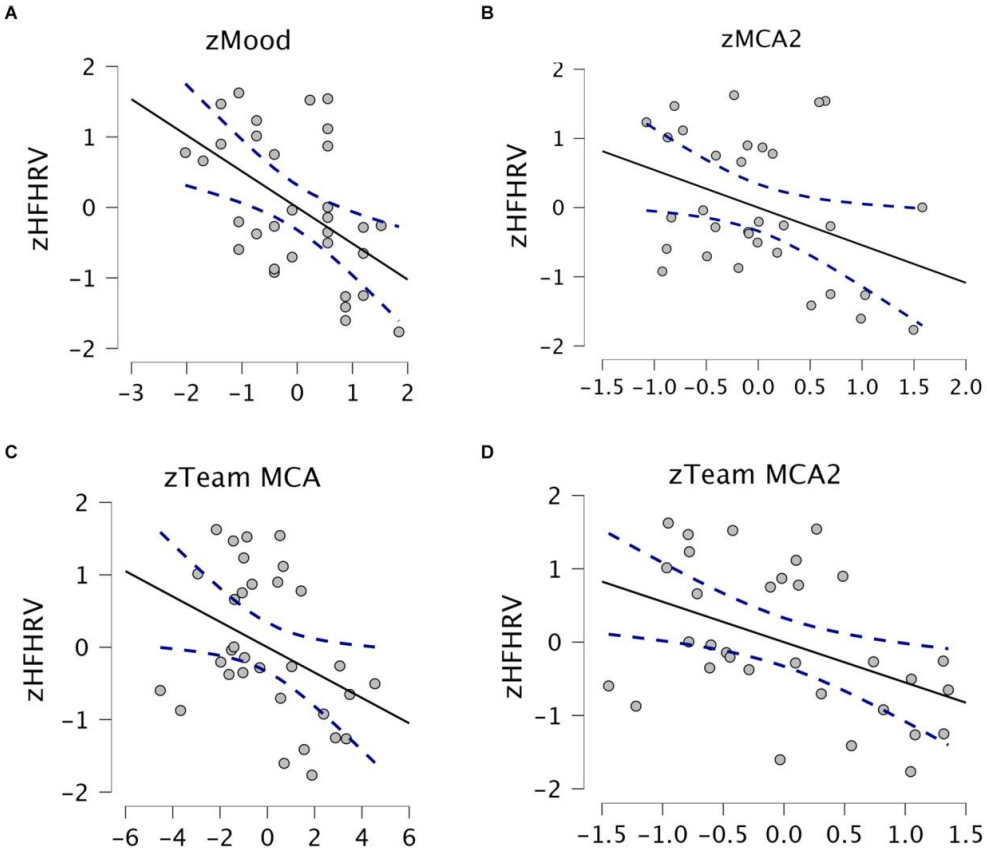

FIGURE 5

Scatter plots with regression lines. Stapled lines are 95% confidence intervals. (A) HFHRV and mood. (B) HFHRV and MCA2. (C) HFHRV and team MCA. (D) HFHRV and team MCA2. HFHRV, High frequency component heart rate variability; MCA, Metacognitive accuracy; MCA2, MCA without Kill chain scores.

Team MCA was significantly different between low and high HFHRV groups (p = 0.017). Tukey's post- hoc test revealed that individuals with low HFHRV had significantly higher team MCA scores than individuals with high HFHRV (MD = 1.78, p_{bonf} = 0.017). Team MCA2 was significantly different between low and high HFHRV groups (p = 0.008). Dunn's post-hoc test revealed that Individuals with low HFHRV had significantly higher team MCA2 scores compared to individuals with high HFHRV (z = 2.63, p_{bonf} = 0.004). Team CSA2 was significantly different between low and high HFHRV groups (p = 0.022). Dunn's post-hoc test revealed that Individuals with low HFHRV had significantly lower team CSA2 scores compared to individuals with high HFHRV (z = 2.28, p_{bonf} = 0.011).

3.3.1.1 Individuals with higher metacognitive accuracy have higher vagal tone than individuals with lower metacognitive accuracy

HFHRV was significantly different between low and high MCA groups ($p = 0.041$). Tukey's post-hoc test showed that individuals with lower metacognitive accuracy had lower HFHRV compared to individuals with higher metacognitive accuracy (MD = −0.71, $p_{bonf} = 0.041$).

TABLE 3 Comparison of differences between groups (N = 32).

		Kruskal-Wallis test			Dunn's *post-hoc*	
Fixed factors	Dependent variables	$H(1)$	p	η^2	z	p_{bonf}
Vagal tone groups (low, high)	Communication demand	7.549	0.006	0.218	2.74	0.003
	CSA	0.645	0.422	−0.011	-	-
	CSA2	1.484	0.223	0.016	-	-
	Team CSA	0.862	0.353	−0.004	-	-
	Team CSA2	5.207	0.022	0.140	−2.28	0.011
	MCA	1.841	0.175	0.028	-	-
	Team MCA2	6.960	0.008	0.198	2.63	0.004
CSA accuracy (low, high)	MCA	6.937	0.008	0.197	2.63	0.004
Team CSA accuracy (low, high)	Team MCA2	5.205	0.023	0.140	2.28	0.011
		Pillai's MANOVA			Tukey's *post-hoc*	
		$F(3,28)$	p	ω^2	MD	p_{bonf}
Vagal tone groups (low, high)	MCA2	1.975	0.170	0.030	-	-
	Team MCA	6.363	0.017	0.144	1.78	0.017
	Mood	9.026	0.005	0.201	0.94	0.005
		One-way ANOVA			Tukey's *post-hoc*	
		$F(1)$	p	ω^2	MD	p_{bonf}
MCA groups (low, high)	HFHRV	4.576	0.041	0.101	−0.71	0.041
Team MCA groups (low, high)	HFHRV	6.301	0.018	0.142	−0.82	0.018
CSA accuracy (low, high)	MCA2	8.393	0.007	0.198	0.67	0.007

Team CSA accuracy (low, high)	Team MCA	14.393	<0.001	0.295	2.55	<0.001

Notes. HFHRV, High frequency component heart rate variability; CSA, Cyber situational awareness. MCA, Metacognitive accuracy; η^2 and ω^2, Effect size; CSA2 and MCA2, CSA and MCA without Kill chain scores.

HFHRV was significantly different between low and high team MCA groups (p = 0.018). Tukey's post-hoc test showed that individuals with lower team metacognitive accuracy had lower HFHRV compared to individuals with higher team metacognitive accuracy (MD = −0.82, p_{bonf} = 0.018). Figures 6E,F show interval plots for differences in HFHRV between high and low MCA groups, and high and low team MCA groups, respectively.

3.3.2 H2: Individuals with higher vagal tone have different self-reported mood ratings than individuals with lower vagal tone

Results are found in Table 3. Mood was significantly different between low and high HFHRV groups (p = 0.005). Tukey's post-hoc test revealed that individuals with low HFHRV had significantly higher mood scores compared to individuals with high HFHRV (MD = 0.94, p_{bonf} = 0.005). Figures 7A,B show the interval plot for differences in mood between high and low HFHRV groups, and valence-arousal plots for each day for high and low HFHRV groups, respectively. The valence-arousal plots suggested that individuals with high vagal tone had more neutral moods on day 3 of the exercise, while individuals with low vagal tone had more positive moods.

3.3.3 H3: Individuals with more correct CSA ratings have higher metacognitive accuracy than individuals with less correct CSA ratings

To assess whether individuals with high MCA were correctly estimating good performance or bad performance, ANOVA and Kruskal-Wallis H tests were performed using MCA2, team MCA, and MCA, and team MCA2 as dependent variables, respectively, and CSA accuracy and team CSA accuracy as fixed factor. Results are found in Table 3. Descriptive statistics for the number and percentage of correct CSA answers on each day for the whole sample, and for MCA groups can be found in Table 4. MCA was significantly different between CSA accuracy groups (p = 0.008). Dunn's post-hoc test revealed that individuals with less accurate CSA

ratings had significantly higher MCA scores compared to individuals with more accurate CSA ratings (z = 2.63, p_{bonf} = 0.004). MCA2 was significantly different between CSA accuracy groups (p = 0.007). Tukey's post-hoc test revealed that individuals with less accurate CSA ratings had significantly higher MCA2 scores compared to individuals with more accurate CSA ratings (MD = 0.67, p_{bonf} = 0.007).

Team MCA was significantly different between team CSA accuracy groups (p < 0.001). Tukey's post-hoc test showed that individuals with lower team CSA accuracy had higher team MCA scores compared to individuals with higher team CSA accuracy (MD = 2.55, p_{bonf} < 0.001). Team MCA2 was significantly different between team CSA accuracy groups (p = 0.023). Dunn's post-hoc test showed that individuals with lower team CSA accuracy had higher team MCA2 scores compared to individuals with higher team CSA accuracy (z = 2.28, p_{bonf} = 0.011).

4 Discussion

In this study, we aimed to assess some of the neurocognitive assumptions of the OLB model (Knox et al., 2018) to begin validating its potential as a neuroergonomic approach for CSA communication in cyber threat situations. This was done in a sample of cyber cadets participating in a cyber engineering exercise by using a combination of psychophysiological, CSA, metacognitive, and team measurements targeted at assessing some of the OLB model's implicit underlying neurocognitive assumptions (Jøsok et al., 2016; Knox et al., 2018). The OLB model outlines an adaptive three-step metacognitive control process for how to communicate efficiently between individuals under varying cyber situational dynamics (Knox et al., 2018). In the OLB model, the communicator integrates self-referential, self-other, situational, and task-goal information to ground communication and establish a shared CSA. This requires the prefrontal part of the brain to coordinate activity across brain structures and networks (Nee and D'Esposito, 2016; Morales et al., 2018; Nee, 2021; Friedman and Robbins, 2022).

Being a proxy for activity in prefrontal structures relevant for OLB-ing (Brunoni et al., 2013a; Nikolin et al., 2017; Chand et al., 2020), we hypothesized that individuals with high vagal tone had higher metacognitive accuracy and imposed less communication demands on their teams compared to individuals with low vagal tone (H1). In our initial analyses, we found that vagal

tone was associated with higher metacognitive accuracy for prospective judgments about individual performance and team performance. This is in line with previous studies suggesting that the DLPFC is involved in prospective metacognitive performance estimations (Vaccaro and Fleming, 2018; Fleur et al., 2021).

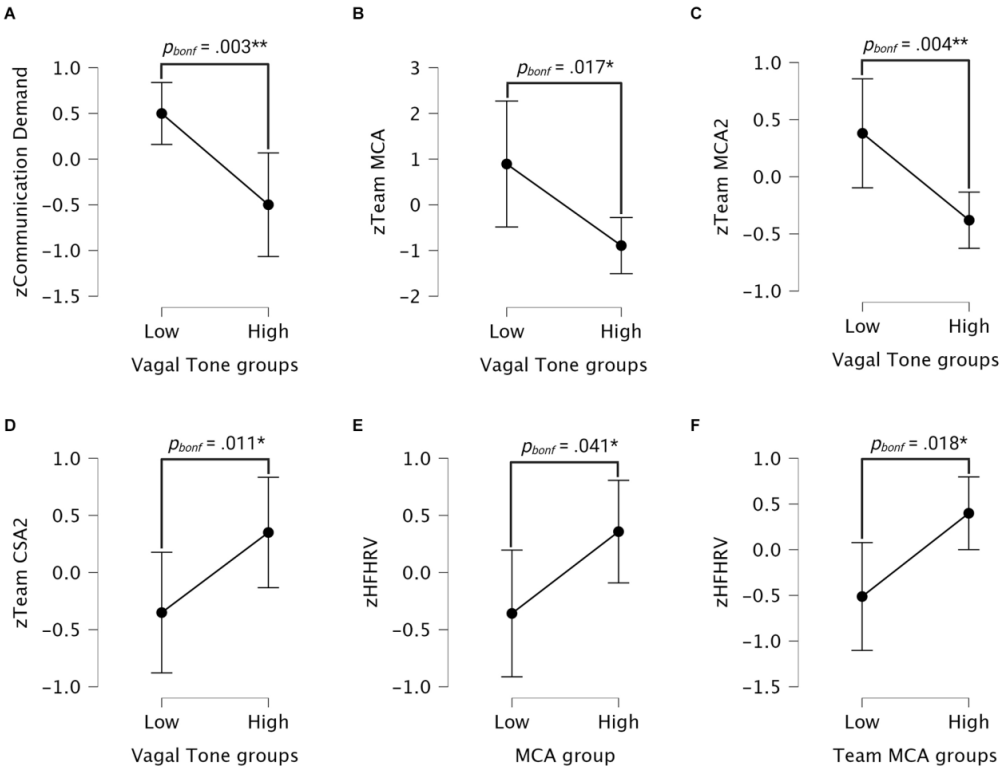

FIGURE 6

Interval plots for group comparisons. (A–D) Interval plots for differences in communication demand, team MCA, team MCA2, and team CSA2 scores between individuals with low and high HFHRV. (E) Interval plot showing differences in HFHRV between high and low MCA groups. (F) Interval plot showing differences in HFHRV between high and low team MCA groups. Whiskers are 95% confidence intervals. MCA, Metacognitive accuracy; CSA, Cyber situational awareness; HFHRV, High frequency component heart rate variability; CSA2 and MCA2, CSA and MCA without Kill chain scores.

In our between-group analyses comparing differences in metacognitive accuracy and communication demands between individuals with low and high vagal tone, we found that team-level metacognitive accuracy was significantly higher in the high vagal tone groups. Individual- level metacognitive accuracy was not significantly different between vagal tone groups. That the findings regarding individual metacognitive accuracy for the whole sample

could not be replicated in the sub-group analysis could be due to the size of the sub-groups. Both vagal tone (Brunoni et al., 2013a; Nikolin et al., 2017; Chand et al., 2020) and prospective metacognitive judgments are influenced by activity in the DLPFC (Fleur et al., 2021). Vagal tone is, however, influenced by several physiological processes other than DLPFC activity (Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology, 1996), as opposed to prospective metacognitive judgments which are dependent on the DLPFC (Vaccaro and Fleming, 2018). Thus, to make sure to account for this possible influence on our results, we did a follow-up analysis assessing differences in vagal tone between individuals with high and low individual and team-level metacognitive accuracy. Vagal tone was higher in individuals with higher metacognitive accuracy for both individual and team-level performance estimations. Finally, in line with our hypothesis, we also found that individuals with high vagal tone imposed lower communication demands on their team compared to individuals with low vagal tone.

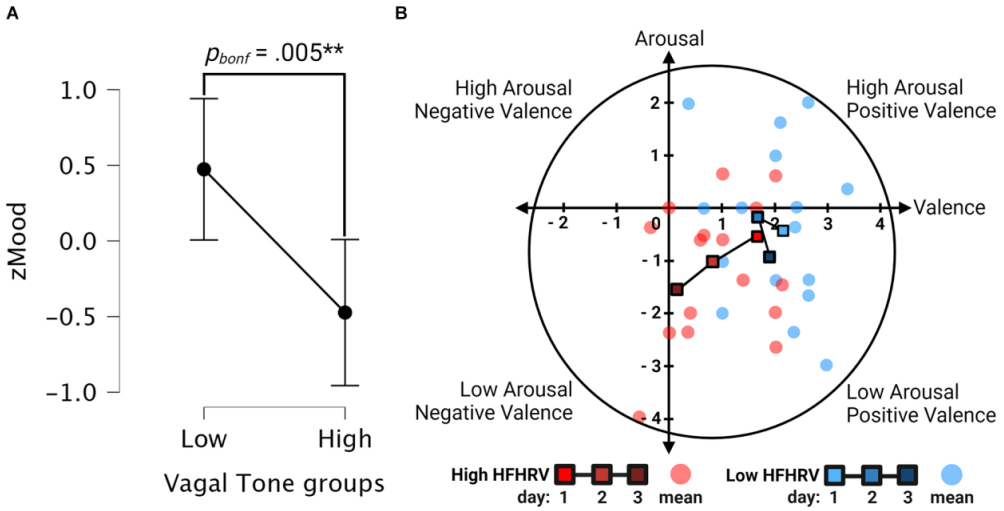

FIGURE 7

Interval and valence arousal plots. (A) Interval plot for differences in mood between high and low HFHRV groups. Whiskers are 95% confidence intervals. (B) Valence-arousal plots for high (red) and low (blue) HFHRV groups. Line with squares indicates HFHRV group-means per day. Colors are the brightest for day 1 and darkest for day 3 of the exercise. Transparent circles indicate the mean for all 3 days for each participant.

TABLE 4 Number and percentage of correct CSA answers for each day (*N* = 32).

			Low MCA		High MCA		Low team MCA		High team MCA	
Variable	Count	%	Count	%	Count	%	Count	%	Count	%
Day 1 Kill chain ratings	4	12.50	2	12.50	2	12.50	2	12.50	2	12.50
Day 1 System critical ratings	6	18.75	2	12.50	4	25.00	2	12.50	4	25.00
Day 1 Severity ratings	2	6.25	0	0.00	2	12.50	0	0.00	2	12.50
Day 1 Action urgency ratings	1	3.12	1	6.25	0	0.00	1	6.25	0	0.00
Day 2 Kill chain ratings	14	43.76	4	25.00	10	62.50	6	37.50	8	50.00
Day 2 System critical ratings	3	9.37	1	6.25	2	12.50	1	6.25	2	12.50
Day 2 Attack severity ratings	7	21.87	2	12.50	5	31.25	2	12.50	5	32.25
Day 2 Action urgency ratings	10	31.25	3	18.75	7	43.75	4	25.00	6	37.50
Day 3 Kill chain ratings	17	53.12	7	43.75	10	62.50	8	50.00	9	56.25
Day 3 System critical ratings	8	25.00	3	18.75	5	31.25	3	18.75	5	31.25
Day 3 Attack severity ratings	7	21.87	1	6.25	6	37.50	3	18.75	4	25.00
Day 3 Action urgency ratings	10	31.25	3	18.75	7	43.75	5	32.25	5	31.25
Day 1 mean team ratings*	13	10.15	5	9.68	8	10.62	5	8.75	8	11.56
Day 2 mean team ratings*	34	26.56	10	24.47	24	28.64	13	22.70	21	30.41
Day 3 mean team ratings*	42	32.81	14	30.72	28	34.89	19	30.31	23	35.31

Notes. CSA, Cyber Situational Awareness; MCA, Metacognitive accuracy. The sum of the percentage of correct sub-group answers is equal to the percentage of correct answers for the whole group multiplied by number of groups. *Count is the total sum of correct CSA assessments across participants' daily assessments, percentage is the mean of the mean percentage of correct CSA assessments within teams.

Our findings should be interpreted in light of previous research suggesting that communication inefficiencies are one of the main problems facing SOC teams (Agyepong et al., 2019; Ask et

al., 2021a). These inefficiencies occur both between analyst-level personnel, for example where cyber operators fail to communicate threat and defense knowledge, ultimately resulting in team members wasting time researching a problem that someone on the team has already solved (Jariwala et al., 2012; Ahrend et al., 2016; Skopik et al., 2016; Staheli et al., 2016). Communication inefficiencies also occur between analysts level and decision-making personnel, where critical information for establishing CSA may get lost as it is communicated from technical personnel and upwards in the decision-making hierarchy to less technical personnel (Staheli et al., 2016; Jøsok et al., 2017; Knox et al., 2018). Suggestions for improving communication between SOC teams have been proposed, such as establishing shared mental models for communication and transactive memories about the expertise and knowledge of team members (Steinke et al., 2015; Hámornik and Krasznay, 2018). This is considered especially critical during cyber threat situations where time pressure is high, and one-way communication is required where all critical information is communicated at once. Our findings may indicate that OLB-related metacognitive processes may help facilitate and proliferate a better understanding of the knowledge and competencies of individuals on the team, and that this is related to establishing better team-level CSA.

Our sample consisted of cyber cadets that know and are used to interact with each other. Nevertheless, our findings may also have relevance for the challenges that arise when information has to be communicated between people that have different priorities spanning the cyber-physical and strategic-tactical dimensions of cyber operations (Jøsok et al., 2016, 2017). Suggested approaches for developing shared mental models for SOC team communication mainly focus on establishing what information should be communicated ahead of time, or understanding the procedures related to performing the tasks of different members of the team (Steinke et al., 2015; Hámornik and Krasznay, 2018). Due to different stakeholders having different communication needs (Ahrend et al., 2016; Jøsok et al., 2016), it is hard to define any set protocol for what to communicate, and it is generally understood that approaches must be adapted to the needs of SOC teams and their clients (Ask et al., 2021a). This is especially the case for communication between technical and non-technical personnel in situations where communication must be adapted according to changing situational dynamics (Jøsok et al., 2017; Ask et al., 2021a). Thus, developing good process-based models for dynamic communication that can be implemented in cyber defense training and education is urgently needed (Knox et al., 2018; Ask et al., 2021a). This is where the findings in the present study may be relevant. Due to the cognitive load associated with the cybersecurity working

environment, models for communication must be feasible to apply in high-stress situations to be sustainable. Applying metacognitive processes in a three-step fashion as outlined in the OLB model may also provide opportunities for regulating stress prior to communication. This may result in an increased capacity for processing the information that is communicated, or remembering what should be communicated. Thus, while having a strategic plan for what to communicate during a cyber threat situation is considered crucial for communication to be efficient (Steinke et al., 2015; Hámornik and Krasznay, 2018), approaches such as the OLB model (Knox et al., 2018) that are designed for situational adaptation may serve as a neuroergonomic complement to facilitate strategic communication.

The present findings may shed light on results from other studies on cyber defense teams indicating that experts impose less communication demands on their teams than novices (Buchler et al., 2016; Lugo et al., 2017a). This may suggest that experts have a better metacognitive understanding of team competence and more efficient (shared) mental models for communication than novices. If expert team communication efficiency reflects a higher rate of adoption of neuroergonomic strategies in response to working under stress, then even unconscious strategy adoption may result in a higher number of shared, albeit implicit mental models for team communication. Overlap of implicit mental models may depend on the degree of strategy convergence that is enforced by environmental pressure. Learning cognitive skills is associated with reduced activity in brain areas responsible for the skill, which is considered a marker for increased processing efficiency (Fleur et al., 2021). However, having an accurate mental model of the competencies of team members may serve as an anchor for cognitive effort one considers necessary for performing well during a cyber threat situation. An example may be finding a compromise between social loafing and effort where the highest level of cognitive output can be sustained for the longest period of time. Previous research has indicated that level 3 situational awareness is more taxing on working memory than preceding levels (Gutzwiller and Clegg, 2013). Cognitive strategies that serve to balance personal knowledge acquisition with cognitive offloading without compromising team performance may compete with strategies for maximizing expertise and being the one to solve any given problem. At intermediate levels of environmental stress, any one strategy, or a flexible combination of the two, maybe equally sustainable. Under increasing loads, however, strategies should converge on those optimizing for balancing cognitive offloading with sustained effort, which may favor metacognitive team processes over individual processes. Strategy convergence may, however,

depend on how salient tasks are, and the interests and priorities of the individual (Wickens et al., 2015).

It has been suggested that individual and team-based metacognitions depend on different processes (Shea et al., 2014). Interestingly, while being associated with the accuracy of prospective performance judgments, vagal tone was not associated with prospective judgments of confidence in individual or team performance but was negatively associated with retrospective confidence judgments of team success. In turn, retrospective judgments of performance were negatively associated with the accuracy of prospective metacognitive judgments of team performance, but not individual performance. Retrospective judgments are associated with activity in the parahippocampal structures and the inferior frontal gyrus (Vaccaro and Fleming, 2018), but are typically assessed at the individual level in neurocognitive studies and not in a team setting. While fast acting connections between the DLPFC and hippocampal structures have been established (Friedman and Robbins, 2022), recent studies show that tracking dynamic social behavior is dependent on interactions between the DLPFC and dorsomedial PFC (McDonald et al., 2020).

This article argues that the processes outlined by the OLB model rely on the coordinated and flexible transition between FPN- and DMN-related information processing, which is a cognitive control process (Nee and D'Esposito, 2016; Nee, 2021; Friedman and Robbins, 2022). Vagal tone measured at rest is associated with connectivity between the DMN and FPN (Chand et al., 2020). The transition between cognitive processes can either be subject to self-regulated metacognitive control (Shimamura, 2008) or stimulus-driven as a result of stress and emotional influence (Baek and Falk, 2018; Poth, 2021). A recent study found that the FPN was involved in metacognitive judgments along with DMN structures, where activity in both the DLPFC and MPFC was negatively associated with confidence judgments (Morales et al., 2018). Emotions are processed differently by DMN and FPN structures (Golkar et al., 2012; Terasawa et al., 2013; Fujimoto et al., 2021; Nejati et al., 2021), while stress disrupts connectivity between the FPN and DMN along with its association with vagal tone (Chand et al., 2020). Previous studies on cyber cadets identified several emotional and self-regulatory processes that may have differing effects on teamwork and communication (Lugo et al., 2016, 2017b, 2021; Knox et al., 2017; Jøsok et al., 2019; Ask et al., 2021b). As the DLPFC is involved in mood processing (Golkar et al., 2012; Nejati et al., 2021), we hypothesized that individuals with higher vagal tone had different self-reported mood ratings than individuals with lower

vagal tone (H2). In line with our second hypothesis, we found that vagal tone was negatively associated with mood. This finding was also replicated in our subgroup analysis where individuals with higher vagal tone had lower self-reported mood than individuals with lower vagal tone.

The valence-arousal plots showing daily mood and arousal for individuals with high and low vagal tone indicated that individuals with high vagal tone had more neutral moods on day 3 of the exercise, while individuals with low vagal tone had more positive moods. In a previous study, we found that variations in daily affect were associated with experienced team workloads among cyber cadets participating in a cyber defense exercise (Ask et al., 2021b). While the significance of such findings may be unclear with respect to exercise outcomes (Lund, 2022), the findings in the present study may serve to further elucidate their relevance beyond suggesting that individual characteristics influence team dynamics. While stress and urgency may disturb analytic cognitive processes (Poth, 2021), positive moods, as opposed to neutral moods may also result in transitioning from analytical processing to stimulus- oriented processing (Baek and Falk, 2018), for example as a result of optimism bias and mood congruent processing, lack of suspicion, or overconfidence (Vishwanath et al., 2018; Canham et al., 2022; Sütterlin et al., 2022). In practice, this may result in reduced situational understanding, as indicated in our study by positive moods being a significant negative predictor of both individual and team-level prospective metacognitive judgments of performance, as well as being a positive predictor of retrospective judgments of team success. Retrospective judgments of team success were as noted negatively associated with the accuracy of team-level metacognitive judgments. These findings also mirror other studies where overconfidence has been associated with worse threat detection abilities among IT and cybersecurity personnel (Butavicius et al., 2016; Jampen et al., 2020; Sütterlin et al., 2022).

In the present study, having high metacognitive accuracy could be either due to accurately judging performance as bad or as good. Thus, it was technically possible that individuals with high metacognitive accuracy could perform equal to- or even worse on CSA estimations than individuals with low metacognitive accuracy as long as they were more correct in their performance estimations. Because good cyber defense decision- making is based on having accurate CSA (Barford et al., 2009), and metacognitive accuracy is necessary for correct SA (Endsley, 2020), we also tested the hypothesis that individuals with higher metacognitive accuracy would have more correct CSA ratings than individuals with lower metacognitive

accuracy (H3). We found that individuals with higher metacognitive accuracy also had more correct CSA ratings at both the individual and team-level. This supports our hypothesis and the findings of Endsley (2020). No measurement of team dynamics other than retrospective judgments of performance was associated with accurately judging team performance and team-level CSA ratings. This stresses the importance of training metacognitive skills to ensure that SOC teams are able to generate and share accurate CSA. In other words, team based training in absence of metacognitive training may not efficiently provide all the skills necessary for ensuring SOC team performance. This should arguably occur during education rather than relying on individual SOC teams to ensure that new recruits learn metacognitive skills. However, this may challenge traditional educational and organizational practices (Jøsok et al., 2017; Knox et al., 2018) as reflected in the plethora of challenges SOC teams face (Agyepong et al., 2019; Ask et al., 2021a). Originally developed as a pedagogical tool, the OLB model (Knox et al., 2018) may serve as a flexible and cost-effective approach to metacognitive training that is easy to implement across learning situations and institutions.

To the best of our knowledge, this is the first study providing neuroergonomic insights into the relationship between communication in teams and metacognitive CSA accuracy in a cybersecurity setting. While we aimed to provide neuroergonomic support for the OLB model, the present findings could also be used to argue for the importance of psychophysiological measurements in recruitment, training, and performance monitoring. Previous research found associations between vagal tone and performance among tactical personnel in non-cybersecurity settings (including military; Tomes et al., 2020). The present study is the first to show that vagal tone may also serve as an indicator of performance in a cybersecurity setting. To the extent that vagal tone reflects the ability for self-regulation (e.g., Segerstrom and Nes, 2007; Reynard et al., 2011), our findings are an addition to a growing body of literature showing relationships between self-regulation and movements in the Hybrid Space (Knox et al., 2017, 2019; Jøsok et al., 2019). Finally, the present findings also provide support for the scarce literature on relationships between vagal tone and metacognitive accuracy (Meessen et al., 2018).

4.1 Limitations and future directions

The aim of this study was to assess the neurocognitive assumptions of the OLB model (Knox et al., 2018) to determine its potential as a neuroergonomic approach to improve communication. We did this using vagal tone as a proxy for neural activity thought to be

relevant for OLB execution (Brunoni et al., 2013a; Nikolin et al., 2017; Chand et al., 2020). The present study goes some length in achieving this, however, future studies should use an intervention design where some participants are trained in explicitly applying the model. While the vagal tone is considered a stable trait that is hard to change with intervention (e.g., Brunoni et al., 2013b; Wheeler et al., 2014; Neyer et al., 2021), metacognition is something that can be trained (Jøsok et al., 2016; Fleur et al., 2021). Thus, it would be both interesting and necessary to assess whether individuals who are trained in applying the OLB model but have low vagal tones perform better than individuals who are not trained in using the model but have high vagal tones. To ensure that this is done in a naturalistic setting may require experimental collaboration between cognitive scientists and cyber defense exercise organizers (Ask et al., 2021a).

Albeit comparing team-level and individual level metacognitive accuracy is not addressed in this study, Table 4 indicates that the number of correct individual answers for each CSA item per day is mostly overlapping between individuals with high individual- and team-level metacognitive accuracy, although slightly favoring individual metacognitive accuracy. However, when looking at the descriptive statistics for the mean percent of correct answers within teams, the proportion of the mean of correct team answers appears larger for individuals with high team metacognitive accuracy, even though the number of their individual contributions is lower. As noted in previous studies (Ask et al., 2021a,b), including both team- and individual-level measurements is important to develop SOC team performance metrics, and future studies should assess how team-level and individual- level metacognition contributes to team performance. In Table 4 it appears that individuals with high individual- and team-level metacognitive accuracy on day one were completely overlapping. The OLB model suggests using metacognition to make communication of CSA between team members more efficient (Knox et al., 2018). Supra-individual metacognitive processes are suggested to be involved in inter-individual cognitive control (Shea et al., 2014), thus it would be interesting to see whether individuals with high metacognitive accuracy in the beginning of a cyber defense exercise influence the evolution of team performance.

As part of the exercise, the cadets were also assessed on leadership skills and factors other than CSA and mission success. It is possible that some participants included these factors when making prospective judgments of their own and the team performance, thus inflating or deflating their confidence relative to our outcome measurements. Because excluding this

possibility would require probing each participant about what they based their estimations on, it is safer to assume that our metacognitive accuracy estimates are conservative. Furthermore, there have been reported sex differences in relationships between social orientations and vagal tone (Lischke et al., 2018). Due to conducting the study in a security setting, we did not ask participants to provide information on their sexes. While the sex of participants is commonly underreported in cybersecurity studies (Ask et al., 2021a), a recent study suggested that sex may play a role in communication among cyber engineers (Fisher, 2022). Future studies should therefore make an effort to also assess whether findings are differentially influenced by sex. A final limitation of the current study is the sample size. While the present study included the entire cohort of the studied population, more studies are needed to replicate findings.

5 Conclusion

Prefrontally modulated vagal tone, an indicator of activity in brain structures relevant for coordinating the cognitive processes underlying OLB model execution, is associated with metacognitive cyber situational awareness and imposing lower communication demands on the team. Based on the assumption that individuals working in high-stress-, high-cognitive load-environments will choose neuroergonomic cognitive strategies to reach task goals, the present findings suggest that the OLB model is neuroergonomic in such environments. Individuals with higher vagal tone had more neutral moods which could be necessary for allocating more attentional resources to analytical processing. Furthermore, individuals with higher CSA had higher metacognitive accuracy compared to individuals with lower CSA supporting previous studies suggesting that metacognitive accuracy is necessary for achieving situational awareness. The present study highlights the potential of using neurophysiological measurements as performance indicators. Future studies are needed to explicitly address the effect of using the OLB model as the basis for a metacognitive intervention to improve communication and team performance, as well as replicating the findings of the present study.

Data availability statement

The datasets presented in this article are not readily available because access to raw and processed data is restricted in accordance with agreement between the researchers and the Norwegian Defense University College, Cyber Academy (NDCA). Requests to access the datasets should be directed to corresponding author.

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. The patients/participants provided their written informed consent to participate in this study. The present study conformed to institutional guidelines and was eligible for automatic approval by the Norwegian Social Science Data Services' (NSD) ethical guidelines for experimental studies. Participation was voluntary and all participants were informed about the aims of the study, the methods applied, that they could withdraw from participation at any time and without any consequences, and that if they did so all the data that was gathered from them would be deleted. After volunteering to participate in the study, participants were asked to provide informed consent on the first page of an online form where baseline data was collected. Participants were asked to generate and remember a unique participant ID that they would use during data collection for the duration of the study.

Author contributions

TA: study design and methods, data collection, analysis, writing of original draft, review and editing. BK: study design, writing of original draft, review and editing. RL and SS: study design and methods, review and editing. IH: exercise organization, scoring of CSA questionnaires for analysis, writing of original draft. All authors contributed to the article and approved the submitted version.

Funding

This study was conducted as part of the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) project. ACDICOM is funded by the Norwegian Research Council (project #302941; Norges Forskningsråd).

Acknowledgments

A preprint of this article is available at PsyArXiv preprints (Ask et al., 2022, preprint).

Conflict of interest

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

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: a systematic review. J. Cyber Security Technol. 4, 125–152. doi: 10.1080/23742917.2019.1698178

Ahrend, J. M., Jirotka, M., and Jones, K. (2016). "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge," in 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), (London, UK). doi: 10.1109/CyberSA.2016.75 03279

Appelhans, B. M., and Luecken, L. J. (2006). Heart rate variability as an index of regulated emotional responding. Rev. Gen. Psychol. 10, 229–240. doi: 10.1037/1089-2680.10. 3.229

Ask, T. F., Knox, B. J., Lugo, R., Helgetun, I., and Sütterlin, S. (2022). Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. PsyArXiv [Preprint]. doi: 10.31234/osf.io/jsnu8

Ask T. F., Lugo, R. G., Knox, B. J., and Sütterlin, S. (2021a). "Human- human communication in cyber threat situations: a systematic review," in HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021. Lecture Notes in Computer Science, ed C. Stephanidis (Cham: Springer), 21–43.

Ask, T. F., Sütterlin, S., Knox, B. J., and Lugo, R. G. (2021b). "Situational states influence on team workload demands in cyber defense exercise," in HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021. Lecture Notes in Computer Science, ed C. Stephanidis (Cham: Springer), 3–20. doi: 10.1007/978-3-030-90328-2_1

Baek, E. C., and Falk, E. B. (2018). Persuasion and influence: what makes a successful persuader. Curr. Opin. Psychol. 24, 53–57. doi: 10.1016/j.copsyc.2018. 05.004

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., et al. (2009). "Cyber SA: situational awareness for cyber defense," in Cyber Situational Awareness Advances in Information Security, eds S. Jajodia, P. Liu, V. Swarup and C. Wang (Cham: Springer), 3–13.

Berntson, G. G., Lozano, D. L., and Chen, Y. J. (2005). Filter properties of root mean square successive difference (RMSSD) for heart rate. Psychophysiology 42, 246–252. doi: 10.1111/j.1469-8986.2005.00277.x

Berntson, G. G., and Stowell, J. R. (1998). ECG artifacts and heart period variability: don't miss a beat! Psychophysiology 35, 127–132.

Botvinick, M. M. (2007). Conflict monitoring and decision making: reconciling two perspectives on anterior cingulate function. Cogn. Affect. Behav. Neurosci. 7, 356–366. doi: 10.3758/cabn.7.4.356

Bradley, M. M., and Lang, P. J. (1994). Measuring emotion: the self-assessment manikin and the semantic differential. J. Behav. Ther. Exp. Psychiatry 25, 49–59.

Brunoni, A. R., Vanderhasselt, M. A., Boggio, P. S., Fregni, F., Dantas, E. M., Mill, J. G., et al. (2013a). Polarity- and valence-dependent effects of prefrontal transcranial direct current stimulation on heart rate variability and salivary cortisol. Psychoneuroendocrinology 38, 58–66. doi: 10.1016/j.psyneuen.2012.04.020

Brunoni, A. R., Kemp, A. H., Dantas, E. M., Goulart, A. C., Nunes, M. A., Boggio, P. S., et al. (2013b). Heart rate variability is a trait marker of major depressive disorder: evidence from the sertraline vs. electric current therapy to treat depression clinical study. Int. J. Neuropsychopharmacol. 16, 1937–1949. doi: 10.1017/S1461145713000497

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

Butavicius, M., Parsons, K., Pattinson, M., and McCormac, A. (2016). Breaching the human firewall: social engineering in phishing and spear-phishing emails. arXiv [Preprint]. doi: 10.48550/arXiv.160 6.00887

Canham, M., Sütterlin, S., Ask, T. F., Knox, B. J., Glenister, L., and Lugo, R. G. (2022). Ambiguous self-induced disinformation (ASID) attacks: weaponizing a cognitive deficiency. J. Info. Warfare 23, 41–58.

Champion, M. A., Rajivan, P., Cooke, N. J., and Jariwala, S. (2012). "Team-based cyber defense analysis," in 2012 IEEE International Multi- Disciplinary Conference on Cognitive Methods in situation Awareness and Decision Support (New Orleans, LA, USA), 218–221. doi: 10.1109/CogSIMA.2012. 6188386

Chand, T., Li, M., Jamalabadi, H., Wagner, G., Lord, A., Alizadeh, S., et al. (2020). Heart rate variability as an index of differential brain dynamics at rest and after acute stress induction. Front. Neurosci. 14:645. doi: 10.3389/fnins.2020. 00645

Chang, C., and Glover, G. H. (2009). Effects of model-based physiological noise correction on default mode network anti-correlations and correlations. Neuroimage 47, 1448–1459. doi: 10.1016/j.neuroimage.2009.05.012

Chen, A. C., Oathes, D. J., Chang, C., Bradley, T., Zhou, Z. W., Williams, L. M., et al. (2013). Causal interactions between fronto-parietal central executive and default-mode networks in humans. Proc. Nat. Acad. Sci. U S A 110, 19944–19949. doi: 10.1073/pnas.1311772110

Duncan, J. (2010). The multiple-demand (MD) system of the primate brain: mental programs for intelligent behaviour. Trends Cogn. Sci. 14, 172–179. doi: 10.1016/j.tics.2010.01.004

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

Endsley, M. R. (1995). Toward a theory of Situation Awareness in dynamic systems. J. Hum. Factors Ergon. Soc. 37, 32–64. doi: 10.1518/001872095779049543

Endsley, M. R. (2020). The divergence of objective and subjective situation awareness: a meta- analysis. J. Cogn. Eng. Decis. Mak. 14, 34–53. doi: 10.1177/1555343419874248

Fisher, K. (2022). The role of gender in providing expert advice on cyber conflict and artificial intelligence for military personnel. Front. Big Data 5:992620. doi: 10.3389/fdata.2022.992620

Flavell, J. H. (1979). Metacognition and cognitive monitoring: a new area of cognitive- developmental inquiry. Am. Psychol. 34, 906–911. doi: 10.1037/0003- 066x.34.10.906

Fleur, D. S., Bredeweg, B., and van den Bos, W. (2021). Metacognition: ideas and insights from neuro- and educational sciences. NPJ Sci. Learn. 6:13. doi: 10.1038/s41539-021-00089-5

Fox, M. D., Snyder, A. Z., Vincent, J. L., Corbetta, M., Van Essen, D. C., and Raichle, M. E. (2005). The human brain is intrinsically organized into dynamic, anticorrelated functional networks. Proc. Nat. Acad. Sci. U S A 102, 9673–9678. doi: 10.1073/pnas.0504136102

Franke, U., and Brynielsson, J. (2014). Cyber situational awareness - a systematic review of the literature. Comput. Security 46, 18–31. doi: 10.1016/j.cose.2014.06. 008

Friedman, N. P., and Robbins, T. W. (2022). The role of prefrontal cortex in cognitive control and executive function. Neuropsychopharmacology 47, 72–89. doi: 10.1038/s41386-021-01132-0

Fujimoto, A., Murray, E. A., and Rudebeck, P. H. (2021). Interaction between decision-making and interoceptive representations of bodily arousal in frontal cortex. Proc. Nat. Acad. Sci. U S A 118:e2014781118. doi: 10.1073/pnas.2014781118

Geisler, F. C. M., and Kubiak, T. (2009). Heart rate variability predicts self-control in goal pursuit. Eur. J. Personal. 23, 623–633. doi: 10.1002/ per.727

Goedhart, A. D., van der Sluis, S., Houtveen, J. H., Willemsen, G., and de Geus, E. J. (2007). Comparison of time and frequency domain measures of RSA in ambulatory recordings. Psychophysiology 44, 203–215. doi: 10.1111/j.1469-8986. 2006.00490.x

Golkar, A., Lonsdorf, T. B., Olsson, A., Lindstrom, K. M., Berrebi, J., Fransson, P., et al. (2012). Distinct contributions of the dorsolateral prefrontal and orbitofrontal cortex during emotion regulation. PLoS One 7:e48107. doi: 10.1371/journal.pone. 0048107

Gutzwiller, R. S., and Clegg, B. A. (2013). The role of working memory in levels of situation awareness. J. Cogn. Eng. Decis. Mak. 7, 141–154. doi: 10.1177/1555343412451749

Hámornik, B. P., and Krasznay, C. (2018). "Ateam-level perspective of human factors in cyber security: security operations centers," in AHFE 2017. AISC, ed D. Nicholson (Cham: Springer), 224–236.

Hagura, N., Haggard, P., and Diedrichsen, J. (2017). Perceptual decisions are biased by the cost to act. eLife 6:e18422. doi: 10.7554/eLife.18422

Hansen, A. L., Johnsen, B. H., and Thayer, J. F. (2003). Vagal influence on working memory and attention. Int. J. Psychophysiol. 48, 263–274. doi: 10.1016/s0167-8760(03)00073-4

Hansen, A. L., Johnsen, B. H., and Thayer, J. F. (2009). Relationship between heart rate variability and cognitive function during threat of shock. Anxiety Stress Coping 22, 77–89. doi: 10.1080/10615800802272251

Hart, S. G., and Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): results of empirical and theoretical research. Adv. Psychol. 52, 139–183.

Hildebrandt, L. K., McCall, C., Engen, H. G., and Singer, T. (2016). Cognitive flexibility, heart rate variability and resilience predict fine-grained regulation of arousal during prolonged threat. Psychophysiology 53, 880–890. doi: 10.1111/psyp. 12632

Jøsok, Ø., Knox, B. J., Helkala, K., Wilson, K., Sütterlin, S., Lugo, R. G., et al. (2017). Macrocognition applied to the hybrid space: team environment, functions and processes in cyber operations. Lecture Notes in Comput. Sci. 486–500. doi: 10.1007/978-3-319-58 625-0_35

Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., and Ward, P. (2016). "Exploring the hybrid space," in Augmented Cognition 2016. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence), eds D. D. D. Schmorrow and C. M. M. Fidopiastis (Cham: Springer) 9744, 178–188.

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

Jampen, D., Gür, G., Sutter, T., and Tellenbach, B. (2020). Don't click: towards an effective anti- phishing training. a comparative literature review. Human-Centric Comput. Info. Sci. 10, 1–41. doi: 10.1186/s13673-020-00237-7

Jariwala, S., Champion, M., Rajivan, P., and Cooke, N. J. (2012). Influence of team communication and coordination on the performance of teams at the iCTF competition. Proc. Hum. Factors Ergon. Soc. Annu. Meet. 56, 458–462. doi: 10.1177/1071181312561044

Kaufmann, T., Sütterlin, S., Schulz, S. M., and Vögele, C. (2011). ARTiiFACT: a tool for heart rate artifact processing and heart rate variability analysis. Behav. Res. Methods 43, 1161–1170. doi: 10.3758/s13428-011-0107-7

Khalil, R., Godde, B., and Karim, A. A. (2019). The link between creativity, cognition and creative drives and underlying neural mechanisms. Front. Neural Circuits 13:18. doi: 10.3389/fncir.2019.00018

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

Knox, B. J., Lugo, R. G., Helkala, K. M., and Sütterlin, S. (2019). Slow education and cognitive agility: improving military cyber cadet cognitive performance for better governance of cyberpower. Int. J. Cyber Warfare Terrorism (IJCWT) 9, 48–66. doi: 10.4018/IJCWT.2019010104

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 HCI International 2017 - Posters' Extended Abstracts (Cham: Springer), 330–338. doi: 10.1007/978-3-319-58750-9_46

Lankton, P. (2007). Endsley's model of situational awareness [jpg]. Available online at: https://en.wikipedia.org/wiki/File:Endsley-SA-model.jpg.

Lif, P., Granasen, M., and Sommestad, T. (2017). "Development and validation of technique to measure cyber situation awareness," in 2017 International Conference on Cyber Situational Awareness, Data Aanalytics and Assessment (Cyber SA), (London, UK). doi: 10.1109/cybersa.2017.8073388

Lischke, A., Mau-Moeller, A., Jacksteit, R., Pahnke, R., Hamm, A. O., and Weippert, M. (2018). Heart rate variability is associated with social value orientation in males but not females. Sci. Rep. 8:7336. doi: 10.1038/s41598-018- 25739-4

Liston, C., Chen, A. C., Zebley, B. D., Drysdale, A. T., Gordon, R., Leuchter, B., et al. (2014). Default mode network mechanisms of transcranial magnetic stimulation in depression. Biol. Psychiatry 76, 517–526. doi: 10.1016/j.biopsych. 2014.01.023

Lugo, R. G., Ask, T. F., Sütterlin, S., and Knox, B. J. (2021). “The influence of team workload demands during a cyber defense exercise on team performance,” in HCI International 2021 - Late Breaking Posters. HCII 2021. Communications in Computer and Information Science, eds C. Stephanidis, M. Antona, S. Ntoa (Cham: Springer), 1499, 545–549. doi: 10.1007/978-3-030-90179-0_70

Lugo, R., Kwei-Nahr, P., Jøsok, Ø., Knox, B. J., Helkala, K., and Sütterlin, S. (2017a). “Team workload demands influence on cyber detection performance,” in 13th International Conference on Naturalistic Decision Making (Bath, UK), 223–225.

Lugo, R., Helkala, K., Knox, B., Josøk, Ø., Lande, N. M., and Sütterlin, S. (2017b). Interoceptive sensitivity as a proxy for emotional intensity and its relationship with perseverative cognition. Psychol. Res. Behav. Manage. 11, 1–8. doi: 10.2147/PRBM. S139790

Lugo, R. G., and Sütterlin, S. (2018). Cyber officer profiles and performance factors. Lecture Notes Comput. Sci. 10906, 181–190. doi: 10.1007/978-3-319-91122- 9_16

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. J. Mil. Stud. 7, 44–52. doi: 10.1515/jms-2016-0005

Lund, M. S. (2022). Øving på cybersikkerheit: ein casestudie av ei cybersikkerheitsøving. Scand. J. Mil. Studies 5, 244–256. doi: 10.31374/sjms.119

McDonald, K. R., Pearson, J. M., and Huettel, S. A. (2020). Dorsolateral and dorsomedial prefrontal cortex track distinct properties of dynamic social behavior. Soc. Cogn. Affect. Neurosci. 15, 383–393. doi: 10.1093/scan/nsaa053

McNeese, M., Cooke, N. J., and Champion, M. A. (2011). “Situating cyber situation awareness,” in Proceedings of the 10th International Conference on Naturalistic Decision Making (Orlando, FL).

Meessen, J., Sütterlin, S., Gauggel, S., and Forkmann, T. (2018). Learning by heart-the relationship between resting vagal tone and metacognitive judgments: a pilot study. Cogn. Process. 19, 557–561. doi: 10.1007/s10339-018-0865-6

Menon, V., and D’Esposito, M. (2022). The role of PFC networks in cognitive control and executive function. Neuropsychopharmacology 47, 90–103. doi: 10.1038/s41386-021-01152-w

Morales, J., Lau, H., and Fleming, S. M. (2018). Domain-general and domain- specific patterns of activity supporting metacognition in human prefrontal cortex. J. Neurosci. 38, 3534–3546. doi: 10.1523/JNEUROSCI.2360-17.2018

Nee, D. E. (2021). Integrative frontal-parietal dynamics supporting cognitive control. eLife 10:e57244. doi: 10.7554/eLife.57244

Nee, D. E., and D’Esposito, M. (2016). The hierarchical organization of the lateral prefrontal cortex. eLife 5:e12112. doi: 10.7554/eLife.12112

Nejati, V., Majdi, R., Salehinejad, M. A., and Nitsche, M. A. (2021). The role of dorsolateral and ventromedial prefrontal cortex in the processing of emotional dimensions. Sci. Rep. 11:1971. doi: 10.1038/s41598-021-81454-7

Neyer, S., Witthöft, M., Cropley, M., Pawelzik, M., Lugo, R. G., and Sütterlin, S. (2021). Reduction of depressive symptoms during inpatient treatment is not associated with changes in heart rate variability. PLoS One 16:e0248686. doi: 10.1371/journal.pone.0248686

Nikolin, S., Boonstra, T. W., Loo, C. K., and Martin, D. (2017). Combined effect of prefrontal transcranial direct current stimulation and a working memory task on heart rate variability. PLoS One 12:e0181833. doi: 10.1371/journal.pone.0181833

Park, G., Van Bavel, J. J., Egan, E. J. L., Vasey, M. W., and Thayer, J. F. (2012). From the heart to the mind’s eye: cardiac vagal tone is related to visual perception of fearful faces at high spatial frequency. Biol. Psychol. 90, 171–178. doi: 10.1016/j.biopsycho.2012.02.012

Park, G., Van Bavel, J. J., Vasey, M. W., and Thayer, J. F. (2013). Cardiac vagal tone predicts attentional engagement to and disengagement from fearful faces. Emotion 13, 645–656. doi: 10.1037/a0032971

Poth, C. H. (2021). Urgency forces stimulus-driven action by overcoming cognitive control. eLife 10:e73682. doi: 10.7554/eLife.73682

Pu, J., Schmeichel, B. J., and Demaree, H. A. (2010). Cardiac vagal control predicts spontaneous regulation of negative emotional expression and subsequent cognitive performance. Biol. Psychol. 84, 531–540. doi: 10.1016/j.biopsycho.2009.07.006

Raichle, M. E. (2015). The brain's default mode network. Ann. Rev. Neurosci. 38, 433–447. doi: 10.1146/annurev-neuro-071013-014030

Raichle, M. E., MacLeod, A. M., Snyder, A. Z., Powers, W. J., Gusnard, D. A., and Shulman, G. L. (2001). A default mode of brain function. Proc. Natl. Acad. Sci. U S A 98, 676–682. doi: 10.1073/pnas.98.2.676

Reynard, A., Gevirtz, R., Berlow, R., Brown, M., and Boutelle, K. (2011). Heart rate variability as a marker of self-regulation. Appl. Psychophysiol. Biofeedback 36, 209–215. doi: 10.1007/s10484-011-9162-1

Segerstrom, S. C., and Nes, S. L. (2007). Heart rate variability reflects self-regulatory strength, effort and fatigue. Psychol. Sci. 18, 275–281. doi: 10.1111/j. 1467-9280.2007.01888.x

Sellers, J., Helton, W. S., Näswall, K., Funke, G. J., and Knott, B. A. (2014). Development of the team workload questionnaire (TWLQ). Proc. Hum. Factors Ergon. Soc. Annu. Meet. 58, 989–993. doi: 10.1177/154193121 4581207

Shea, N., Boldt, A., Bang, D., Yeung, N., Heyes, C., and Frith, C. D. (2014). Supra- personal cognitive control and metacognition. Trends Cogn. Sci. 18, 186–193. doi: 10.1016/j.tics.2014.01.006

Shimamura, A. P. (2008). "A neurocognitive approach to metacognitive monitoring and control," in Handbook of Metamemory and Memory, eds J. Dunlosky and R. A. Bjork (New York, NY: Psychology Press), 373–390.

Skopik, F., Settanni, G., and Fiedler, R. (2016). A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. Comput. Security 60, 154–176. doi: 10.1016/j.cose.2016.04. 003

Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., et al. (2016). "Collaborative data analysis and discovery for cyber security," in SOUPS 2016: Twelfth Symposium on Usable Privacy and Security (Denver, CO).

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., et al. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Security Privacy 13, 20–29. doi: 10.1109/MSP.2015.71

Sütterlin, S., Lugo, R., Ask, T., Veng, K., Eck, J., Fritschi, J., et al. (2022). "The role of IT background for metacognitive accuracy, confidence and overestimation of deep fake recognition skills," in Augmented Cognition. HCII 2022. Lecture Notes in Computer Science, eds D. D. Schmorrow and C. M. Fidopiastis (Cham: Springer), 13310, 103–119. doi: 10.1007/978-3-031-05457-0_9

Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology (1996). Heart rate variability. Standards of measurement, physiological interpretation and clinical use. Circulation 93, 1043–1065. doi: 10.1161/01.CIR.93.5.1043

Terasawa, Y., Fukushima, H., and Umeda, S. (2013). How does interoceptive awareness interact with the subjective experience of emotion? An fMRI study. Hum. Brain Mapp. 34, 598–612. doi: 10.1002/hbm.21458

Thayer, J. F., Ahs, F., Fredrikson, M., Sollers, J. J., 3rd, and Wager, T. D. (2012). A meta-analysis of heart rate variability and neuroimaging studies: implications for heart rate variability as a marker of stress and health. Neurosci. Biobehav. Rev. 36, 747–756. doi: 10.1016/j.neubiorev.2011.11.009

Tomes, C., Schram, B., and Orr, R. (2020). Relationships between heart rate variability, occupational performance and fitness for tactical personnel: a systematic review. Front. Public Health 8:583336. doi: 10.3389/fpubh.2020.583336

Vaccaro, A. G., and Fleming, S. M. (2018). Thinking about thinking: a coordinate-based meta- analysis of neuroimaging studies of metacognitive judgements. Brain Neurosci. Adv. 2:2398212818810591. doi: 10.1177/2398212818810591

Vishwanath, A., Harrison, B., and Ng, Y. J. (2018). Suspicion, cognition and automaticity model of phishing susceptibility. Commun. Res. 45, 1146–1166. doi: 10.1177/0093650215627483

Wheeler, A., Denson, L., Neil, C., Tucker, G., Kenny, M., Beltrame, J., et al. (2014). Investigating the effect of mindfulness training on heart rate variability in mental health outpatients: a pilot study. Behav. Change 31, 175–188. doi: 10.1017/bec.2014.14

Wickens, C. D., Gutzwiller, R. S., and Santamaria, A. (2015). Discrete task switching in overload: a meta-analyses and a model. Int. J. Hum. Comput. Stud. 79, 79–84. doi: 10.1016/j.ijhcs.2015. 01.002

Williams, D. P., Feeling, N. R., Hill, L. K., Spangler, D. P., Koenig, J., and Thayer, J. F. (2017). Resting heart rate variability, facets of rumination and trait anxiety: implications for the perseverative cognition hypothesis. Front. Hum. Neurosci. 11:520. doi: 10.3389/fnhum.2017. 00520

Williams, D. P., Koenig, J., Carnevali, L., Sgoifo, A., Jarczok, M. N., Sternberg, E. M., et al. (2019). Heart rate variability and inflammation: a meta-analysis of human studies. Brain Behav. Immun. 80, 219–226. doi: 10.1016/j.bbi.2019.03.009

Winston, J. S., Vuilleumier, P., and Dolan, R. (2003). Effects of low-spatial frequency components of fearful faces on fusiform cortex activity. Curr. Biol. 13, 1824–1829. doi: 10.1016/j.cub.2003.0 9.038

Zhou, H. X., Chen, X., Shen, Y. Q., Li, L., Chen, N. X., Zhu, Z. C., et al. (2020). Rumination and the default mode network: meta-analysis of brain imaging studies and implications for depression. Neuroimage 206:116287. doi: 10.1016/j. neuroimage.2019.116287

5.3. A 3D Mixed Reality Visualization of Network Topology and Activity Results in Better Dyadic Cyber Team Communication and Cyber Situational Awareness

Torvald F. Ask[1,2]*, Kaur Kullman[3,4], Stefan Sütterlin[2,5,6], Benjamin J. Knox[1,2,7], Don Engel[4] and Ricardo G. Lugo[1,2]

[1]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway,

[2]Faculty of Health, Welfare and Organization, Østfold University College, Halden, Norway,

[3]Doctoral School of Information and Communication Technology, Institute of Computer Science, Tallinn University of Technology, Tallinn, Estonia,

[4]Center for Space Sciences and Technology, University of Maryland, Baltimore County, Baltimore, MD, United States,

[5]Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany,

[6]Centre for Digital Forensics and Cybersecurity, Tallinn University of Technology, Tallinn, Estonia, [7]Norwegian Armed Forces Cyber Defense, Oppland, Norway

Background: Cyber defense decision-making during cyber threat situations is based on human-to-human communication aiming to establish a shared cyber situational awareness. Previous studies suggested that communication inefficiencies were among the biggest problems facing security operation center teams. There is a need for tools that allow for more efficient communication of cyber threat information between individuals both in education and during cyber threat situations.

Methods: In the present study, we compared how the visual representation of network topology and traffic in 3D mixed reality vs. 2D affected team performance in a sample of cyber cadets ($N = 22$) cooperating in dyads. Performance outcomes included network topology recognition, cyber situational awareness, confidence in judgements, experienced communication demands, observed verbal communication, and forced choice decision-making. The study utilized network data from the NATO CCDCOE 2022 Locked Shields cyber defense exercise.

Results: We found that participants using the 3D mixed reality visualization had better cyber situational awareness than participants in the 2D group. The 3D mixed reality group was generally more confident in their judgments except when performing worse than the 2D group

on the topology recognition task (which favored the 2D condition). Participants in the 3D mixed reality group experienced less communication demands, and performed more verbal communication aimed at establishing a shared mental model and less communications discussing task resolution. Better communication was associated with better cyber situational awareness. There were no differences in decision-making between the groups. This could be due to cohort effects such as formal training or the modest sample size.

Conclusion: This is the first study comparing the effect of 3D mixed reality and 2D visualizations of network topology on dyadic cyber team communication and cyber situational awareness. Using 3D mixed reality visualizations resulted in better cyber situational awareness and team communication. The experiment should be repeated in a larger and more diverse sample to determine its potential effect on decision-making.

1. Introduction

Decision-making in Cyber Threat Situations (CTSs) is subject to many challenges due to the interconnectedness between decision-making agents and assets in cyber and physical space, and the high levels of uncertainty inherent to the cyber domain (Jøsok et al., 2016). This results in decision-making often having to be made on an insufficient information basis which makes it difficult to predict the impact of decisions on own and third-party assets, as well as on adversarial behavior (Jøsok et al., 2016). Other challenges to decision-making include competence differences between analyst-level and decision-making personnel (Knox et al., 2018), which are roles that often are assigned to different individuals within organizations doing cybersecurity operations (e.g., Security Operation Centers; SOCs).

Due to the interconnectedness between assets and decision-making agents in the cyber and physical domains and the resulting human-human and human-machine interactions, cybersecurity operations unfold in a complex sociotechnical system. According to the Situational Awareness (SA) model (Figure 1A) proposed by Endsley (1988, 1995), establishing SA for decision-making in sociotechnical systems is achieved in three levels, where all levels must be achieved in order to have full SA.

SA Level 1 is the perception stage and involves perceiving the elements in a situation. SA Level 2 is the comprehension stage and involves understanding the relationship between the perceived elements. SA Level 3 involves using the understanding of the relationship between

the elements to predict future states of the system that the situation is occurring in, and how those future states will be affected by decision-making (Endsley, 1995).

In a cybersecurity setting, SA is increasingly referred to as Cyber SA (CSA; Barford et al., 2009; Franke and Brynielsson, 2014). Extending on the formal definition of SA (Endsley, 1988), CSA is considered a subset of SA and can in general terms be defined as "*the perception of the elements in the [cyber] environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future*" (Franke and Brynielsson, 2014, p. 4). It should be noted, however, that it is acknowledged that actions in the physical domain may influence events in cyberspace and vice versa (Jøsok et al., 2016). Consequently, stakeholders and decision-makers are often required to have a SA that simultaneously accounts for the impact of decisions in both the cyber and the physical domain.

Seven requirements for achieving CSA for cyber defense decision-making have been suggested (Barford et al., 2009). These requirements can be arranged under the SA model proposed by Endsley (Figure 1B). To achieve SA Level 1 during a CTS, one must have perceived indicators of compromise allowing for (1) awareness of the current situation; (2) awareness of the impact of the attack; (3) awareness of adversarial behavior; and (4) awareness of the quality and trustworthiness of CSA information. To achieve SA Level 2, one must have (5) awareness of why and how the current situation is caused (e.g., if it is an automatic or directed attack), and (6) awareness of how situations evolve. To achieve SA Level 3, one must be able to (7) assess plausible future outcomes.

Decision-making in CTSs is based on communication between human agents that often differ in technical competence (Knox et al., 2018). The point of communication is to establish a shared CSA between the analyst and the decision-maker such that the decisionmaker can make good cyber defense decisions. This communication happens in the form of the analyst communicating a Recognized Cyber Picture (RCP) which is based on the analyst's CSA and contains carefully selected and actionable cyber threat information tailored to the needs of the recipient (Ahrend et al., 2016; Staheli et al., 2016; Ask et al., 2021a). A recent review of performance-related factors in SOC teams suggested that insufficient communication was among the biggest challenges faced by SOC team analysts but also one of the least researched topics (Agyepong et al., 2019). Another recent review (Ask et al., 2021a) that specifically looked at communication between humans in CTSs found that (a) there were no common best practices for information sharing; (b) technological aids (e.g., visualization tools and

information sharing platforms) were not suited to fit the needs of the analysts; (c) there was a lack of studies simultaneously assessing individual- and team-level performance metrics; and (d) there was a general need for developing shared mental models for effective cyber threat communication.

In contrast to many other working environments, the personnel working within the cyber domain (NATO Cooperative Cyber Defense Center of Excellence, 2016) do not have direct sensory access to the space where events are taking place. In other words, when cyber personnel such as analysts are establishing CSA they are essentially trying to predict the future state of an environment they cannot directly observe. Instead, they are dependent on (1) tools that can detect and visualize events and activities in their cyber domain; and (2) their own mental models of that space. This may be a source of friction when relaying information between individuals because different individuals may have different mental models of the same phenomena, with corresponding differences in their understanding of the causal relationships contributing to those phenomena. This may affect what information different individuals think is important during a cyber threat situation (Ask et al., 2021a). For instance, previous research on the RCP needs of local- and national-level stakeholders in Sweden showed that no one listed knowledge about adversarial behavior as important for their RCPs (Varga et al., 2018). If awareness of adversarial behavior is required for achieving SA Level 1 during a CTS and is necessary to make good cyber defense decisions (Barford et al., 2009), then ignoring information of adversarial behavior may result in an insufficient CSA. Thus, stakeholders may have a mental model of causal relationships during a CTS that affect what kind of prioritizations they have and decisions that they make based on those prioritizations (Ask et al., 2021a).

While developing shared mental models have been suggested to ensure successful RCP communication during CTSs (Steinke et al., 2015; Ask et al., 2021a), little is known about the effect of visualization tools for cyber threat information communication and shared CSA such as how network topology is represented visually. The mammalian brain has evolved a neural architecture with an innate ability to process and understand information that relates to time and space (Eichenbaum, 2014; Ray and Brecht, 2016; Berggaard et al., 2018). Typical representations of network topology are in two dimensions (2D), which loses temporal and spatial relationships between nodes in the network, in addition to not scaling well with increased (but often necessary) complexity. Virtual Reality (VR) and Mixed Reality (MR) tools

that are able to visualize CSA-relevant information such as network topology as 3D objects in space and time, may aid in the development of shared mental models for efficient RCP communication between technical and non-technical personnel (Kullman et al., 2018, 2019a,b, 2020). For instance, SA level 3 is the most vital stage for decision-making and appears to be the stage that is the most dependent on human working memory (Gutzwiller and Clegg, 2013). 3D visualizations of network topology in VR/MR may leverage automatic neurocognitive processes for encoding spatial information (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008) when individuals are establishing a shared mental model of events in the network. If this allows CTS information to be encoded more efficiently (e.g., Legge et al., 2012; Wagner et al., 2021), it may also allow for more working memory capacity to be allocated to sharing knowledge about the course and impact of current and future events. Reducing the load on working memory may in turn support establishing shared SA level 3 (Gutzwiller and Clegg, 2013) for decision-making in CTSs (Kullman et al., 2019a).

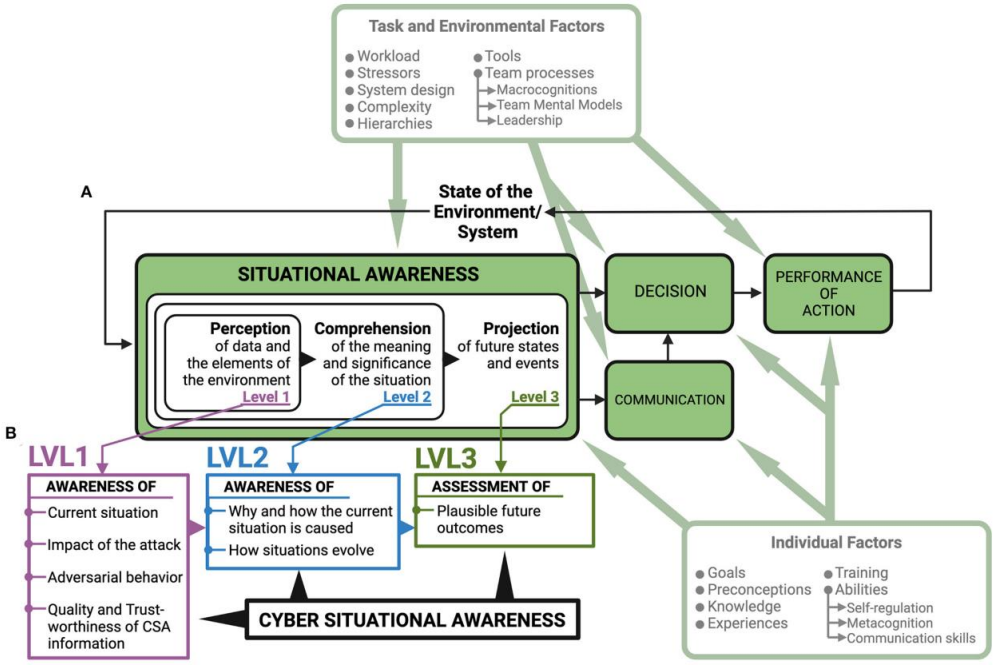

FIGURE 1

Situational Awareness model with suggested requirements for achieving Cyber Situational Awareness. (A) Situational Awareness is achieved in three stages (Endsley, 1995). To account for the separation between analysts and decision-makers in SOCs (Knox et al., 2018; Ask et al., 2021a), a "communication" element has been added to the model. (B) Seven requirements that can be organized under the Endsley model need to be met to achieve Cyber Situational Awareness for

cyber defense (Barford et al., 2009). Establishing Cyber Situational Awareness, communicating for shared Cyber Situational Awareness, and decision-making based on Cyber Situational Awareness is influenced by individual factors such as emotion, metacognition, self-regulation, and communication skills (Jøsok et al., 2016, 2019; Knox et al., 2017, 2018; Ask et al., 2021b, 2023; Sütterlin et al., 2022) and task and environmental factors such as team-processes including macrocognitions, team mental models, and leadership (Jøsok et al., 2017; Ask et al., 2021a). Modified from Lankton (2007).

Studies on VR navigation in humans and mice (Bohbot et al., 2017; Safaryan and Mehta, 2021) showed that they were able to generate brain waves in areas relevant for navigation, attention, learning, and memory (Winson, 1978; Seager et al., 2002). Similarly, previous VR research in humans showed that participants were able to use knowledge about the relationship between geometrical shapes in abstract space to navigate that space in a first-person VR navigation task (Kuhrt et al., 2021). This may further indicate that 3D visualizations that allow for exploring and interacting with network data in a way that facilitates spatial encoding of CSA information could leverage neurocognitive processes (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008) that are currently underused in cyber defense.

The Virtual Data Explorer (VDE; Kullman et al., 2018, 2019a) was developed to visualize network topology in a manner that is idiosyncratic to the mental models that analysts use to conceptualize the network (Figure 2). Based on interviews with expert analysts, the VDE is able to visualize the relationship between nodes in an actual network in space and time (Kullman et al., 2018, 2019a,b, 2020). The visualizations produced by the VDE are interactive and can be shared between individuals, even remotely, thus allowing for collaborative development of shared mental models of events in the network. The VDE may therefore be a useful aid in the knowledge-transfer between technical and non-technical personnel such that shared CSA can be achieved to facilitate good cyber defense decision-making (Kullman et al., 2019a).

The VDE uses two distinct sets of information to visualize network topology: (1) the nodes included in a set of network traffic, and (2) mockup connections during a specified time-window or an attack path (Kullman et al., 2018). For the sake of clarity, we want to specify that the VDE is not a tool for carrying out forensic analyses. Instead, by visualizing network topology in time and space according to the mental model of the operator (Kullman et al., 2018, 2019a), the VDE may be a neuroergonomic tool for analysts to deepen their own understanding of how a CTS relates to the network they are tasked with defending, and for sharing CSA in complex working environments such as cybersecurity (Kullman and Engel, 2022a,b).

In the present study, we assess the effect of 3D visualization of network topology on communication and collaboration for CSA and cyber defense decision-making. The aim of this study is to determine if a 3D MR representation of a network attack, visualized by VDE is better than a 2D representation for (1) achieving Cyber Situational Awareness; (2) cyber team communication; and (3) decision-making among cooperating dyads during a simulated CTS.

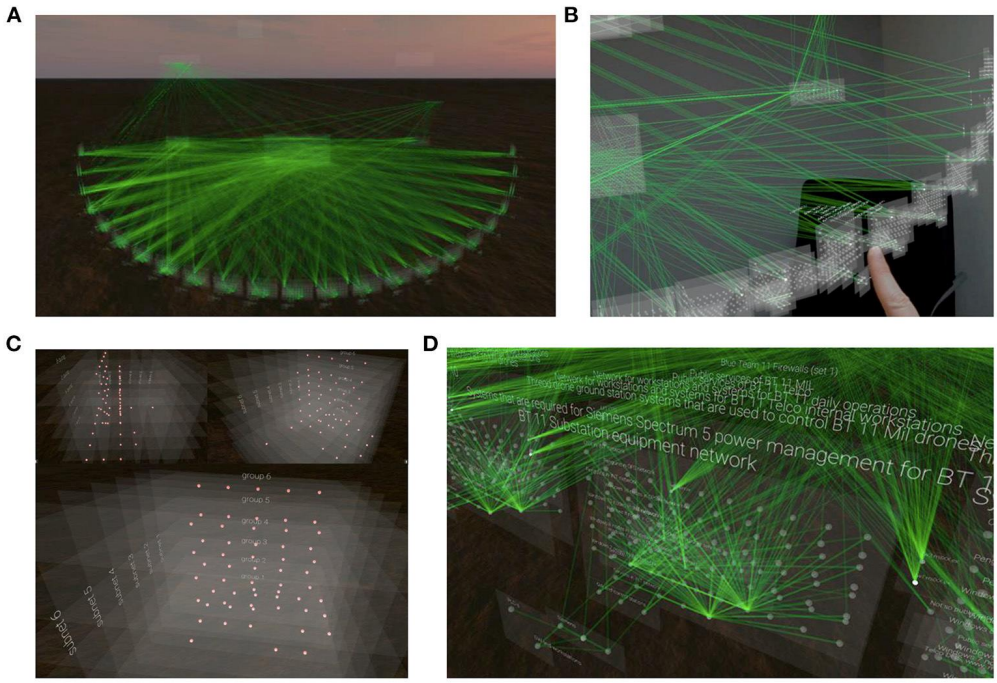

FIGURE 2

Visualization of network topography using the Virtual Data Explorer app. (A) Full overview of the metashape of the actual network that was used during the NATO CCDCOE 2018 Locked Shields event as visualized in VR using the VDE app. (B) An individual interacting with the network topography in MR. (C) A close-up of nodes in the network from different angles and without the edges representing the connections between them. (D) A close-up of Blue Team nodes in the network with descriptive information and the edges that connect them. Images taken from Kullman et al. (2019a).

2. Materials and methods

2.1. Ethics statement

This study was conducted under the Advancing Cyber Defense by Improved Communication of Recognized Cyber Threat Situations (ACDICOM) project. The present study conformed to institutional guidelines and was eligible for automatic approval by the Norwegian Social

Science Data Services' (NSD) ethical guidelines for experimental studies. Participation was voluntary and all participants were informed about the aims of the study; the methods applied; that they could withdraw from participation at any time and without any consequences; and that, if they did so, all the data that was gathered from them would be deleted. After volunteering to participate in the study, participants were asked to provide informed consent on the first page of an online form where baseline data was collected. Participants were asked to generate and remember a unique participant ID that they would use during data collection for the duration of the study.

2.2. Participants and design

This experiment employed a pseudo-randomized head-to-head design using VDE in the experimental condition and the packet capture software Arkime (formerly Moloch) as the control condition. Participants (N = 22, mean age = 22.5, female = 5) were cyber cadets recruited from the Norwegian Defense University College, Cyber Academy (NDCA). Half of the cadets were specializing in military Information Communication Technology (ICT) systems while the other half were specializing in cyber operations.

The study consisted of two parts distributed over 3 days, where day one was used for gathering informed consent, and collecting demographic and baseline cognitive trait data. Results related to the cognitive data will be reported elsewhere. Day two and three was used for the experiment. After providing informed consent and filling out initial questionnaires, participants were randomized in dyads and allocated to either the VDE or the Arkime condition. During the experiment, dyads had to collaborate to familiarize themselves with the network topology and to identify indicators of compromise. The participants in the VDE condition used HoloLens 2 (Microsoft) for the MR visualizations of network topology as their only aid. The participants in the Arkime condition also had a 2D schematic illustration of the network topology available to them in paper format.

The network topology and activity used for this experiment was visualized using network data from the 2022 Locked Shields Cyber Defense Exercise (CDX) provided by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). The experiment lasted for approximately 2 h per dyad.

2.3. HoloLens 2

Microsoft HoloLens 2 (Microsoft, Redmond, DC) has become the most common MR headset to be used for various research studies, fielded by enterprises and governments for Interactive Stereoscopically Perceivable Multidimensional Data Visualizations (ISPMDV; see Kullman and Engel, 2022b for an introduction), where its mostly used for either geospatial or natively spatial datasets. For the purposes of this study, HoloLens 2 was chosen for its capabilities, ease of software development, and existing compatibility with VDE.

2.4. The Virtual Data Explorer and visualization of network topology

VDE (Kullman et al., 2018, 2019a,b, 2020; [https://coda.ee/]) enables a user to perceive the spatial layout of a dataset, for example the topology of a computer network, while the resulting ISPMDV (Kullman and Engel, 2022a,b) can be augmented with additional data, like TCP/UDP session counts between network nodes. Users can customize ISPMDV layouts using textual configuration files that are parsed by a VDE Server and used while showing the visualization by a VDE Client.

VDE functionality is decoupled to server and client components in order to accommodate timely processing of large query results (from the user's dataset) in a more powerful environment (than a wireless MR headset) before data is visualized either by a VR or MR headset. The VDE Server also acts as a relay to synchronize the visualizations (e.g., grabbed objects position in connected users' views) between connected users' sessions so that a connected user's actions manipulating a visual representation of data can be synchronized with other connected users working with that same dataset.

Only a subset of VDE capabilities was employed in the present study: the dataset was preloaded to the headset along with the application (to avoid any possible networking related issues) while VDE Server was used only to facilitate multi-user sessions.

A previous study indicated that there was a need for more experimental collaboration between cognitive scientists and CDX organizers (Ask et al., 2021a). For this study, a NATO CCDCOE Locked Shields 2022 CDX Blue Team's network topology was visualized for the participants with VDE and overlaid with edges (network session counts) between cubes (networked entities). Within view at any given time (depending on user's location and direction) were up to 958 nodes and groups, with up to 789 edges.

All study participants perceived the ISPMDV being positioned in the same location and direction in the room where the study was conducted (see Figure 3A, image on the left).

Participants did not have the capability to reposition the visualization components permanently, but they could grab (pinch) a node to better understand its connections while temporarily moving the node around. Once the participant let go of the node, it returned smoothly to its initial location.

As the study participants did not have prior knowledge of Locked Shields 2022 networks and topology, the topology visualization they experienced was not created based on their mental models (as would be the suggested course of using VDE after employing mental model mapping method for cybersecurity; Kullman et al., 2020). Instead, the participants received an introduction about the topology as described in the task one procedures (Section 2.7.1.).

2.5. Arkime packet capture software

Arkime (v3.4.2 [https://arkime.com/]) was used for preparing the dataset from Locked Shields 2022 network traffic both for the VDE ISPMDV view, as well as for the comparative group that used 2D and textual information. Participants were given access to an Arkime instance and taught the basics of using its interface (Sessions and Connections tabs). In the Connections tab, participants had a 2D graph view (see Figure 3B, image on the right) onto the exact same set of nodes and edges that VDE participants had with HoloLens. When participants hoovered over the edges connecting nodes (hosts) to each other, the amount of traffic was displayed on a left-hand panel as described in the task two procedures (Section 2.7.2.).

2.6. Hardware functionality and operational stability

The HoloLens 2 headsets had a tendency to overheat after a period of use, upon which the Windows Operating System running the headset froze the VDE application. This left the network visualization flickering in the user's view. As this issue only started to manifest during the second half or the 1st day of the study, we suspected that the problem originated from thermal issues. To keep the study going, we relied on three HoloLens 2 headsets, of which two were used by a dyad on the floor while the third one was being charged. Rapid charging and then discharging while the headset's GPU and CPU were being heavily utilized by the VDE application seemed to have been too much for the headset's thermal dissipator. Switching a participant's malfunctioning headset during a trial was sub-optimal, hence we needed a more sustainable setup. The solution for the HoloLens 2 overheating problem was to use power delivery capable battery packs. The setup on the 2nd day was for the users to wear the headsets, while having battery packs in their pockets that were connected to the headsets with power

delivery capable cables. This allowed the headsets to be used uninterrupted for the duration of a given dyad's trial.

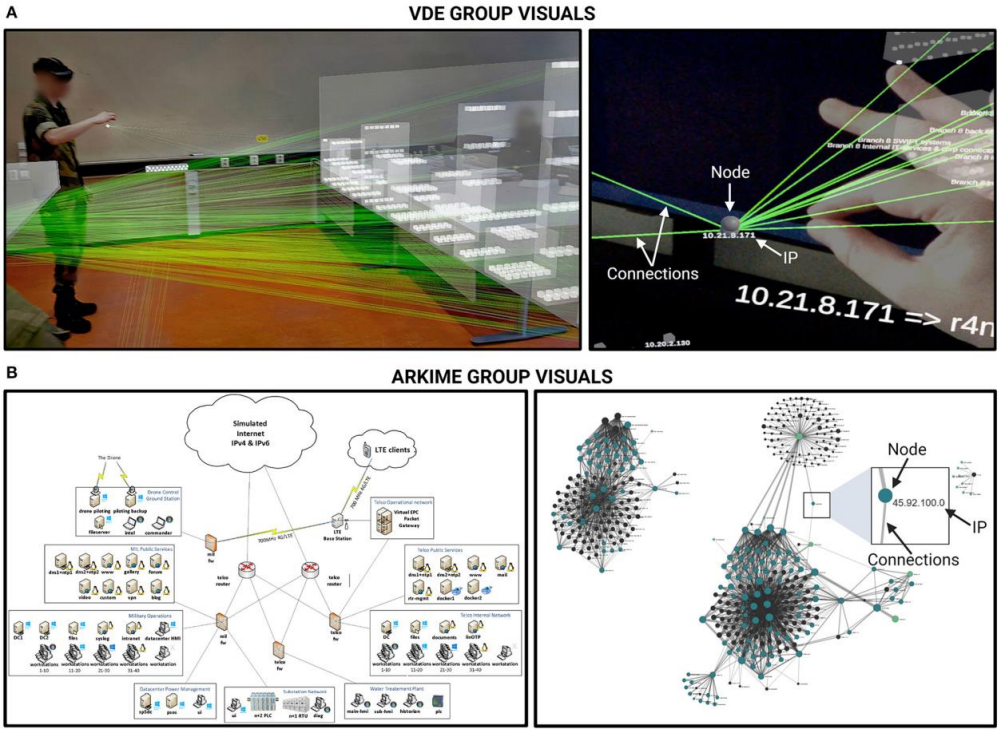

FIGURE 3

Overview of the visualization tools used in each condition. (A) The Virtual Data Explorer (VDE) representation of the network topology. The first image in the panel (left-hand side) depicts an overview of the network layout used in the present study. The second image (right-hand side) is a representative close-up (taken from Kullman and Engel, 2022a). White arrows have been superimposed on the image on the right to indicate node/hosts, edges that represent connections between nodes, and the host IP address. (B) Images depicting the 2D network topology as shown in the Arkime condition. The first image in the panel (left-hand side) depicts an approximation of the 2D representation of network topology as shown in the paper schematics. The second image (right-hand side) depicts a graph representation of the network topology as shown in the Arkime software, where dots are hosts and edges are the connections between them. Participants could zoom in, select nodes to see exclusive connections, session number, and so on. Black arrows have been superimposed on the image on the right to indicate node/host, edges that represent connections between nodes, and the host IP address.

2.7. Procedure

The study was conducted at the NDCA. The two experimental conditions were conducted in parallel, one dyad at a time, and in separate rooms that were secluded from other activities. The

experiment consisted of two parts. In the first part, one participant from each dyad was introduced to the network topology which they then had to explain to the other participant in the dyad. In the second part, participants in each dyad had to collaborate to identify indicators of compromise. Measurements were done thrice; baseline measures upon arrival and then outcome measures after each part of the experiment. For the outcome measures after each part, participants filled out questionnaires assessing task success, confidence in answers, and how they experienced communicational, coordination, emotional, and performance monitoring load related to their teamwork. After part two the participants also had to answer some CSA-related questions that they were not explicitly asked to solve in the task instructions they were given. During the experiment, verbal communication and the time dyads spent on finishing each task was scored by observers. Figure 4 shows an overview of the study and each part of the experiment.

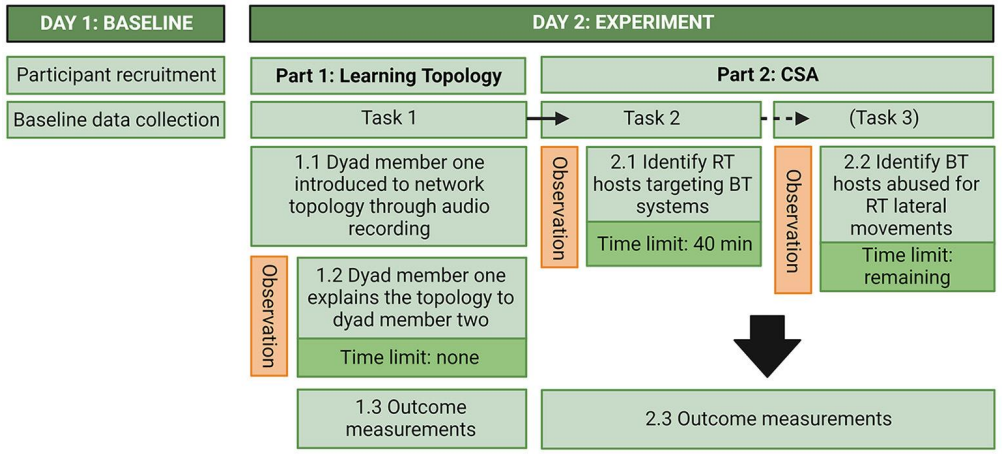

FIGURE 4

Overview of the experiment. RT, Red Team; BT, Blue Team; CSA, Cyber Situational Awareness; VDE, Virtual Data Explorer.

2.7.1. Task one: Understanding the network topology

Upon arriving at the experiment, both participants in the dyad were given a link to the online form which they accessed with laptops. The dyads in the VDE condition spent a few minutes having the HoloLenses they were going to use calibrated to their eyes before filling out the questionnaires. The dyads were referred to as teammates for the duration of the experiment.

After filling out the questionnaires related to the baseline measurements the form presented a prompt telling the participant to pause and wait for instructions. After both participants were

done filling out the questionnaires, one participant was asked to wait outside the room until summoned by the experimenter. The other participant in the dyad was then either told to put on the HoloLenses (if in the VDE condition) to see the 3D representation of the network topology or seated at a table where the 2D schematics of the network topology was depicted (Arkime condition).

Upon confirming that they saw a network in front of them, the participants were played an English audio recording explaining that what they saw was the network that the Blue Team had to defend during the Locked Shields 2022 CDX. The recording lasted for 3 min and 30 seconds. It was explained to them what nodes each segment in the network consisted of, what was considered normal activity, where known Red Team nodes were, and which nodes were unknown. In the VDE condition, the participant was instructed to walk through the nodes and also how to interact with the nodes to probe for further information (e.g., touch node to see the IP address or pinch node to lift up in order to see which nodes it was connected to).

The briefing was only given once (which was stated in the beginning of the recording). After the recording was over, the participant was given the instruction that their task would be to explain the network topology to their teammate. They were instructed to get confirmation from their teammate that they had understood the topology upon which they would either (1) re-explain if their teammate did not understand or (2) let the experimenter know that they had completed the task. After confirming that they had understood the task, the other participant in the dyad was summoned and then the first participant was told to start at their convenience. In the VDE condition, the participant that was summoned was told to put on their HoloLens and confirm that they saw the network representation in front of them before the first participant in the dyad was given the signal to start. There were no time constraints on this task. After signaling that the task was over, the participants were instructed to access their laptops and continue filling out the questionnaires until getting to a prompt asking them to wait for further instructions. In the VDE condition, the participants were instructed to remove their HoloLenses while answering the questionnaires.

2.7.2. Task two: Identifying Red Team hosts targeting Blue Team systems

After both participants were done filling out the questionnaires, they received the instructions for the second task. In the VDE condition, both participants were told to put on their HoloLenses again. This time the 3D representation of the network topology was updated with

more edges connecting each node. The edges varied in brightness depending on the number of sessions (traffic) associated with the connections.

In the Arkime condition, both participants were introduced to a graph representation of the Blue Team network topology in Arkime. They were instructed (1) that they could select nodes to see their associated IP addresses and communications targets (represented by edges between the nodes); and (2) that they could see the session count (amount of traffic) associated with each connection by hovering over the edges connecting each node. The edges varied in thickness depending on the amount of traffic associated with the connection.

The dyads were then instructed to collaborate to find the top five Red Team hosts (nodes) targeting Blue Team systems according to the amount of traffic associated with each connection. For this task, they were given pen and paper to note the IP address associated with each identified Red Team host. The dyads were instructed to confirm with each other when they were done with the task before notifying the experimenter.

Both conditions saw the same network, with the same number of nodes and edges and the same amount of traffic. Participants in the VDE condition could not see the session count associated with each connection but could only use the edge brightness as cue. The participants had 40 min to finish the task, although this was not disclosed to them.

Upon notifying the experimenter that they had finished the task, the participants were given the instructions for the third task. If the time ran out before a dyad could finish the task, they were stopped by the experimenter and told to finish the last set of questionnaires.

2.7.3. Task three: Identifying Blue Team hosts abused for Red Team lateral movements

For the third task, the dyads were instructed to collaborate to find evidence, if any, of Red Team lateral movements and to note down the top five Blue Team hosts that were possibly abused for that purpose according to the amount of traffic associated with the connection.

The dyads were told that they had a time limit and what the duration of that time limit was (which was the time remaining from the 40 min they had to finish the previous task). As for the previous task, they were instructed to confirm amongst each other that they had finished the task before signaling to the experimenter that they were done.

After completing the task (or if the time ran out), the dyads were instructed to complete the last set of questionnaires. This was done individually. They were allowed to look at their notes from

tasks two and three when answering questions about hosts and IP addresses but were not allowed to communicate or collaborate when answering the questionnaires.

After the Arkime group was done with the experiment, they also did the first task of the VDE condition, receiving instructions as described previously. The roles for task one were the same as in the Arkime condition, meaning that the participant who explained the topology to their teammate in the Arkime condition also did so in the VDE condition. Initially, we wanted the Arkime group to run through the entire experiment in the VDE condition as well. Due to time constraints and the experiment needing to be conducted on the same day, this was limited to completing the first task. Data related to these measurements will be reported elsewhere.

2.8. Data measures

2.8.1. Understanding the network topology

Per definition (Endsley, 1988; Franke and Brynielsson, 2014), to acquire CSA during a CTS in a cyber environment, one must necessarily know the normal state of the environment. To assess the participants' understanding of the network topology, we used a questionnaire partly inspired by the CSA for Analysts Questionnaire (Lif et al., 2017). The CSA questionnaire asks participants to draw a description of the network topology with sources and targets of attack. As our measurements were collected digitally, we employed a forced choice questionnaire where participants had to choose the one of four images that had the most correct 2D depiction of the network topology they had reviewed. The images varied in how connections between Blue Team segments were depicted, while some network segments were missing from the incorrect topology images. To avoid problems with resolution, the images were numbered and presented on laminated A3 paper while the participant provided their answers in the online form. Correct answers were scored as 1 and incorrect answers were scored as 0.

Our initial plan was to have two sets of forced choice questionnaires (in two different formats) that both conditions had to answer. One set would include the 2D schematics that were used in the forced choice questionnaire administered in the present study, while the other set of network topology images would be based on the 3D representation in VDE. Each set of questionnaires would therefore favor the condition where the format matched the condition (e.g., the 2D images favor the Arkime condition where 2D representations of the network topology is part of the tools available to the participants). The idea was that, if one condition performed better on the forced choice set that favored the other condition, this would say something about the

level of understanding of the network topology that the participants were able to extract from either the 2D schematics or the VDE representation. However, due to time restraints, we could only use one set of forced choice questionnaires. As the current forced choice questionnaire favors the Arkime condition, it also serves as a test for whether the VDE representation induces overconfidence if the VDE group performs worse on this test than the Arkime group but is more or equally confident in their answers.

2.8.2. CSA item 1: Adversarial behavior

To assess the outcome of task two, one of the items asked: "What are the possible Red Team hosts that were targeting the Blue Team systems?". The participants had to write down the five IP addresses that they identified during task two. The answers were used to generate three variables: (1) total number of hosts identified, (2) total number of correctly identified hosts, and (3) total number of sessions associated with correctly identified hosts.

2.8.3. CSA item 2: Impact of the attack

To further assess the participants' CSA, they were asked to "Choose Blue Team segments in which the Red Team has been trying to compromise Blue Team hosts". For this item, the participants were given a multiple-choice questionnaire listing five Blue Team segments that were possibly affected. The participants could choose as many as they wanted. Because all of the segments were affected, answers on this item were scored by adding up all the segments that were chosen by the participants giving a numerical score ranging from 0 (the minimum of correct answers) to 5 (the maximum of correct answers).

2.8.4. CSA item 3: Situational report

To assess their comprehension of the cyber threat situation (awareness of the current situation, what caused it, and how it may evolve), participants were asked to answer three qualitative, openended questions. The questions were taken from a SITREP developed by one of the co-authors for use in cyber defense exercises. The questions included: "(1) Describe the activity you saw (specific but not overly detailed)", "(2) What type of incident do you think it was?", and "(3) If you could suggest anything - which actions should be done?".

The answers were blinded and scored individually by one of the co-authors who participated at Locked Shields 2022 exercise and had access to the ground truth of the dataset used. The answers were scored on a 5-point scale ranging from 0 (not correct/irrelevant) to 1

(correct/relevant). The answers were given an overall k-score ranging from 0 (not thorough) to 9 (thorough) to indicate the level of thoroughness combined in the answers to all three questions.

2.8.5. CSA item 4: Adversarial behavior and impact of attack

To measure the outcome of task three, participants were asked: "If any, what were the indicators of Red Team lateral movements in Blue Team networks? Name BT hosts that were (possibly) (ab)used for that purpose." The participants had to write down the IP addresses that they identified during task three. Answers on this item were used to generate three variables: (1) total number of hosts identified, (2) total number of correctly identified hosts, and (3) total number of sessions associated with correctly identified hosts.

Because the information required to solve task three was available to all participants at all times from the initiation of task two, all participants had to answer this item regardless of whether they were given the opportunity to solve task three or not.

2.8.6. Confidence in answers

After each question, participants were asked to rate how confident they were in their answers on a 11-point scale ranging from 0 to 100%.

2.8.7. Decision-making forced-choice task

To assess the effect of condition on decision-making, participants were asked to answer a forced-choice decision-making question with four possible alternatives. The item asked: "If you could only pick one course of action, which would you pick?". The four alternatives were: (1) Cut off all connectivity from the friendly networks to outside, (2) Start incident response on selected hosts, (3) Launch attacks against the hosts that the suspected adversaries might be using, or (4) Cut off connectivity to a selection of network segments. An additional question was asked: "If you picked 4, what would be your suggested network segments?". Each choice was used to generate four variables scored as 0 (not chosen) and 1 (chosen).

2.8.8. Team workload questionnaire (select items)

The Team Workload Questionnaire (TWLQ; Sellers et al., 2014) was used to assess how participants experienced workload demands on team tasks during the exercise. The items are scored on an 11point Likert scale ranging from very low to very high. High scores indicate

higher levels of subjective workload. The TWLQ consists of six subscales divided on two dimensions, the Teamwork component (communication, coordination, team performance monitoring) and Task-Team component (time-share, team emotion, team support). For the purpose of the present study, we were mainly interested in the communication demand item as an indicator of whether the VDE would reduce communication demands. We were also interested in the items related to coordination demand, demand for controlling their own emotions, and demand for monitoring their own performance. The four TWLQ items were administered two times; the first at the end of task one and the second at the end of the experiment.

2.8.9. Structured observation

Structured observation was performed to assess the frequency of occurrence for four verbal communication behaviors: (1) Orient, Locate, Bridge (OLB) processes, (2) perceptual shared mental modeling, (3) task resolution, and (4) communication dysfunction.

OLB behaviors included communication behaviors related to perspective taking and grounded communication to achieve a shared understanding of the situation in accordance with the OLB model (Knox et al., 2018). Some examples included when members of the dyads asked questions to probe each other's understanding of what was communicated; adjusted language (from technical to less technical) to make sure the recipient understood the significance of what was communicated; and gave each other updates to maintain a mutually shared overview of what they were doing and discovering at any given moment.

Perceptual shared mental model behaviors included verbal communication related to achieving a shared perception of anything related to the task. Examples included utterances such as "Come here and look at this," "When I stand here I see x," "Do you see this node? It is communicating with that node over there," and so on.

A previous observational study indicated that team communication related to task resolution was different between welland poor-performing teams during a CDX (Jariwala et al., 2012). In our study, task resolution behaviors included verbal communication related to the status or completion of the specific tasks that they were assigned. Examples included participants in the dyad asking each other "How many hosts have we found now?", "How many hosts did we have to find again?", and "Should we say that we have completed the task?".

Communication dysfunction behaviors included communication where participants in the dyad talked over/interrupted each other, did not answer each other's questions, argued, went too long (over 2 min) without communicating, and so on. Examples included instances where a participant started explaining what they were seeing and the other participant interrupting them to talk about what they were seeing.

Two observers/coders, one per condition, were used for the scoring of items. Score per dyad was determined by noting frequency of behavioral occurrence during the experiment. The coders agreed how to categorize the behaviors prior to the experiment, and the same coders were used throughout the experiment to ensure reliability. To assess inter-rater reliability, both observers simultaneously scored one of the dyads followed by performing a two-way mixed, absolute, single measures intra-class correlation (ICC) analysis on the raw scores for each item (Shrout and Fleiss, 1979; Hallgren, 2012). Interrater reliability was excellent (ICC = 0.871; Cicchetti, 1994). The observers also noted the time (minutes) spent to finish each task.

2.8.10. User experience measurements

To measure the experience participants had with using the HoloLens 2 and the VDE, we administered the User experience in Immersive Virtual Environment questionnaire (Tcha-Tokey et al., 2016). This data will be reported elsewhere.

2.8.11. Cognitive tests and self-report measures

We collected a range of cognitive trait and state data including measurements that have been identified as relevant for performance in previous studies on cyber cadets and cyber security personnel (Knox et al., 2017; Lugo and Sütterlin, 2018; Jøsok et al., 2019; Ask et al., 2021b; Sütterlin et al., 2022). For instance, positive moods and overconfidence has been found to be associated with poorer metacognitive judgments of CSA during a cyber engineering exercise (Ask et al., 2023), and in detecting cyber threats not directly related to network intrusion (Sütterlin et al., 2022). Conversely, self-regulation abilities measured through self-report and neurophysiological indicators were found to predict cognitive flexibility in terms of mental context shifting during a cyber defense exercise (Knox et al., 2017; Jøsok et al., 2019) and better metacognitive judgements of performance (Ask et al., 2023), respectively. Furthermore, metacognition, self-regulation, and cognitive flexibility are necessary for establishing and communicating CSA (Jøsok et al., 2016; Knox et al., 2018; Endsley, 2020; Ask et al., 2023). Cognitive data was collected with tests and self-report questionnaires on both days of the

experiment. The cognitive data collected on day one included cognitive styles, cognitive flexibility, emotion regulation, vividness of mental imagery, and rumination. The cognitive data collected during the experiment included affective states (baseline) and metacognition (projections for how well they thought they would perform at baseline and correction of how well they thought they had performed after the experiment was over). As noted, the results related to the cognitive data will be reported elsewhere.

2.9. Data analysis

The data were summarized and presented in tables using mean (M) and standard deviations (SD) for continuous and numerical variables, and frequency (count) and percentage (%) for ordinal variables.

The Shapiro-Wilk test of normality and confirmatory visual inspection revealed that most variables were not normally distributed. The exceptions included part one communication demands, part one coordination demands, part one performance monitoring demands, confidence in CSA 1 answers, confidence in CSA 3 descriptions, part two emotion demands, part two performance monitoring demands, and task two OLB. Nonparametric tests were performed for all subsequent analyses except for those variables.

For the non-parametric analyses, the Kruskal-Wallis H test was used for comparisons between the VDE group and the Arkime group. Results were presented as H statistic (degrees of freedom; df), p-values, and effect size. Effect size (η^2) for Kruskal-Wallis H test was calculated as $(H - k + \text{df})/(n - k)$; where H was the Kruskal-Wallis statistic, k was the number of groups, and n was the total number of observations ($n = 22$). Dunn's Post-Hoc test was used to assess significant relationships for non-parametric variables between groups and was reported as z-statistic and Bonferroni adjusted p-values (p_{bonf}).

For the parametric analyses, one-way ANOVAs were performed. Results for ANOVA were reported as F statistic(df), p-values, and effect size. Effect size (ω^2) for ANOVA was calculated as [sum of squares between − $(k - 1)$ mean square within]/(sum of squares total + mean square within). Tukey's post hoc test was used to assess significant relationships for parametric variables between groups and was reported as mean difference (MD) and p_{bonf}. Between-group differences were visualized in interval plots with 95% confidence intervals.

The relationship between communication variables that were significantly different between the groups and CSA variables that were significantly different between the groups were

assessed with Spearman correlation (2-tailed) on *z*-transformed variables. Results were visualized in a heat map and presented as correlation coefficients (ρ) and *p*-values. Separate regression analyses were performed for significant relationships. Results were reported as standardized beta (β), *p*-values, adjusted R^2 (R^2_{Adj}), and F(df) statistics.

Alpha levels for hypothesis testing were set at the 0.05 level for all analyses. All data were analyzed using JASP version 0.15 (JASP Team, 2021).

3. Results

Table 1 presents descriptive statistics of participant characteristics and experimental outcome measurements.

TABLE 1 Descriptive statistics (N= 22).

	Tota			VDE			Arkime		
Variables	M	SD	Count (%)	M	SD	Count (%)	M	SD	Count (%)
Age	22.59	1.36		22.50	1.44		22.70	1.33	
Gender (male)			17 (77.27)			7 (58.33)			10 (100.00)
Military IT systems			13 (59.01)			8 (66.66)			5 (50.00)
Cyber operations			9 (40.90)			4 (33.33)			5 (50.00)
Part 1									
Select correct image	0.59	0.50	13 (59.09)	0.33	0.49	4 (33.33)	0.90	0.31	9 (90.00)
Confidence in choice	61.36	35.49		41.66	33.25		85.00	21.21	
Communication demand	5.90	1.95		5.91	1.73		5.90	2.28	
Coordination demand	4.90	1.82		5.25	1.60		4.50	2.06	
Emotional demand	3.81	3.01		3.66	2.93		4.00	3.26	

Performance monitoring demand	5.13	2.03		4.66	1.96		5.70	2.05	
Part 2									
CSA 1 total RT hosts	3.36	1.62		4.41	1.16		2.10	1.10	
CSA 1 correct RT hosts	2.59	2.01		4.00	1.34		0.90	1.19	
CSA 1 RT hosts total traffic	26525.77	28681.35		48583.25	20069.14		56.80	104.19	
CSA 1 confidence	41.81	26.30		54.16	23.14		27.00	22.63	
Finished task 2 < 40 min	0.72	0.56	16 (72.72)	0.66	0.49	8 (66.66)	0.80	0.42	8 (80.00)
CSA 2 total BT segments	1.59	0.73		2.00	0.73		1.10	0.31	
CSA 2 confidence	40.90	29.09		52.50	26.32		27.00	27.10	
CSA 3 SITREP—activity	0.62	0.36		0.77	0.31		0.45	0.35	
CSA 3 SITREP—incident	0.60	0.42		0.72	0.40		0.45	0.40	
CSA 3 SITREP—actions	0.52	0.42		0.60	0.44		0.42	0.39	
CSA 3 SITREP—K-score	5.04	3.25		6.16	3.29		3.70	2.79	
CSA 3 confidence	38.63	22.52		47.50	19.59		28.00	22.01	
CSA 4 total BT hosts	0.96	1.61		1.50	1.97		0.30	0.67	
CSA 4 correct BT hosts	0.81	1.53		1.33	1.87		0.20	0.63	
CSA 4 BT hosts total traffic	640.54	1086.05		732.50	1040.58		530.20	1184.88	
CSA 4 confidence	40.90	32.05		56.66	27.08		22.00	27.80	

Communication demand	7.63	0.84		7.33	0.77		8.00	0.81	
Coordination demand	6.72	1.77		6.50	2.23		7.00	1.05	
Emotional demand	4.63	2.59		4.41	2.93		4.90	2.23	
Performance Monitoring demand	6.09	2.11		5.91	2.39		6.30	1.82	
Forced decision-making									
Decision 1	0.04	0.21	1 (4.54)	0.08	0.28	1 (8.33)	0.00	0.00	0 (0.00)
Decision 2	0.90	0.29	20 (90.90)	0.83	0.38	10 (83.33)	1.00	0.00	10 (100.00)
Decision 3	0.00	0.00	0 (0.00)	0.00	0.00	0 (0.00)	0.00	0.00	0 (0.00)
Decision 4	0.04	0.21	1 (4.54)	0.08	0.28	1 (8.33)	0.00	0.00	0 (0.00)

CSA, Cyber situational awareness; RT, Red team; BT, Blue team; SITREP, Situational report.

3.1. The effect of VDE on cyber situational awareness

3.1.1. Baseline network topology recognition

Kruskal-Wallis *H* test was performed to assess the differences of condition on task one outcome variables. Table 2 shows the results of the comparisons between the VDE group and the Arkime group on selecting the correct image depiction of the network topology, confidence in image selection, and TWLQ item responses.

The Kruskal-Wallis test showed that the VDE group selected the correct network topology image significantly different from the Arkime group ($p = 0.009$). Dunn's post hoc test showed that the VDE group selected the correct network topology image significantly less than the Arkime group ($z = -2.63$, $p_{bonf} = 0.004$).

The Kruskal-Wallis test showed that the confidence in image selection was significantly different between the VDE group and the Arkime group ($p = 0.006$). Dunn's post hoc test

showed that the VDE group was significantly less confident in their image selection than the Arkime group (z =−2.73, p_{bonf} = 0.003).

No significant differences were observed on any of the TWLQ items measured after the completion of task one.

TABLE 2 Task 1 comparisons between VDE and Arkime (N = 22).

	Kruskal-Wallis test			Dunn's *post hoc*	
Variables	*H* (1)	*p*	η2	z	p_{bonf}
Select the correct image	6.916	0.009	0.295	−2.630	0.004
How confident are you about this?	7.469	0.006	0.323	−2.733	0.003
Emotional demand	0.059	0.808	−0.047	-	-
	One-way ANOVA			Tukey's *post hoc*	
	F (1)	*p*	ω2	MD	p_{bonf}
Performance monitoring demand	1.442	0.244	0.020	-	-
Communication demand	0.000	0.985	0.000	-	-
Coordination demand	0.919	0.349	0.000	-	-

η^2, Effect size; p_{bonf}, Bonferroni adjusted p-values; Bold, significant differences; ω^2, Effect size; MD, Mean difference.

3.1.2. Red team movements, attack severity, and situational reports

Kruskal-Wallis *H* test was performed to assess the differences in the effect of condition on task two and three outcome variables. Table 3 shows the results of the comparisons between the VDE group and the Arkime group on identifying Red Team hosts targeting Blue Team systems, identifying affected blue team segments, assessment of the observed activity, assessment of what incident it was, suggestions of what actions to do as response, identifying Blue Team hosts abused for Red Team lateral movements, confidence in responses, and TWLQ item responses.

Two dyads, one from VDE group and one from Arkime group, spent >40 min on exploring the topology in task one. The dyad in the VDE group spent the least amount of time of all dyads on finishing task two (15 min). The dyad in the Arkime group could not finish task two in <40

min. The maximum amount of time spent to finish task two was 35 min. Thus, the amount of time the dyads had to finish task three ranged from five to 25 min.

There were no significant differences between the groups with respect to finishing task two within the 40-min time limit ($p = 0.495$). In general, the VDE group had higher scores than the Arkime group on all performance outcomes and lower scores on all team workload measures during the second part of the experiment, although not all of these differences were significantly different between groups.

3.1.3. CSA 1: Identifying RT hosts targeting BT systems

The Kruskal-Wallis *H* test showed that the total number the of identified Red Team hosts targeting Blue Team systems was significantly different between the VDE and the Arkime group ($p < 0.001$). Dunn's post hoc test showed that the VDE group identified significantly more Red Team hosts targeting Blue Team systems compared to the Arkime group ($z = 3.40$, $p_{bonf} < 0.001$).

The Kruskal-Wallis *H* test showed that the total number of correctly identified Red Team hosts targeting Blue Team systems was significantly different between the VDE group and the Arkime group ($p < 0.001$). Dunn's post hoc test showed that the VDE group identified significantly more correct Red Team hosts targeting Blue Team systems compared to the Arkime group ($z = 3.58$, $p_{bonf} < 0.001$). Figure 5A shows interval plots for the differences in correctly identified Red Team hosts targeting Blue Team systems.

The Kruskal-Wallis *H* test showed that the activity associated with the correctly identified Red Team hosts targeting Blue Team systems was significantly different between the VDE group and the Arkime group ($p < 0.001$). Dunn's post hoc test showed that the VDE group identified significantly more highly-active Red Team hosts targeting Blue Team systems compared to the Arkime group ($z = 3.97$, $p_{bonf} < 0.001$). Figure 5B shows interval plots for the differences in the traffic associated with correctly identified Red Team hosts targeting Blue Team systems.

One-Way ANOVA showed that confidence in having correctly identified Red Team hosts targeting Blue Team systems was significantly different between the VDE group and the Arkime group ($p = 0.012$). Tukey's post hoc test showed that the VDE group was significantly more confident in having correctly identified Red Team hosts targeting Blue Team systems compared to the Arkime group (MD = 27.45, $p_{bonf} = 0.012$). Figure 5C shows interval plots for the differences in how confident participants were in having identified the correct hosts.

TABLE 3 Comparison of task two and task three results between VDE and Arkime (N= 22).

	Kruskal-Wallis test			Dunn's *post hoc*	
Variables	*H* (1)	*p*	η2	z	^{p}bonf
CSA 1. Number of identified possible RT hosts that were targeting the BT systems	11.603	<0.001	0.530	3.406	<0.001
CSA 1. Correctly identified RT hosts that were targeting the BT systems	12.867	<0.001	0.593	3.587	<0.001
CSA 1. Correctly identified RT hosts that were targeting the BT systems—traffic total	15.822	<0.001	0.741	3.978	<0.001
CSA 2. Compromised BT Segments correctly identified	8.863	0.003	0.393	2.977	0.001
CSA 2. How confident are you about this?	4.121	0.042	0.156	2.030	0.021
Finished task 2 on time	0.467	0.495	−0.026	-	-
CSA 3. SITREP—Describe the activity you saw	4.035	0.045	0.151	2.009	0.022
CSA 3. SITREP—What incident do you think it was?	2.743	0.098	0.087	-	-
CSA 3. SITREP—Which actions should be done?	0.988	0.320	−0.000	-	-
CSA 3. SITREP—Thoroughness K-score	3.044	0.081	0.102	-	-
CSA 4. Total BT hosts abused for RT lateral movements	1.735	0.188	0.037	-	-
CSA 4. Correctly identified BT hosts abused for RT lateral movements	3.681	0.055	0.134	-	-
CSA 4. BT hosts abused for RT lateral movements—Traffic	0.515	0.473	−0.024	-	-
CSA 4. How confident are you about this?	6.651	0.010	0.282	2.579	0.005

Communication demand	3.919	0.048	0.145	−1.980	0.024
Coordination demand	0.029	0.866	−0.048	-	-
	One-way ANOVA			Tukey's *post hoc*	
	F (1)	*p*	ω2	MD	^{p}bonf
CSA 1. How confident are you about this?	7.667	0.012	0.233	27.458	0.012
CSA 3. SITREP—How confident are you about the descriptions above?	4.832	0.040	0.148	19.500	0.040
Emotion demand	0.182	0.674	0.000	-	-
Performance monitoring demand	0.172	0.682	0.000	-	-

η^2, Effect size; p_{bonf}, Bonferroni adjusted *p*-values; Bold, significant differences; CSA, Cyber situational awareness; RT, Red Team; BT, Blue Team; SITREP, Situational report; ω^2, Effect size; MD, Mean Difference.

3.1.4. CSA 2: Identifying compromised BT segments

The Kruskal-Wallis *H* test showed that the number of identified Blue Team segments compromised by the Red Team was significantly different between the VDE group and the Arkime group ($p = 0.003$). Dunn's post hoc test showed that the VDE group identified significantly more Blue Team segments that were compromised by the Red Team compared to the Arkime group ($z = 2.97$, $p_{bonf} = 0.001$).

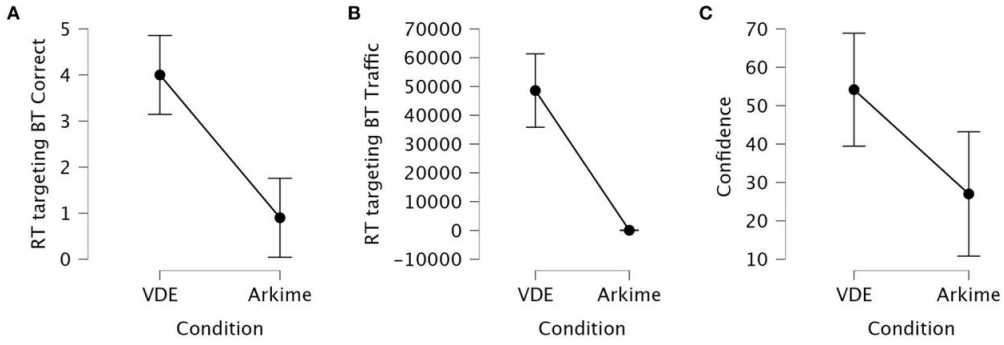

FIGURE 5

Interval plots for the differences in identifying Red Team hosts targeting Blue Team systems. (A) Correctly identified Red Team hosts. (B) Traffic associated with correctly identified Red Team hosts. The number of sessions associated with correctly identified hosts ranged from 27,083 to 75,554 in the VDE group while ranging from 0 to 254 in the Arkime group. (C) Confidence in answers. Whiskers are 95% confidence intervals.

The Kruskal-Wallis *H* test showed that confidence in having correctly identified Blue Team segments compromised by the Red Team was significantly different between the VDE group and the Arkime group (p = 0.042). Dunn's post hoc test showed that the VDE group was significantly more confident in having correctly identified Blue Team segments compromised by the Red Team compared to the Arkime group (z = 2.03, p_{bonf} = 0.021). Figure 6 shows interval plots for differences between the VDE group and the Arkime group in having identified compromised Blue Team segments and confidence in having identified compromised Blue Team segments.

3.1.5. CSA 3: Situational report

The Kruskal-Wallis *H* test showed that the accuracy score for the description of what type of activity they saw was significantly different between the VDE group and the Arkime group (p = 0.045). Dunn's post hoc test showed that the VDE group had a significantly higher accuracy score compared to the Arkime group (z = 2.00, p_{bonf} = 0.022).

The accuracy score for the description of type of incident it was (p = 0.098), the relevance score for the suggestion of actions that should be done (p = 0.320), and the thoroughness k-score (p = 0.081) were not significantly different between the groups.

One-Way ANOVA showed that confidence in the SITREP descriptions was significantly different between the VDE group and the Arkime group (p = 0.040). Tukey's post hoc test showed that the VDE group had a significantly higher confidence in their SITREP answers compared to the Arkime group (MD = 19.50, p_{bonf} = 0.040).

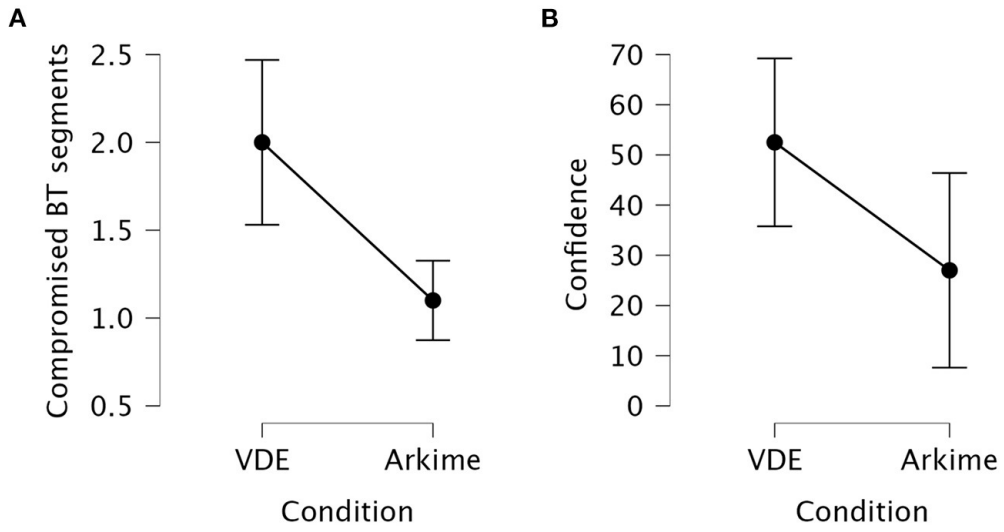

FIGURE 6

Interval plots for the differences in identifying compromised Blue Team systems. (A) Identified compromised Blue Team systems. (B) Confidence in having identified compromised Blue Team segments. Whiskers are 95% confidence intervals.

3.1.6. CSA 4: Identifying BT hosts abused for RT lateral movements

The Kruskal-Wallis *H* test showed that neither the total number of Blue Team hosts abused for Red Team lateral movements ($p = 0.188$), the number of correctly identified Blue Team hosts abused for Red Team lateral movements ($p = 0.055$), nor the number of sessions associated with correctly identified Blue Team hosts abused for Red Team lateral movements ($p = 0.473$) were significantly different between the groups, although the difference in the number of correctly identified Blue Team hosts abused for Red Team lateral movements approached significance.

The Kruskal-Wallis *H* test showed that confidence in the answers was significantly different between the VDE group and the Arkime group ($p = 0.010$). Dunn's post hoc test showed that the VDE group had a significantly higher confidence in their answers compared to the Arkime group ($z = 2.57$, $p_{bonf} = 0.005$).

3.2. The effect of VDE on cyber team communication

3.2.1. Self-reported communication demands

The Kruskal-Wallis *H* test showed that the communication demands during part two of the experiment was significantly different between the VDE group and the Arkime group (p = 0.048). Dunn's post hoc test showed that the VDE group experienced significantly lower communication demands compared to the Arkime group ($z = -1.98$, $p_{bonf} = 0.024$). No other TWLQ measures were significantly different between the groups. Figure 7A shows interval plots displaying differences in part two communication demands between the groups.

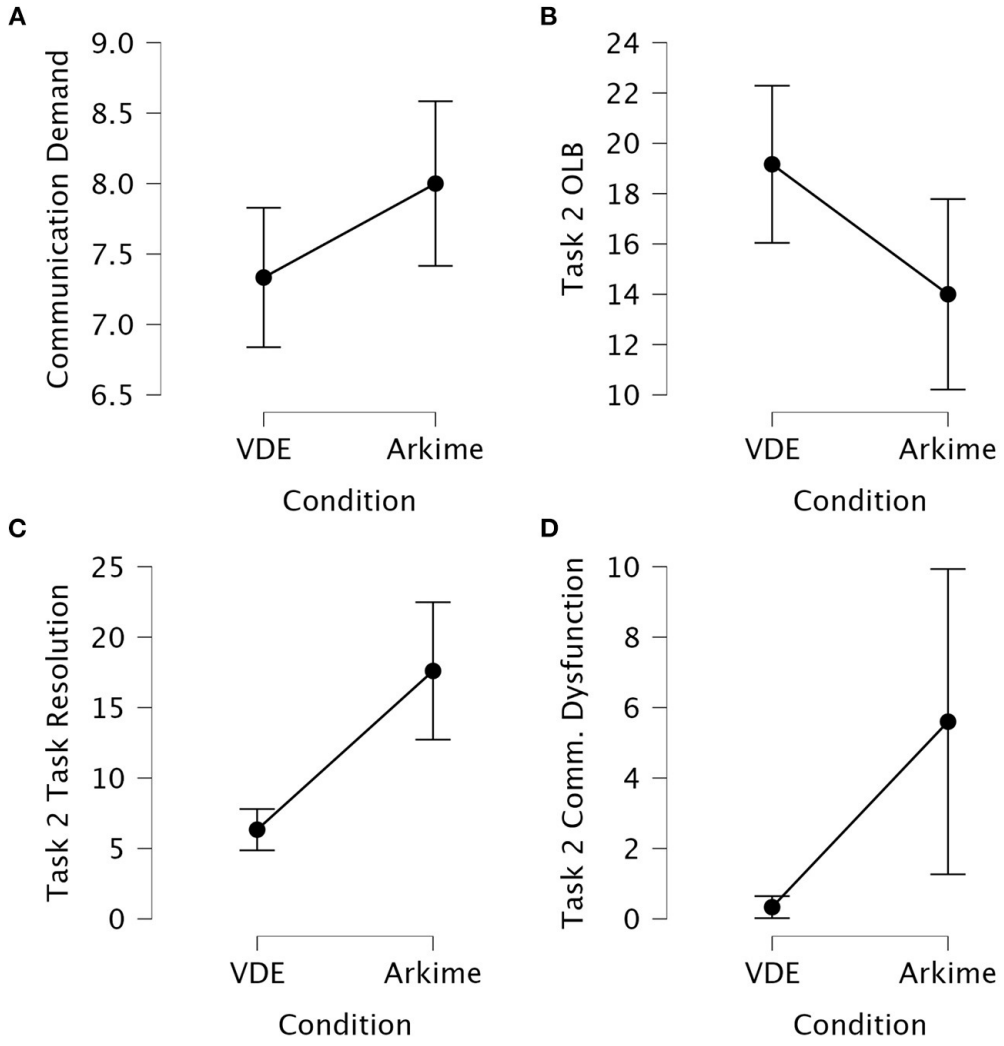

FIGURE 7

Interval plots for between-group differences in self-reported and observed communication variables. (A) Self-reported communication demands after part two of the experiment. (B) Observed task two OLB communication. (C) Observed task

two task resolution communication. (D) Observed task two communication dysfunction. Whiskers are 95% confidence intervals.

3.2.2. Observation of communication behaviors

Kruskal-Wallis H tests and One-Way ANOVAs were used to assess differences on the observed verbal communication scores between the VDE group and the Arkime group. Table 4 presents the result of the comparisons. Figures 7B–D shows interval plots for between-group differences in task two OLB communication, task two task resolution communication, and task two communication dysfunction.

TABLE 4 Comparison of observational scores between VDE and Arkime (N = 22).

		Kruskal-Wallis test			Dunn's *post hoc*	
Variables	M ± SD	*H* (1)	*p*	η2	z	^{p}bonf
Task 1 OLB	10.45 ± 13.00	4.145	0.042	0.157	2.036	0.021
Task 1 perceptual shared mental models	9.00 ± 11.75	0.461	0.497	−0.026	-	-
Task 1 task resolution	6.36 ± 11.08	0.000	1.000	−0.50	-	-
Task 1 communication dysfunction	0.27 ± 0.63	0.000	1.000	−0.50	-	-
Task 1 time to finish (min)	11.72 ± 15.46	0.000	1.000	−0.50	-	-
Task 2 perceptual shared mental models	16.90 ± 5.54	0.018	0.894	−0.049	-	-
Task 2 task resolution	11.45 ± 7.46	15.968	<0.001	0.748	−3.996	<0.001
Task 2 communication dysfunction	2.72 ± 4.80	4.101	0.043	0.155	−2.025	0.021
Task 2 time to finish (min)	28.90 ± 9.12	13.013	<0.001	0.600	−3.607	<0.001
Task 3 OLB	6.09 ± 8.79	0.916	0.339	−0.004	-	-
Task 3 perceptual shared mental models	5.45 ± 7.96	1.162	0.281	0.008	-	-
Task 3 task resolution	3.00 ± 3.59	0.898	0.343	−0.005	-	-

Task 3 communication dysfunction	0.90 ± 1.54	1.825	0.177	0.041	-	-
Task 3 time to finish (min)	6.27 ± 7.09	0.299	0.585	−0.035	-	-
		One-way ANOVA			Tukey's *post hoc*	
		F (1)	*p*	ω2	MD	$_{p}$bonf
Task 2 OLB	16.81 ± 5.62	5.625	0.028	0.174	5.167	0.028

η^2, Effect size; p_{bonf}, Bonferroni adjusted *p*-values; Bold, significant differences; OLB, Orient, Locate, Bridge; ω^2, Effect size; MD, Mean difference.

The Kruskal-Wallis H test showed that the VDE group had significantly different task one OLB scores compared to the Arkime group ($p = 0.042$). Dunn's post hoc test showed that the VDE group performed significantly more OLB communications during task one compared to the Arkime group ($z = 2.03$, $p_{bonf} = 0.021$). No other comparisons from task one were significant.

The one-way ANOVA showed that the VDE group had significantly different task two OLB scores compared to the Arkime group ($p = 0.028$). Tukey's post hoc test showed that the VDE group performed significantly more OLB communications during task two compared to the Arkime group (MD = 5.16, $p_{bonf} = 0.028$).

The Kruskal-Wallis H test showed that the VDE group had significantly different task two task resolution scores compared to the Arkime group ($p < 0.001$). Dunn's post hoc test showed that the VDE group performed significantly less task resolution communications during task two compared to the Arkime group ($z = -3.99$, $p_{bonf} < 0.001$). The Kruskal-Wallis H test showed that the VDE group had significantly different task two communication dysfunction scores compared to the Arkime group ($p = 0.043$). Dunn's post hoc test showed that the VDE group had significantly less communication dysfunction during task two compared to the Arkime group ($z = -2.02$, $p_{bonf} = 0.021$). The Kruskal-Wallis H test showed that the VDE group had significantly different task two Time-to-finish scores compared to the Arkime group ($p < 0.001$). Dunn's post hoc test showed that the VDE group had significantly lower time-to-finish scores during task two compared to the Arkime group ($z = -3.60$, $p_{bonf} < 0.001$).

Perceptual shared mental models were not significantly different between the groups. No comparisons were significantly different between groups with respect to task three observational scores.

3.2.3. Relationship between communication variables and CSA items

Spearman correlations were performed to assess the relationship between communication variables and CSA variables that were significantly different between the VDE group and the Arkime group. Figure 8 presents a heat map showing the results from the correlational analysis.

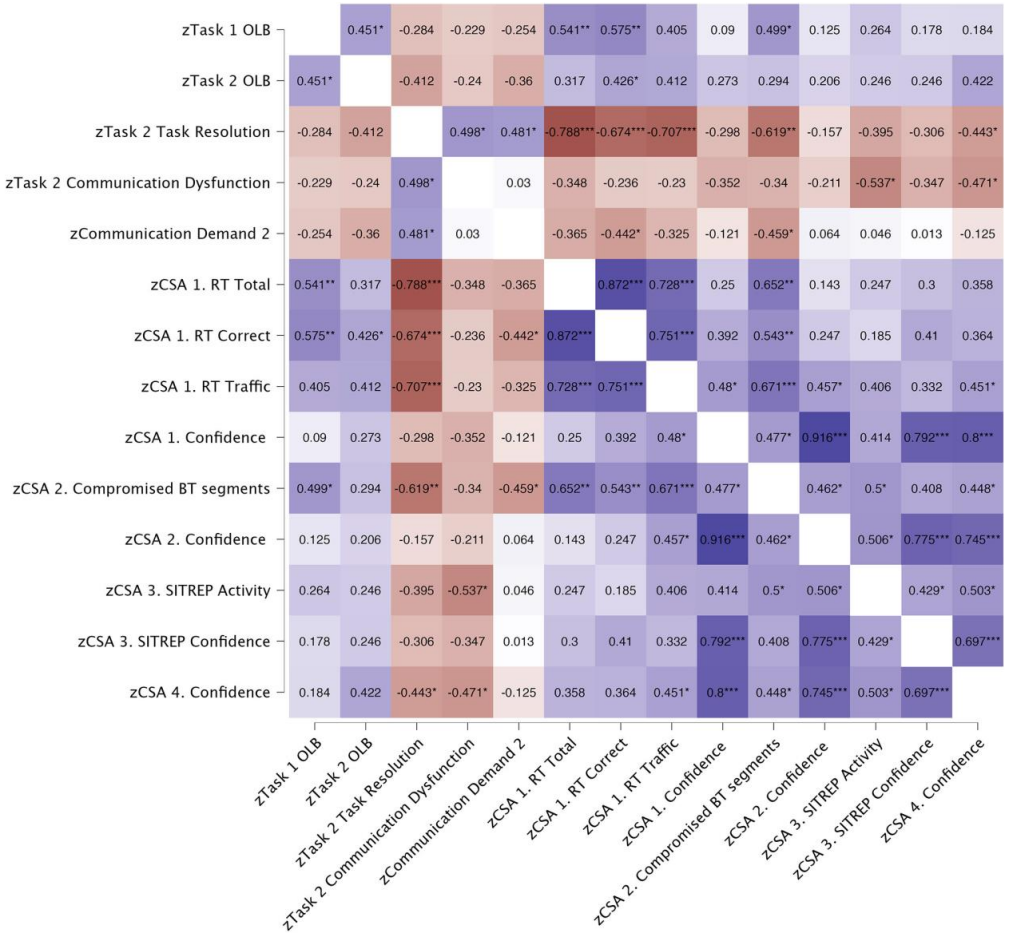

FIGURE 8

Heat map showing results from Spearman (_) correlations. All correlations are 2-tailed. Blue color indicates positive correlations. Red color indicates negative correlations. *$p < 0.050$, **$p < 0.010$, ***$p < 0.001$. OLB, Orient, Locate, Bridge (Knox et al., 2018); CSA, Cyber situational awareness; RT, Red team; BT, Blue team; SITREP, Situational report.

Task one OLB scores were significantly and positively correlated with task two OLB scores ($p = 0.035$), total number of identified Red Team hosts targeting Blue Team systems ($p = 0.009$), total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.005$), and identifying compromised Blue Team segments ($p = 0.018$).

Task two OLB scores were significantly and positively correlated with total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.048$).

Task two Task resolution scores were significantly and positively correlated with task two Communication dysfunction ($p = 0.018$), communication demands ($p = 0.024$), and negatively correlated with total number of identified Red Team hosts targeting Blue Team systems ($p < 0.001$), total number of correctly identified Red Team hosts targeting Blue Team systems ($p < 0.001$), total amount of traffic associated with correctly identified Red Team hosts targeting Blue Team systems ($p < 0.001$), identifying compromised Blue Team segments ($p = 0.002$), and confidence in having identified Blue Team hosts abused for Red Team lateral movements ($p = 0.039$).

Task two communication dysfunction scores were significantly and negatively correlated with the accuracy score for the description of what type of activity they saw ($p = 0.010$), and confidence in having identified Blue Team hosts abused for Red Team lateral movements ($p = 0.027$).

Part two communication demands were significantly and negatively correlated with total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.039$), and identifying compromised Blue Team segments ($p = 0.031$).

No other correlations were significant.

Separate linear regressions were performed for significant correlations. Significant results are shown in Table 5. Task two task resolution was a significant negative predictor of total number of identified Red Team hosts targeting Blue Team systems ($p < 0.001$), total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.002$), total amount of traffic associated with correctly identified Red Team hosts targeting Blue Team systems ($p < 0.001$), and identifying compromised Blue Team segments ($p = 0.008$). No other relationships were significant.

T ask two communication dysfunction was a significant negative predictor of the accuracy score for the description of what type of activity they saw ($p = 0.012$), and confidence in having identified Blue Team hosts abused for Red Team lateral movements ($p = 0.012$).

Communication demands was a significant negative predictor of the total number of correctly identified Red Team hosts targeting Blue Team systems ($p = 0.034$). No other relationships were significant.

TABLE 5 Linear regressions ($N_{=}$ 22).

Predictor	Dependent variable	β	*p*	*R*2Adj	*F* (1)
Task two task resolution	RT hosts targeting BT systems total	−0.763	<0.001	0.561	27.845
Task two task resolution	RT hosts targeting BT systems correct	−0.630	0.002	0.366	13.142
Task two task resolution	RT hosts targeting BT systems traffic	−0.665	<0.001	0.415	15.889
Task two task resolution	Identifying compromised BT segments	−0.547	0.008	0.264	8.534
Task two communication dysfunction	SITREP—Describe the activity you saw	−0.524	0.012	0.238	7.553
Task two communication dysfunction	BT hosts abused for RT lateral movements confidence	−0.525	0.012	0.239	7.594
Communication demands	RT hosts targeting BT systems correct	−0.454	0.034	0.166	5.178

RT, Red team; BT, Blue team; SITREP, Situational report.

3.3. The effect of VDE on decision-making

All the participants except two ($n = 20$) picked the “Start incident response on selected hosts” option on the forced-choice decision-making task. Thus, there was no difference between the groups. The other two participants, both in the VDE condition but not in the same dyad, picked the “Cut off all connectivity from the friendly networks to outside” and the “Cut off connectivity to a selection of network segments” options.

4. Discussion

Cyber defense decision-making during CTSs is based on human communication aiming to establish a shared CSA between analyst-level and decision-making personnel (Knox et al., 2018). Communication for shared CSA is one of the main problems facing SOC team analysts (Knox et al., 2018; Agyepong et al., 2019; Ask et al., 2021a). Current visualization tools to support achieving a shared understanding of the CTS include 2D graphs and schematics of network topology. These visualization tools do not scale well with increasing complexity. Furthermore, SA level 3 appears to be the SA stage most dependent on human working memory (Gutzwiller and Clegg, 2013). The mammalian brain has developed an innate ability to understand time and space (Eichenbaum, 2014; Ray and Brecht, 2016; Berggaard et al., 2018). 3D representations of network topology may leverage automatic spatial sensory processes (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008) that reduce load on working memory during communication. Thus, 3D visualizations may be more neuroergonomic than 2D representations by facilitating more efficient communication and shared situational understanding during CTSs, which could support decision-making (Kullman et al., 2019a). In this study, we compared how the representation of a network topology in 3D MR (Kullman et al., 2018, 2020) vs. 2D affected topology recognition, CSA, team communication and decision-making in a sample of cyber cadets.

In the first part of the experiment, the Arkime group performed better than the VDE group on the task where participants had to identify the correct depiction of the network topology among four 2D schematics. This finding was not surprising as the correct depiction was in the same format as the 2D schematic the Arkime group had used to familiarize themselves with the topology.

3D visualizations of network topology are expected to be neuroergonomic in the sense that they leverage innate neurocognitive processes that encode spatial information. Additionally, the VDE visualizes network data based on the mental model that operators have of the network they are defending (Kullman et al., 2020). While both being neuroergonomic and conserving connections and sessions between nodes, the topological layout as visualized in the VDE does not represent the actual reality of the network. This may be problematic if the 3D visualizations contribute to a false sense of confidence in one's understanding of the topology by virtue of being visually persuasive. For instance, previous studies on cyber cadets have shown that high self-confidence in combination with intuitive decision-making can have detrimental effects on

performance when counterintuitive decisions are required (Lugo et al., 2016). Interestingly, while performing worse, the VDE group was also less confident in their answers on the topology recognition task. Thus, the 3D visualizations did not give a false sense of confidence with respect to topology recognition.

Awareness of adversarial behavior is suggested to be necessary for achieving CSA for cyber defense decision-making (Barford et al., 2009) although non-technical stakeholders may underestimate the importance of such information (Varga et al., 2018). This may have severe consequences for decision-making if analyst-level personnel and decision-makers have different mental models of the CTS and the network, especially if analyst-level personnel are not aware of this discrepancy during RCP communication (Ask et al., 2021a). Because the VDE allows for visualizing, thus sharing the mental models that the analyst have of the network topology (Kullman et al., 2018, 2020), this potential gap in information requirements (Varga et al., 2018) may be bridged more efficiently if adversarial behavior can be visualized during RCP sharing. While non-technical personnel were not included in the present study, the VDE group outperformed the Arkime group on all metrics when they were tasked to identify the top five Red Team hosts targeting Blue Team systems. This was true for correctly identifying Red Team hosts targeting Blue Team systems, but especially apparent for the traffic associated with the identified Red Team hosts where the differences in the session number associated with the identified connections differed in the tens of thousands. Moreover, the VDE group identified the connection with the highest amount of associated traffic while the Arkime group did not. Considering that the Arkime group could see the session number associated with the connections when hovering over the edge connecting the nodes while the VDE group had to go by edge brightness alone, this difference in performance is arguably the most salient of the experimental results.

Considering the role of working memory in SA (Gutzwiller and Clegg, 2013), it could be that using edge brightness as a cue for traffic provided an advantage over having access to actual session statistics due to complexity reduction freeing up cognitive resources. Albeit being allowed to write down their discoveries (e.g., host IP, session number), having the actual statistics available may result in deliberately or habitually engaging in analytical procedures that require the application of additional cognitive processes. This may include processes that tax attention allocation and working memory which could be detrimental to performance in a working environment that is already taxing on cognitive resources (Champion et al., 2012;

Sawyer and Hancock, 2018). Alternatively, or additionally, it could be that having the network topology fixed in space and at a scale where participants could walk from node to node, facilitated a method of loci/memory palace-effect (Legge et al., 2012; Wagner et al., 2021), due to the spatial encoding of information (Stackman et al., 2002; Angelaki and Cullen, 2008; Moser et al., 2008). By using edge brightness as the singular attentional cue combined with a spatial layout, the VDE may have improved performance by allowing for increased ease of visuo-cognitive processing of the state of the network. But what if participants were tasked to find the bottom five Red Team hosts (e.g., rare or ambiguous signals) targeting Blue Team systems (with session number above zero)? For instance, would edge brightness then be distracting, or would the differences in performance remain? This question should be addressed in future studies.

Interestingly, and without knowing that they had outperformed participants in the Arkime group, some of the participants in the VDE condition expressed that they would have liked to have session number available for inquiry. This may further suggest that taxing habitual or procedural (e.g., trained) cognitive processes could have contributed to performance differences between the groups. In a realistic scenario, however, the VDE would not be used to replace packet capture software or any investigative tools. Instead, the SOC analysts would have all their usual tools available to them, while the VDE would be an additional tool that analysts could use to interact with network data according to their information processing needs (Kullman and Engel, 2022a,b). If analysts would prefer to inquire about session statistics, they could either probe for that through common means or incorporate it in VDE. This, in turn, serves to deepen their understanding of the cyber environment they are operating within on their own terms, either for themselves or when communicating with team analysts, decision-makers, or stakeholders (Kullman et al., 2019a).

Awareness of the impact of an attack is also suggested to be necessary for achieving CSA for good cyber defense decision-making (Barford et al., 2009). In the present study, the VDE group identified more Blue Team segments that were compromised by the Red Team than the Arkime group. Given the level of uncertainty that is inherent to the cyber domain (Jøsok et al., 2016), this difference in impact awareness may be advantageous when attempting to reduce the level of experienced uncertainty both when attempting to understand the situation but also perhaps when evaluating the trustworthiness of CSA information, especially for non-technical

personnel. The latter is also suggested to be important for achieving CSA for cyber defense decision-making (Barford et al., 2009).

To assess the potential effect of VDE on RCP communication, we asked participants to provide a short situational report based on three open-ended questions which were later used to generate three scores based on accuracy and relevance. In line with Barford et al. (2009), the questions were aimed at measuring (a) awareness of the current situation by describing the activity they saw, (b) what caused it by describing what type of incident it was, and (c) how the situation may evolve by suggesting which actions should be taken. A k-score was generated based on the overall thoroughness of the situational report. Although the VDE group scored higher than the Arkime group on all four measures, only the activity description score was significantly different between the groups.

In the present study, the VDE group identified more Blue Team hosts that were abused for Red Team lateral movements. However, this was not significantly different between the groups (although the number of correctly identified abused Blue Team hosts approached significance). Considering the difference in performance on task two, the lack of difference in performance on task three could be due to the time limit that the participants had to work under. It could also be due to the limited sample size. This will have to be addressed in future studies.

During the second part of the experiment, the VDE group was more confident in their answers than the Arkime group on all CSA measures. This should be considered in light of the fact that the VDE group performed significantly better than the Arkime group on several of the performance outcomes while having higher scores on all performance outcomes (although not all were significantly different). The outcome measures for the fourth CSA question (the question relating to task three) was the only measure where not one of the scores were significantly different between the groups. When also considering the lower confidence scores when the VDE group actually performed worse than the Arkime group, it could indicate that these performance estimations are well-founded. A second interpretation could be that the cyber cadets have good metacognitive accuracy irrespective of the conditions they were assigned to. Previous studies on cyber cadets have indicated that they are similar in their cognitive profiles (Lugo and Sütterlin, 2018), and that cyber cadets with higher metacognitive accuracy have better CSA, while overconfident cyber cadets have worse CSA (Ask et al., 2023). Assessing the metacognitive accuracy of the participants with respect to performance

outcomes will be addressed in the study examining the cognitive measures that were taken during the experiment.

It is important to restate here that the VDE is not a tool for conducting forensic analyses per se. It is a neuroergonomic tool for visualizing network topology in accordance with the analyst's mental model of the network (Kullman and Engel, 2022a,b). This allows the analyst to not have to spend working memory on mentally maintaining or navigating the representation of their mental models when they are seeking to understand a CTS. Because individuals collaborating in VDE will have the same spatial mental model of the network (Kullman and Engel, 2022a,b), less mental effort may be required to ground communication, thus making knowledge transfer more efficient. While the experimental tasks and preliminary nature of the present study does not capture traditional SOC activities with sufficient realism, it still goes some way in capturing how the VDE influences communication processes when individuals are collaborating to establish CSA.

During the second part of the experiment, participants in the VDE condition experienced a lower communication demand compared to participants in the Arkime condition, suggesting that the VDE improves communication efficiency. Thus, when considering that communication inefficiencies are one of the biggest but least researched problems facing SOC team analysts (Agyepong et al., 2019; Ask et al., 2021a), this finding may indicate that the VDE could aid in solving some of those communication problems.

Previous studies have indicated that task-related communication is different between poor and well performing cyber teams during CDXs (Jariwala et al., 2012; Ask et al., 2023) but that expert cyber analysts communicate less than novice cyber analysts (Buchler et al., 2016; Lugo et al., 2017). This could indicate that experts communicate more effectively (e.g., are better at OLB processes; Knox et al., 2018) and more readily achieve a shared mental model of the tasks they are solving and of the cyber threat situation (Ask et al., 2023). A recent review found that there was a lack of studies characterizing the communication in cyber defense settings such as the purpose of communication and the type of communication (Ask et al., 2021a). In the present study, we noted the frequency of dyadic verbal communication as they related to OLB processes, task resolution, achieving a shared perceptual mental model, and communication dysfunction. We found that the VDE group performed significantly more OLB communication (which are aimed at achieving a shared understanding of a situation; Knox et al., 2018) during task one and task two, while the Arkime group performed significantly more task resolution

communications and had more communication dysfunctions during task two. In our regression analysis, both observed and self-reported communication variables that were scored higher in the Arkime group compared to the VDE group were negative predictors of CSA scores. This could indicate that the VDE facilitates more efficient cyber team communication and should be assessed further in future studies. The possibility for using VDE in remote dyadic cooperation should also be assessed in future studies to assess whether these potential effects are present when body language cues are not available to the participants.

In the present study, almost all participants picked the same decision regardless of assigned condition or individual performance. This is likely due to cohort effects such as training but could also potentially be due to the specific cognitive profiles that the cyber engineering profession selects for Lugo and Sütterlin (2018). This could explain why the relevance score for the actions suggested in the situation report were not different between the groups. Future studies should include a more diverse sample to avoid potential confounding influences on the effect of VDE on decision-making. Because the VDE visualizations are established through an interview with the user of the visualizations (the analysts; Kullman et al., 2018, 2020), the 3D layout of the network topology in VDE is generated through usercentric cooperative-design principles. Due to the participants not being familiar with the network they were working with in the current experiment, the 3D layout was predefined. Usually, a cyber analyst will know the network they are operating within, thus, there is always a possibility that the unfamiliarity of the network made participants choose “safer” and similar decision-making options.

4.1. Limitations and future perspectives

The present study has a few limitations. The VDE group had higher scores on all performance measures and lower scores on all team workload measures during the second part of the experiment, although not all of these were significantly different. It is hard to say whether differences would have reached significance with a larger sample size. Considering this possibility, the experiment should be repeated in a larger sample.

With most behavioral experiments, there is a question of whether the experimental design produces results that can be generalized to a real-world setting. Due to being high stakes and unfolding in a complex working environment, defensive cyber operations can be stressful and often entail being exposed to a number of distractors (e.g., security alerts that are false positives) that may degrade performance over time (Champion et al., 2012; Sawyer and

Hancock, 2018). Future studies should therefore include more distractors to ensure that results have high ecological value. This could include explicating time limits on all tasks, or exposing participants to periodic security alerts and increasing indicators of compromise (scenario injections). This in turn would allow the assessment of how taxing different senses and cognitive systems affect VDE vs. Arkime usability for CSA generation, team communication, and decision-making. Furthermore, applying the VDE in a setting that captures SOC tasks with more realism, including analyst-to-decisionmaker communication will be necessary to fully validate the potential usability of the VDE for achieving a shared CSA.

While the overall performance of the HoloLens 2 was good, there were some instances where the HoloLens 2 headsets overheated which negatively affected application's stability and forced a few minute-long breaks while the headset was being replaced. Wearing a battery pack that provided the HoloLens 2 device with additional power appeared to solve the problem but the form factor of the battery pack and absence of dedicated gear (the participants kept the battery in their pocket) made it a somewhat awkward experience. This should be addressed in future research to ensure a more seamless experience that works under various conditions.

5. Conclusions

In the present study, a collaborative, 3D mixed reality representation of a network topology and network attack provided better CSA compared to using paper-based, 2D topology schematics and graph representation in the packet capture software Arkime.

The most apparent difference was in the detection of the top five Red Team hosts targeting Blue Team systems. The traffic associated with the identified Red Team hosts in the mixed reality condition differed in the tens of thousands. This is remarkable, as participants in the mixed reality condition could only use edge brightness as a cue for traffic while participants in the Arkime condition could see the actual session number statistics. Observed and self-reported communication was better for dyads in the VDE condition and was associated with their CSA. This may suggest that the VDE has neuroergonomic benefits when SOC team analysts need to communicate for shared CSA. Although participants in the mixed reality condition had higher CSA, we were not able to measure its effect on decision-making. This could be due to cohort effects such as training or the modest sample size. Finally, the experimental tasks and preliminary nature of the study does not reflect SOC tasks with sufficient realism. Thus, to

truly assess the potential effects of VDE on communication for shared CSA, the study should be repeated in a naturalistic setting with a larger and more diverse sample.

Data availability statement

The datasets presented in this article are not readily available because access to raw and processed data is restricted in accordance with agreement between the researchers and the Norwegian Defense University College, Cyber Academy (NDCA).

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. The patients/participants provided their written informed consent to participate in this study.

Author contributions

TA: experimental design, data collection, statistical analysis, and writing the original draft, review, and editing. KK: development of the data visualization application, experimental design, and writing, review, and editing of the original draft. SS: experimental design, review, and editing of original draft. BK: experimental design, data collection, review, and editing of original draft. DE: writing, review, and editing. RL: experimental design, data collection, statistical analysis, and writing, review, and editing of original draft. All authors approved the final draft of the manuscript.

Funding

This study was funded by the Norwegian Research Council (project #302941). Development of the Virtual Data Explorer was partly supported by the Army Research Laboratory under Cooperative Agreement No. W911NF-17-2-0083 and in conjunction with the CCDC Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center. Development of the Virtual Data Explorer is partly supported by NASA under Award No. 80GSFC21M0002.

Acknowledgments

A huge thank you to the Norwegian Defense Cyber Academy for help with facilitating the experiment and to the NATO CCDCOE for giving us access to the Locked Shields 2022 network data. A preprint of this manuscript is available via PsyArXiv (Ask et al., 2022).

Conflict of interest

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

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: a systematic review. J. Cyber Security Technol. 4, 125–152. doi: 10.1080/23742917.2019.1698178

Ahrend, J. M., Jirotka, M., and Jones, K. (2016). "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge," in 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). (London, UK). doi: 10.1109/CyberSA.2016.7503279

Angelaki, D. E., and Cullen, K. E. (2008). Vestibular system: the many facets of a multimodal sense. Ann. Rev Neurosci. 31, 125–150. doi: 10.1146/annurev.neuro.31.060407.125555

Ask, T. F., Knox, B. J., Lugo, R. G., Helgetun, I., and Sütterlin, S. (2023). Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. Front. Human Neurosci. 16, 1092056. doi: 10.3389/fnhum.2022.1092056

Ask, T. F., Kullman, K., Sütterlin, S., Knox, B. J., Engel, D., and Lugo, R. G. (2022). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. PsyArXiv [Preprint]. doi: 10.31234/osf.io/sphgn

Ask, T. F., Lugo, R. G., Knox, B. J., and Sütterlin, S. (2021a). "Humanhuman communication in cyber threat situations: a systematic review," in HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021, ed C. Stephanidis (Cham: Springer), 21–43. doi: 10.1007/978-3-030-903 28-2_2

Ask, T. F., Sütterlin, S., Knox, B. J., and Lugo, R. G. (2021b). "Situational states influence on team workload demands in cyber defense exercise," in HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021, ed C. Stephanidis (Cham: Springer), 3–20. doi: 10.1007/978-3-030-903 28-2_1

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., et al. (2009). "Cyber SA: situational awareness for cyber defense," in Cyber Situational Awareness Advances in Information Security, eds S. Jajodia, P. Liu, V. Swarup and C.Wang (Cham: Springer) 3–13. doi: 10.1007/978-1-4419-0140-8_1

Berggaard, N., Bjerke, I., Paulsen, A. E. B., et al. (2018). Development of parvalbuminexpressing basket terminals in layer II of the rat medial entorhinal cortex. eNeuro 5, e0438. doi: 10.1523/ENEURO.0438-17.2018

Bohbot, V. D., Copara, M. S., Gotman, J., and Ekstrom, A. D. (2017). Low-frequency theta oscillations in the human hippocampus during real-world and virtual navigation. Nat. Commun. 8, 14415. doi: 10.1038/ncomms14415

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

Champion, M. A., Rajivan, P., Cooke, N. J., and Jariwala, S. (2012). "Team-based cyber defense analysis," in 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in situation Awareness and Decision Support (New Orleans, LA. USA), 218–221. doi: 10.1109/CogSIMA.2012.6188386

Cicchetti, D. V. (1994). Guidelines, criteria, and rules of thumb for evaluating normed and standardized assessment instruments in psychology. Psychol. Assess. 6, 284–290. doi: 10.1037/1040-3590.6.4.284

Eichenbaum, H. (2014). Time cells in the hippocampus: a new dimension for mapping memories. Nat. Rev. Neurosci. 15, 732–744. doi: 10.1038/nrn3827

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society 32nd Annual Meeting (Santa Monica, CA) 97–101. doi: 10.1177/154193128803200221

Endsley, M. R. (1995). Toward a theory of Situation Awareness in dynamic systems. J. Hum. Factors Ergon. Soc. 37, 32–64. doi: 10.1518/001872095779049543

Endsley, M. R. (2020). The divergence of objective and subjective situation awareness: a meta- analysis. J. Cogn. Eng. Decis. Mak. 14, 34–53. doi: 10.1177/1555343419874248

Franke, U., and Brynielsson, J. (2014). Cyber situational awareness - a systematic review of the literature. Comput. Security 46, 18–31. doi: 10.1016/j.cose.2014.06.008

Gutzwiller, R. S., and Clegg, B. A. (2013). The role of working memory in levels of situation awareness. J. Cogn. Eng. Decis. Mak. 7, 141–154. doi: 10.1177/1555343412451749

Hallgren, K. A. (2012). Computing inter-rater reliability for observational data: An overview and tutorial. Tutor. Quant Methods Psychol. 8, 23–34. doi: 10.20982/tqmp.08.1.p023

Jariwala, S., Champion, M., Rajivan, P., and Cooke, N. J. (2012). Influence of Team Communication and Coordination on the Performance of Teams at the iCTF Competition. Proc. Human Factors Ergon. Soc. Ann. Meet. 56, 458–462. doi: 10.1177/1071181312561044

JASP Team (2021). JASP (Version 0.15) [Computer software].

Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., and andWard, P. (2016). "Exploring the hybrid space," in Augmented Cognition 2016. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence), eds D. D. D. Schmorrow and C. M. M. Fidopiastis (Cham: Springer), 9744, 178–188. doi: 10.1007/978-3-319-39952-2_18

Jøsok, Ø., Knox, B. J., Helkala, K., Wilson, K., Sütterlin, S., Lugo, R. G., et al. (2017). Macrocognition applied to the Hybrid Space: Team environment, functions and processes in Cyber Operations. in International Conference on Augmented Cognition (Cham: Springer), 486–500. doi: 10.1007/978-3-319-58625-0_35

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., and Helkala, K. (2019). Selfregulation and cognitive agility in cyber operations. Front. Psychol. 10, 875. doi: 10.3389/fpsyg.2019.00875

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

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

Kuhrt, D., St. John, N. R., Bellmund, J. L. S., Kaplan, R., and Doeller, C. F. (2021). An immersive first-person navigation task for abstract knowledge acquisition. Sci. Rep. 11, 5612. doi: 10.1038/s41598-021-84599-7

Kullman, K., Asher, N. B., and Sample, C. (2019b). "Operator impressions of 3D visualizations for cybersecurity analysts," in Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal, ed. Cruz, Tiago; Simoe, Paulo. (Reading, UK: ACPI) 257–266.

Kullman, K., Buchanan, L., Komlodi, A., and Engel, D. (2020). "Mental model mapping method for cybersecurity," in HCI for Cybersecurity, Privacy and Trust. HCII 2020, eds. A. Moallem (Cham, Springer). doi: 10.1007/978-3-030-50309-3_30

Kullman, K., Cowley, J. A., and Ben-Asher, N. (2018). "Enhancing cyber defense situational awareness using 3D visualizations," in Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018: National Defense University, Washington DC, USA (Washington DC: Academic Conferences and Publishing International Limited) 369–378.

Kullman, K., and Engel, D. (2022a). "User interactions in virtual data explorer," in Augmented Cognition. HCII 2022, eds. D.D. Schmorrow, C.M. Fidopiastis (Cham: Springer) 13310. doi: 10.1007/978-3-031-05457-0_26

Kullman, K., and Engel, D. (2022b). Interactive stereoscopically perceivable multidimensional data visualizations for cybersecurity. J. Defence Secur. Technol. 4, 37–52. doi: 10.46713/jdst.004.03

Kullman, K., Ryan, M., and Trossbach, L. (2019a). VR/MR supporting the future of defensive cyber operations. IFAC-PapersOnLine 52, 181–186. doi: 10.1016/j.ifacol.2019.12.093

Lankton, P. (2007). Endsley's model of situational awareness [jpg]. Available online at: https://en.wikipedia.org/wiki/File:Endsley-SA-model.jpg (accessed September 13, 2022).

Legge, E. L., Madan, C. R., Ng, E. T., and Caplan, J. B. (2012). Building a memory palace in minutes: equivalent memory performance using virtual versus conventional environments with the Method of Loci. Acta Psychol. 141, 380–390. doi: 10.1016/j.actpsy.2012.09.002

Lif, P., Granasen, M., and Sommestad, T. (2017). "Development and validation of technique to measure cyber situation awareness," in 2017 International Conference on Cyber Situational Awareness, Data Aanalytics and Assessment (Cyber SA), (London, UK). doi: 10.1109/CyberSA.2017.8073388

Lugo, R., Kwei-Nahr, P., Jøsok, Ø., Knox, B. J., Helkala, K., and Sütterlin, S. (2017). "Team workload demands influence on cyber detection performance," in 13th International Conference on Naturalistic Decision Making (Bath, UK) 223–225.

Lugo, R. G., and Sütterlin, S. (2018). Cyber officer profiles and performance factors. International Conference on Engineering Psychology and Cognitive Ergonomics (Cham: Springer). 181–190. doi: 10.1007/978-3-319-91122-9_16

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. J. Mil. Stud. 7, 44–52. doi: 10.1515/jms-2016-0005

Moser, E. I., Kropff, E., and Moser, M. B. (2008). Place cells, grid cells, and the brain's spatial representation system. Ann. Rev Neurosci. 31, 69–89. doi: 10.1146/annurev.neuro.31.061307.090723

NATO Cooperative Cyber Defense Center of Excellence (2016). NATO Recognizes cyberspace as a 'domain of operations' at the Warsaw summit. Available online at: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html (accessed September 13, 2022).

Ray, S., and Brecht, M. (2016). Structural development and dorsoventral maturation of the medial entorhinal cortex. eLife 5, e13343. doi: 10.7554/eLife.13343.019

Safaryan, K., and Mehta, M. R. (2021). Enhanced hippocampal theta rhythmicity and emergence of eta oscillation in virtual reality. Nat. Neurosci. 24, 1065–1070. doi: 10.1038/s41593-021-00871-z

Sawyer, B. D., and Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. Human Factors. 60, 597–609. doi: 10.1177/0018720818780472

Seager, M. A., Johnson, L. D., Chabot, E. S., Asaka, Y., and Berry, S. D. (2002). Oscillatory brain states and learning: Impact of hippocampal theta-contingent training. Proc. Nat. Acad. Sci USA. 99, 1616–1620. doi: 10.1073/pnas.032662099

Sellers, J., Helton, W. S., Näswall, K., Funke, G. J., and Knott, B. A. (2014). Development of the team workload questionnaire (TWLQ). Proc. Hum. Factors Ergon. Soc. Annu. Meet. 58, 989–993. doi: 10.1177/1541931214581207

Shrout, P. E., and Fleiss, J. L. (1979). Intraclass correlations: Uses in assessing rater reliability. Psychol. Bull. 86, 420–428. doi: 10.1037/0033-2909.86.2.420

Stackman, R. W., Clark, A. S., and Taube, J. S. (2002). Hippocampal spatial representations require vestibular input. Hippocampus 12, 291–303. doi: 10.1002/hipo.1112

Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., et al. (2016). "Collaborative data analysis and discovery for cyber security," in SOUPS 2016: Twelfth Symposium on Usable Privacy and Security (Denver, CO).

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., et al. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Secur. Privacy 13, 20–29. doi: 10.1109/MSP.2015.71

Sütterlin, S., Lugo, R., Ask, T., Veng, K., Eck, J., Fritschi, J., et al. (2022). "The role of IT background for metacognitive accuracy, confidence and overestimation of deep fake recognition skills," in Augmented Cognition. HCII 2022. Lecture Notes in Computer Science, eds D. D. Schmorrow and C. M. Fidopiastis (Cham: Springer) 13310, 103–119. doi: 10.1007/978-3-031-05457-0_9

Tcha-Tokey, K., Christmann, O., Loup-Escande, E., and Richir, S. (2016). Proposition and validation of a questionnaire to measure the user experience in immersive virtual environments. Int. J. Virtual Real. 16, 33–48. doi: 10.20870/IJVR.2016.16.1.2880

Varga, S., Brynielsson, J., and Franke, U. (2018). "Information Requirements for National Level Cyber Situational Awareness," in 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (Barcelona, Spain) 774-781. doi: 10.1109/ASONAM.2018.8508410

Wagner, I. C., Konrad, B. N., Schuster, P., Weisig, S., Repantis, D., Ohla, K., et al. (2021). Durable memories and efficient neural coding through mnemonic training using the method of loci. Sci. Adv. 7, eabc7606. doi: 10.1126/sciadv.abc7606

Winson, J. (1978). Loss of hippocampal theta rhythm results in spatial memory deficit in the rat. Science 201, 160–163. doi: 10.1126/science.663646

Chapter 6

6 Critical Discussion

The aim of the research reported in Chapter 5 was to apply neuroergonomics to understand and improve human-to-human communication in recognized cyber threat situations. Specifically, the thesis aimed to identify performance indicators and interventions in the context of cyber teams operating in complex information environments. This chapter includes a critical discussion of the work presented in this thesis. It focuses on some critical points and shortcomings and concludes with suggestions for future work. While the importance of transparency with respect to study limitations is self-evident, the main purpose of this critical discussion is to highlight some of the implications that result from the main challenge for conducting high-quality human factors research, which is the role that of relevant stakeholders (e.g., CDX organizers) have in helping researchers gain access to 1) relevant participants, and 2) to facilitate researcher involvement in the planning stages of CDXs to ensure that relevant and quality measurements can be employed. The following chapter (Chapter 7) will summarize the contribution of the thesis, putting it into the larger perspective of the aims of the project and the field of research on human factors in cybersecurity.

6.1. Limitations

The work presented in this thesis is of a preliminary nature and has a few but major limitations that makes it challenging to draw any conclusions about the significance of the findings outside the context of the studies and the cohorts participating in them.

6.1.1 Sample size and study population

The primary research articles included in chapter 5.2 and 5.3 had small sample sizes ($N = 32$ after exclusion if missing cases, and $N = 22$, respectively). With small sample sizes, one can only detect large effects, thus any false positive (Type I error) will have a large effect size, which may lead to exaggerated confidence in the significant relationships (Button et al., 2013). For instance, in simulated analyses, when sampling two uncorrelated variables with $N = 15$ and $N = 100$, the effect size of false positive correlations fall in the range of 0.5-0.75 and 0.2-0.25, respectively (Makin & Orban de Xivry, 2019). Studies with $N \approx 20$ are worthless at estimating effect sizes (Brysbaert, 2019). It is also necessary to mention that assumptions of normality are

hard to test rigorously in small samples, meaning that statistical tests showing no violations may not be accurate (Ghasemi & Zahediasl, 2012).

Another point to mention is that with alpha = 0.05, 5% of all tests will yield a significant result in absence of a true effect. This means that the higher the number of tests, the more likely it is to detect false positive correlations (e.g., increased risk of family-wise errors). This is commonly countered by adjusting for multiple comparisons; however, this is problematic in small samples (Vickerstaff et al., 2019). Small sample sizes increase the likelihood of not detecting true effects (Type II error) and adjusting for multiple comparisons reduces statistical power considerably thus increasing the likelihood of Type II errors (Vickerstaff et al., 2019). This problem is more severe in small samples when considering the fact that the median-split analysis in chapter 5.2 also reduces statistical power (DeCoster et al., 2011).

In addition to consisting of small sample sizes, the primary research included in this work was solely based on cyber cadets at the NDCA. Although they were at the end of their education, they are considered novices. While they may have unique profiles that could be indicative of trait-level cognitive and emotional processing tendencies (Lugo & Sütterlin, 2018; Lugo et al., 2019), in other words, profiles that will remain with them as they progress through their careers, it is still difficult to generalize the findings in chapter 5.2 and 5.3 to the wider populations of professionals and experts, even if the statistical issues were not present.

To deal with the challenges outlined above, replication of results in larger samples is needed to verify the results presented in 5.2 and 5.3. This requires some specific considerations given the nature of the population of interest. According to the 2023 ISC2 Global Workforce Study, the estimated global cybersecurity workforce in 2023 was 5,5 million (ISC2, 2023). Let us assume that the job market is saturated (contrary to the fact that the workforce is growing; ISC2, 2023), and that the entire global cybersecurity workforce are analysts. Let us assume that the findings in (Lugo & Sütterlin, 2018; Lugo et al., 2019) are true, that cyber analysts in general (but Norwegian cyber cadets (novices) specifically, as they make up the samples) are different from the normal population on cognitive and emotional measures, thus constituting a unique population. Getting individuals working in cybersecurity to volunteer for research, who work twelve-hour shifts and whose jobs it is to be suspicious about giving away information (including about themselves as it can be used for social engineering), is challenging. Being a potentially unique (Lugo & Sütterlin, 2018; Lugo et al., 2019), relatively rare (ISC2, 2023), and hard-to-access population, it requires extra efforts to establish replication within and

between cases, and to include sufficient controls (as the efforts in Lugo & Sütterlin, 2018; Lugo et al., 2019) to establish confidence intervals (Makin & Orban de Xivry, 2019).

6.1.2 Concurrent validity and construct validity

Concurrent validity and construct validity are important issues in cybersecurity research that are worthy of addressing properly, especially in the context of the work presented in this thesis. Due to being a complex field with very little knowledge about relevant cognitive human factors (Gutzwiller et al., 2015; Lugo & Sütterlin, 2018), and due to lacking reliable performance metrics for SOC team analysts (Agyepong et al., 2019; Gutzwiller et al., 2020), there is a need for developing (neuro-)cognitive performance metrics. While there certainly are many neurocognitive constructs that could be indicators of performance, one of the main challenges of transferring the assessment of these constructs from a lab setting to a naturalistic setting is the identification of valid ways of measuring the constructs that also are relevant for performance in a complex and dynamic environment. In a lab setting, neurocognitive constructs are studied in isolation by eliminating or controlling for factors that can influence them with respect to the relationships that researchers wish to assess. In an applied setting, the ideal is to find constructs that are performance indicators, meaning that their influence on specific outcomes should persist under the influence of additional, uncontrollable factors in the testing environment. This implies cycles of trial and error that are inherent to the scientific process but may be difficult to go through in settings with sufficient realism. For instance, CDXs are very expensive, they often require months of planning, and their main purpose is to provide participants with tasks and environments that represent realistic settings and scenarios. Participating in such exercises should lead to the development of skills that allow for the detection and mitigation of security threats as they occur in the real world. National security may be at stake. The ability for scientists to conduct useful research in such settings requires both willingness and most importantly the capacity for collaboration on the side of the organizers. Privacy and security concerns aside, the main issues organizers face in collaboration with researchers are:

- Allocating time to involve them in the planning phases of the exercise to help identify measurements that fit the specific setting and scenario, and to iron out the logistics of when and how to conduct measurements,
- Allocating time and facilities for measurements prior to, during, and after the exercise for baseline and outcome measurements, and

- Not interfering too much with the learning and performance of the participants to ensure that the resources that went into the exercise were well spent.

The logistics and purpose of CDXs may make it difficult for organizers to approve of true experimentation if the result of manipulation is negatively affecting the performance and learning outcomes of some of the participants. Furthermore, measurements conducted during the exercise take time away from participants being engaged in the exercise by introducing extra tasks (e.g., filling out a form) that they may find frustrating or unnecessary. This may especially be the case if it is not completely obvious how measurements relate to the problems they are solving as part of the exercise. Questionnaires measuring moods or cognitive tests may be examples of measurements that do not seem that relevant at the moment (even questionnaires measuring cyber SA; Lif et al., 2018, 2020). While participants are informed about the relevance of the measurements and when they will be conducted when being recruited to the study, their attitude towards the measurements may shift when they are under stress. Conducting self-report measurements at the end of a long day of intensive analytical work may affect how much effort participants put in their responses. Thus, the risk for response fatigue needs careful consideration. Dealing with these issues on the side of the researcher necessitates some level of ingenuity with respect to how constructs are measured. The need for measurements to fit the context of the exercise and to be executed within time constraints means developing or adapting measurements during planning phases of the exercise. Because CDXs are conducted on set dates and measurements are developed leading up to them, properly validating the selected novel indicators (beyond the predictive validity demonstrated through hypothesis testing) ultimately becomes a post facto endeavor.

While the research included in this work relies on tests and inventories where reliability and validity have been established, this work also includes measurements that were either developed for the specific study or recently proposed. Thus, their validity is currently being investigated and is therefore not well-established. Measurements that are not well-established are the measurements of prospective metacognitive awareness in paper II, measurements of cyber SA in paper II and III, and the structured observation of communication behaviors in paper III. The concurrent and construct validity of these measurements should therefore not be taken for granted.

The formula used to quantify metacognition in paper II produces the deviation between expected performance (rated from 0 to 100%) and percentage of correct answers. Because the

combined score on the four SA variables that were either correct (1) or incorrect (0) are converted to a scale ranging from 0 to 100, it results in the possible values being 0, 25, 50, 75, and 100. While these steps are explained in the paper, the variable may be interpreted as being a more fine-grained measure than it actually is if these steps are not read.

The questionnaire used to assess cyber SA in cyber cadets during NDCA's annual cyber engineering exercise in paper III was the one proposed by Lif and colleagues (2017). It is still undergoing validation and amendments; the average ratings of perceived relevance of the questions according to participants have been slightly above medium (Lif et al., 2018, 2020). To address relevance, we asked one of the organizers of the cyber engineering exercise whether the cyber SA questionnaire would be relevant and also had them score the questionnaires after the exercise.

The measurements of cyber SA in paper III were developed to fit the specific tasks in the experiment. The measurements were partly inspired by the cyber SA questionnaire by Lif and colleagues (2017), partly inspired by a situational report structure developed for CDXs by one of the co-authors on the paper, and some questions that asked about specific activities in the network.

To the extent that there are disagreements in the literature with respect to what SA entails in teams and how to measure it (Salmon et al., 2008) and the consequences this has for cyber SA, a developing concept which currently has no reliable measures (Gutzwiller et al., 2016, 2020; Ofte & Katsikas, 2023), one would be intellectually dishonest if not questioning the validity of the construct.

The structured observation method in paper III was developed for the experiment based on the papers reviewed in chapter 5.3 and assessed the frequency of occurrence for four verbal communication behaviors: (1) OLB behaviors, (2) perceptual shared mental modeling, (3) task resolution, and (4) communication dysfunction. What was identified as OLB behaviors and why they were important was based on the OLB model proposed by Knox and colleagues (2018) and is thought to reflect metacognition and perspective taking. Perceptual shared mental modeling consists of verbal communication related to achieving a shared visual and spatial perception of task relevant information but was mainly assessed through communication behaviors facilitating joint attention. Task resolution communication was identified as important based on observations from a qualitative study (Jariwala et al., 2012).

Communication dysfunction behaviors identified as important were based on reports from (Champion et al., 2012; Henshel et al., 2016; Jariwala et al., 2012). One of the dysfunctional behaviors was prolonged silence (considered an indication of communication breakdown; Champion et al., 2012; Jariwala et al., 2012) which may not be dysfunctional with respect to building SA and may even be a sign of expertise (Buchler et al., 2016).

Vagal tone is influenced by a myriad of physiological and behavioral processes and changes throughout the day (Tiwari et al., 2021) and is also susceptible to noise (Rohr et al., 2024). A meta-analysis on the relationship between heart rate variability and self-regulation reported conflicting and weak or negligible associations that were independent of the self-regulatory domain assessed (Zahn et al., 2016). The study has some methodical limitations. Keywords specifically pertaining to vagal tone were not included in the study's search strategy (Laborde & Mosley, 2016; Zahn et al., 2016), and the grouping of cognitions was too broad, a limitation that is addressed by the authors (Zahn et al., 2016). While more recent meta-analyses (Magnon et al., 2022; Schmaußer et al., 2022) seem to go against the findings in (Zahn et al., 2016), it is still worth mentioning that there is conflicting meta-analytic evidence regarding the validity of vagal tone as a marker of cognitive functioning. If vagal tone is downstream of the dorsolateral prefrontal cortex activity (Schmaußer et al., 2022) involved in processes underlying self-regulated contextual adaptation, then transcranial stimulation of dorsolateral prefrontal cortex should improve self-regulated behavior. The findings from studies on this are very variable and highlight the contribution of factors such as heterogeneity in experimental paradigms, regulatory domain, and study quality, that the effect of stimulation depends on ongoing neural activity, and the influence of duration and dosage of stimulation (Kelley et al., 2019). This latter point also appears to translate to links between dorsolateral prefrontal cortex and vagal tone, as a recent study suggested that the relationship between transcranial stimulation over dorsolateral prefrontal cortex and vagal tone may be dependent on dose (Razza et al., 2024). In sum, while vagal tone may be influenced by dorsolateral prefrontal cortex activity (Schmaußer et al., 2022), there is still room for questioning what this means with respect to cognition and self-regulated behaviors.

Despite the challenges related to the sample size and construct and concurrent validity, the work presented in this thesis demonstrates the feasibility of applying neuroergonomic approaches to study and improve communication in cyber threat situations. Generating 3D representations of network topology and traffic during simulated cyber threats is a particularly

promising approach that warrants further investigation also with respect to assessing the impact it has on mental load. Overcoming the challenges discussed in chapter 6.5 will be a crucial next step.

6.2. Future perspectives

Replication is needed to validate the results included in this thesis. More work is needed to determine the significance of the findings with respect to actual performance in cybersecurity settings as it is unclear what the relationship between communication, cyber SA, and decision-making is. There are several study designs that would be interesting to further determine the significance of the findings. To the extent that vagal tone may be a performance indicator, it would be worthwhile to divide cyber operators in teams based on whether they have high or low vagal tone during a CDX. Then increase task complexity (e.g., increase the number of potential SA elements needed to evaluate or workload) in stages, for example for each day, then measure the relationship between vagal tone, communication and coordination demand, and metacognitive accuracy per stage of complexity to determine the degree that cognitive control and agility has with increased task complexity. It would be necessary to include decision-making outcomes as well to determine whether any potential relationships have an impact on decision-making.

As for the role of mood regulation and mood-congruent processing on performance, it would be interesting to assess the relationship between vagal tone and multiple cyber-relevant task outcomes where performance is related to emotional bias, meaning that there are several tasks where performance either favors or is not in favor of negativity bias, positivity bias, and neutral bias. It would be interesting to see if there is a tendency to regulate among individuals with high vagal tone, which may be detrimental to performance on tasks where emotional biases are beneficial but not when it is detrimental.

It would also be interesting to repeat the VDE versus 2D experiment with dyads where some dyads only have high vagal tone, high and low vagal tone, and only low vagal tone, to see if there are significant interaction effects between condition and vagal tone, or if VDE improves communication and cyber SA irrespective of vagal tone.

As for the VDE experiments, the experiments must be replicated with more realistic tasks, and include SIEMs in both conditions, perhaps by including the VDE as an extra tool during a CDX that can be used during collaboration or when briefing senior but non-technical

officers. It would also be interesting to compare stationary VDE using VR to ambulatory VDE using MR. Furthermore, in MR, when individuals are in the same room, dyads can read each other's body language while this is not possible in VR. It would thus be interesting to assess whether these different qualities have a meaningful impact on dyad performance. Another interesting phenomenon that would be worth exploring if the VDE is used during a CDX that spans multiple days is that of memory with respect to synaptic replay. During sleep, the brain replays neuronal activity coding for navigation (walking activity) at compressed speeds to facilitate memory consolidation (Girardeau & Zugaro, 2011; Whitlock & Moser, 2009). It would be interesting to see if ambulatory VDE exploration leads to better recall of cyber threat information compared to stationary use, both with stationary VDE and traditional 2D tools. It would also be interesting to see if dividing information load between different sensory modalities has an effect on mental load in groups using 3D visualizations compared to groups using 2D visualizations.

It is also necessary to validate our prospective metacognition measurements and to, for instance, account for the relationship between judgment hesitancy and need for evidence accumulation (Desender et al., 2022). Future work should investigate the relationship between metacognitive efficiency and effort adjustments during CDXs when/if figuring out that their initial projection was biased, and track changes in prospective and retrospective metacognitive judgements of performance and actual performance over the duration of the exercise. It would also be interesting to investigate further the association between mood and metacognition. For example, it may be worthwhile asking participants 1) to what extent they think their moods influence how they process information, and 2) if they think there are times at work when it is better to be in a positive mood than neutral or negative, negative is better than positive or neutral, and neutral is better than positive or negative.

Aside from the need for replication and operationalization of variables, there are some basic yet important questions that are currently unanswered that will need to be addressed to ensure that neurocognitive performance indicators are in fact of neuroergonomic value. Future studies should attempt to quantify information loss during dyadic communication of cyber threat information and its impact on SA and decision-making, assess the differences in effect of cumulative SA information versus abstraction/synthesis of SA information on decision-making, and quality versus quantity of SA information (as a follow-up on the findings of Buchler et al., 2016 with respect to communication and SA). It would also be valuable to assess

the effect that team members with good metacognitive abilities have on team members with poorer metacognitive abilities with respect to workload demands, and SA. It is worth investigating further the differences in analyst SA and what they share in reports based on how they understand the priorities and information needs of their superiors/decision-makers. There needs to be more research on expert cyber operators. Finally, the applicability (transferability) of findings from neuroscience research to a field where the people who are meant to benefit from it do not have backgrounds in biology needs to be ensured (Lund, 2022).

Chapter 7

7 Summary of contributions

This chapter summarizes the contributions of the work presented in this thesis. As stated previously, the research conducted as part of the thesis project has aimed to "solve specific and practical problems faced by individuals or groups" and identifies as belonging to the class of applied research. The specific problem was related to human-to-human communication in cyber threat situations, specifically in the context of cyber teams operating in complex information environments. To address this problem, the research has relied on a number of converging methods including systematic review, neurophysiological measurements by use of sensors, cyber defense exercises, laboratory studies, metacognitive and SA measurements, emotional self-report measurements, interventions using XR to visualize network topology and activity, structured observations of communication, and self-reported communication demands. In order to evaluate the extent to which the thesis research has managed to provide actionable results, contributions will be discussed in terms of their practical applicability and in order of descending novelty and significance. This discussion will be followed by key takeaways and some ethical reflections.

One of the main challenges to conducting research on operative cyber personnel, especially those tasked with analytical work, is the lack of established performance metrics (Agyepong et al., 2019). This makes it hard to evaluate the significance of research. Cognitive constructs related to flexible attentional control such as cognitive agility and metacognition have been proposed as performance indicators relevant for navigating and communicating in complex information environments (Jøsok et al., 2016, 2019; Knox et al., 2017, 2018), but the operationalizations have yet to be validated by having influence on performance related outcomes with direct relevance for cyber operations. The work presented in this thesis builds on these previous suggestions by conducting objective, neurophysiological measures related to flexible attentional control, behavioral measures of metacognitive abilities, self-reported emotional states, cutting-edge measurements of cyber SA, and self-reported team communication outcomes during a CDX. To this end, study II in this thesis includes one of the first works to apply sensors to cybersecurity teams during a CDX in an attempt to assess vmHRV as a neurophysiological indicator of flexible attentional control. The findings demonstrated the feasibility and relevance of including such measures in the context of a CDX,

which could indicate potential use cases for wearable sensor technologies in the assessment of cyber teams. Since wearable technologies are sufficiently mature, and as there already is a heavy investment of effort in applying such technologies in operative contexts, at least in military sectors (Hinde et al., 2021; Shi et al., 2022; Taylor et al., 2023, 2024), one should expect less friction against adoption at organizational levels, especially for measurements that have relevance for performance. The most notable findings were the associations between vmHRV measured at rest two days before the exercise commenced, and self-reported mood and metacognitive judgments during the exercise. Both of these outcome measures were related to measures of cyber SA and biases in the judgment of team performance. Thus, vmHRV is a plausible performance indicator that relates to how cyber teams navigate complex information, further indicated by individuals with lower vmHRV experiencing higher communication demands than individuals with high vmHRV. This latter finding should be interpreted with caution, however, the sum of the evidence in this study suggests that there is neuroergonomic support for a relationship between cognitive agility and metacognition, and that it is relevant for navigating cyber operative working-environments and SA building. In sum, wearable technology can readily be applied in CDXs to support cyber analyst training and performance monitoring, which is needed to further validate the significance of results.

The third study included in this thesis also offers novel and practical contributions. The study is one of the first works to apply XR in an experiment as means to improve complex information processing and team communication during a simulated cyber threat. It is also the very first study to use NATO CCDCOE Locked Shields network data in an experiment. While the sample sizes equate to a pilot study on the level of generalizing results, the study included most of the cohort in the studied population thus being of relevance to the that group of future national-level cybersecurity experts. A strength of the study was the inclusion of a head-to-head design where one of the leading softwares for treating and visualizing pcaps comprised the tools used by the control group. The results of the experiment suggested that using mixed reality to facilitate 3D visualizations of network topology and activity during a simulated network attack improved operational communication in dyadic cyber teams, and that this communication was related to dyadic collaborative performance with respect to making accurate red team-related discoveries in complex network data. With respect to the practical significance of these results, the MR technology has matured since the experiments (battery time has improved significantly) and the main challenge to implementing this in CDXs is the willingness and capacity of facilitators. You will run out of physical space before you run out

of number of headsets with synced visualizations. Of important note, the VDE platform (Kullman et al., 2018) and the 3D visualizations used in study III is not a tool for conducting forensic work or detecting threats. It is meant to visualize network data within a predefined window of time, which makes it suitable for use cases when one wish to understand the normal state of a network (for one's own sake or when training novices), develop a deeper understanding of network activity surrounding an already identified cyber-attack, or as a method for facilitating ease of collaboration and communication with respect to specific activity in a specific network. While the relevance of the intervention on decision-making could not be established, the implementation of the VDE as a supplement to collaborative practices in CDXs is promising.

The systematic review conducted in study I identified a number of strengths and gaps in the pre-existing research on human-to-human communication in cyber threat situations. The findings reported in this review is actionable to other researchers wanting to improve communication practices. To this end, findings in the research suggested that the underreporting of the sex of participants in studies made it hard to evaluate whether there are gender differences in the factors that influence communication-related performance. This finding was the basis for an independent study (Fisher, 2022) that used qualitative measures to investigate whether there were gender differences related to communication among Norwegian cyber cadets. The findings suggested that communication was influenced by perceived gender stereotypes. The review also identified studies providing qualitative reports of communication behaviors that could be relevant predictors of performance outcomes. As there is a need for standardizing measures of communication that can be related to cyber team performance, the structural observations used to quantify communication behaviors of possible relevance and relating them to performance outcomes is a first step towards developing more communication-related performance metrics. Furthermore, by applying measures of cyber SA for analysts (Lif et al., 2017) and relating them to metacognition, mood processing, and vagal tone, this thesis has contributed towards the establishing of performance metrics for cyber analysts, which in the case of cyber SA is lacking (Gutzwiller et al., 2020).

The use of neuroscience and neuroergonomic approaches in this thesis work has broadened the scope of how cyber team performance can be assessed. Still, the present research contains some methodological shortcomings that need to be addressed. One of the main contributors towards methodological shortcoming is the difficulty of recruiting relevant

participants in high numbers and organizational restrictions related to implementing high-quality measures in naturalistic studies such as those conducted in CDXs. The systematic review and the critical discussion in this thesis have highlighted the need for more involved collaboration between researchers and CDX organizers. Because the applicability of outcomes are related to the quality of the research, a practical contribution of the thesis has been to address this issue.

7.1. Key takeaways

Applying sensor technology to measure neurophysiological indicators of performance during CDXs is feasible.

XR technology may be a useful aid to improve operational communication in cyber teams. The technology is mature enough to be implemented in CDXs.

There is a need for more involved collaboration between researchers and CDX organizers to ensure high quality results. In other words, more experimentation and less piggybacking.

7.2. Ethical Reflections

The vmHRV measures used in the present work are largely determined by genetics (Golosheykin et al., 2017; Wang et al., 2009). As it has potential to serve as a predictor of job-performance in certain contexts, there is always the possibility that the findings of such research will be used in job-selection processes and possibly used in a discriminatory way. Such practices are thus not only discriminating on the basis of neurophysiology but also genetics. The implementation of vmHRV in selection processes should therefore be subject to cost-benefit analysis. The more relevant the position is for high stakes settings such as national security, the more tolerable is the cost.

Chapter 8

8 Conclusion

The work included in this thesis has contributed with a theoretical framework that can be used to identify and investigate performance indicators in cybersecurity and to develop interventions. Findings from the studies included in this thesis seem to fall in line with what one would expect from neuroscientific literature. The results suggest that vagal tone is associated with metacognitive judgements and mood, and that mood also is associated with metacognitive judgments. The relationship between vagal tone and communication demands are hard to interpret due to discrepancies in the findings. Tools that utilize multi-sensory integration when visualizing network topology and traffic in 3D appear to result in better dyadic communication and SA compared to 2D visualization tools, but this has no observable effect on decision-making. Due to the small sample sizes, the studies need to be replicated in larger samples to validate the results. There is a need for larger studies with more involved collaboration between cognitive neuroscientists and organizers of CDXs to allow for proper investigation of whether identified indicators impact performance in a meaningful way. Scientists need to be mindful of the challenges that organizers face while at the same time trying to make measurements integrated in exercise reports. To this end, developing scoring systems with red teamers that can be applied to reports and the performance of participants will be useful. The work described in this thesis is an important step towards applying neuroergonomic approaches to improve human communication in cybersecurity.

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, *4*(3), 125–152. https://doi.org/10.1080/23742917.2019.1698178

Ahrend, J. M., Jirotka, M., & Jones, K. (2016). On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In *2016 International Conference on Cyber Situational Awareness. Data Analytics and Assessment (CyberSA)*, *2016*, 1-10 (London, UK). https://doi.org/10.1109/CyberSA.2016.7503279

Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., Welch, I., Camtepe, S. A., & Kim, D. D. (2022). A survey on cyber situation awareness systems: framework, techniques, and insights. *ACM Computing Surveys*, *55*, 1–37. https://doi.org/10.1145/3530809

Alberts, D., and Garstka, J. (2004). *Network Centric Operations conceptual framework version 2.0.* Technical Report, US Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration, US Department of Defense.

Aldao, A., Dixon-Gordon, K. L., & De Los Reyes, A. (2016). Individual differences in physiological flexibility predict spontaneous avoidance. *Cognition & emotion*, *30*(5), 985–998. https://doi.org/10.1080/02699931.2015.1042837

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of human vulnerabilities on cybersecurity. *Computer Systems Science & Engineering*, *40*(3), 1153-1166. https://doi.org/10.32604/csse.2022.019938

Appelhans, B. M., & Luecken, L. J. (2006). Heart rate variability as an index of regulated emotional responding. *Review of General Psychology*, *10*(3), 229-240. https://doi.org/10.1037/1089-2680.10.3.229

Ask, T. F., Sütterlin, S., Knox, B. J., Lugo, R. G. (2021). Situational states influence on team workload demands in cyber defense exercise. In *Stephanidis C. (ed) HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning and Culture. HCII 2021. Lecture Notes in Computer Science*, (Cham: Springer), 3–20. Doi:10.1007/978-3-030-90328-2_1

Ayaz, H., & Dehais, F. (2019). (Eds.). *Neuroergonomics: The Brain at Work and in Everyday Life*. London: Elsevier; Academic Press.

Badre, D., & Nee, D. E. (2018). Frontal cortex and the hierarchical control of behavior. *Trends in cognitive sciences*, *22*(2), 170–188. https://doi.org/10.1016/j.tics.2017.11.005

Baird, J. R. (1986). Improving learning through enhanced metacognition: a classroom study. European *Journal of Science Education*, *8*(3), 263–282. https://doi.org/10.1080/0140528860080303

Baker, L., & Brown, A. L. (1984). Metacognitive skills and reading. In *Pearson, P. D. (ed.) Handbook of Reading Research Vol. 1*, 353–395 (Longman, New York).

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., & Yen, J. (2010). Cyber SA: situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (eds) *Cyber Situational Awareness. Advances in Information Security*, *46*, 3–13 (Cham: Springer). https://doi.org/10.1007/978-1-4419-0140-8_1

Benarroch, E. E. (1993). The central autonomic network: functional organization, dysfunction, and perspective. *Mayo Clinic proceedings*, *68*(10), 988–1001. https://doi.org/10.1016/s0025-6196(12)62272-1

Berggaard, N., Bjerke, I. E., B Paulsen, A. E., Hoang, L., T Skogaker, N. E., Witter, M. P., & van der Want, J. J. L. (2018). Development of parvalbumin-expressing basket terminals in layer II of the rat medial entorhinal cortex. *eNeuro*, 5(3), ENEURO.0438-17.2018. https://doi.org/10.1523/ENEURO.0438-17.2018

Berntson, G. G., Bigger, J. T., Jr, Eckberg, D. L., Grossman, P., Kaufmann, P. G., Malik, M., Nagaraja, H. N., Porges, S. W., Saul, J. P., Stone, P. H., & van der Molen, M. W. (1997). Heart rate variability: origins, methods, and interpretive caveats. *Psychophysiology*, *34*(6), 623–648. https://doi.org/10.1111/j.1469-8986.1997.tb02140.x

Bilash, O. M., Chavlis, S., Johnson, C. D., Poirazi, P., & Basu, J. (2023). Lateral entorhinal cortex inputs modulate hippocampal dendritic excitability by recruiting a local disinhibitory microcircuit. *Cell reports*, *42*(1), 111962. https://doi.org/10.1016/j.celrep.2022.111962

Birch, S. A., Li, V., Haddock, T., Ghrear, S. E., Brosseau-Liard, P., Baimel, A., & Whyte, M. (2017). Perspectives on perspective taking: how children think about the minds of others. *Advances in Child Development and Behavior*, *52*, 185–226. https://doi.org/10.1016/bs.acdb.2016.10.005

Blaser, B. L., Weymar, M., & Wendt, J. (2023). The effect of a single-session heart rate variability biofeedback on attentional control: does stress matter?. Frontiers in psychology, 14, 1292983. https://doi.org/10.3389/fpsyg.2023.1292983

Bohbot, V. D., Copara, M. S., Gotman, J., & Ekstrom, A. D. (2017). Low-frequency theta oscillations in the human hippocampus during real-world and virtual navigation. *Nature communications*, *8*, 14415. https://doi.org/10.1038/ncomms14415

Boldt, A., & Gilbert, S. J. (2022). Partially overlapping neural correlates of metacognitive monitoring and metacognitive control. *The Journal of neuroscience : the official journal of the Society for Neuroscience*, *42*(17), 3622–3635. https://doi.org/10.1523/JNEUROSCI.1326-21.2022

Botvinick, M. M., Braver, T. S., Barch, D. M., Carter, C. S., & Cohen, J. D. (2001). Conflict monitoring and cognitive control. *Psychological Review*, *108*(3), 624–652. https://doi.org/10.1037/0033-295x.108.3.624

Bradley, M. M., & Lang, P. J. (1994). Measuring emotion: the self-assessment manikin and the semantic differential. *Journal of Behavior Therapy and Experimental Psychiatry*, *25*, 49–59.

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity*, *8*(1), tyac001. https://doi.org/10.1093/cybsec/tyac001

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

Brunyé, T. T., Beaudoin, M. E., Feltmanm, K. A., Heaton, K. J., McKinley, R. A., Vartanian, O., Tangney, J. F., Erp, J. V., Vergin, A., Merla, A., & Whittaker, A. (2022). Neuroenhancement in military personnel: conceptual and methodological promises and challenges. *STO Technical Report* STO-MP-HFM-334, 1 1-32.

Brysbaert, M. (2019). How many participants do we have to include in properly powered experiments? A tutorial of power analysis with reference tables. *Journal of cognition, 2*(1), 16. https://doi.org/10.5334/joc.72

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

Buchler, N., laFleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Frontiers in Psychology*, *9*. doi:10.3389/fpsyg.2018.02133

Buckley, J., Cohen, J. D., Kramer, A. F., McAuley, E., & Mullen, S. P. (2014). Cognitive control in the self-regulation of physical activity and sedentary behavior. *Frontiers in human neuroscience*, *8*, 747. https://doi.org/10.3389/fnhum.2014.00747

Butler, E. A., Egloff, B., Wilhelm, F. H., Smith, N. C., Erickson, E. A., & Gross, J. J. (2003). The social consequences of expressive suppression. *Emotion (Washington, D.C.)*, *3*(1), 48–67. https://doi.org/10.1037/1528-3542.3.1.48

Button, K. S., Ioannidis, J. P., Mokrysz, C., Nosek, B. A., Flint, J., Robinson, E. S., & Munafò, M. R. (2013). Power failure: why small sample size undermines the reliability of neuroscience. *Nature reviews. Neuroscience*, *14*(5), 365–376. https://doi.org/10.1038/nrn3475

Caltagirone, S., Pendergast, A., & Betzl, C. (2013). *The diamond model of intrusion analysis*. Center for Cyber Intelligence Analysis and Threat Research, 1-61. Hanover, MD.

Campitelli, G., & Labollita, M. (2010). Correlations of cognitive reflection with judgments and choices. *Judgment and Decision Making*, *5*(3), 182-191. https://doi.org/10.1017/S1930297500001066

Canadian Centre for Cyber Security (2021). "*Cyber threat and cyber threat actors*". Cyber.gc.ca, [https://cyber.gc.ca/en/guidance/cyber-threat- andcyber-threat-actors]

Canali, S., Schiaffonati, V., & Aliverti, A. (2022). Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLOS digital health*, *1*(10), e0000104. https://doi.org/10.1371/journal.pdig.0000104

Canham, M., Posey, C., & Bockelman, P.S. (2020). Confronting information security's elephant, the unintentional insider threat. In Schmorrow, D., Fidopiastis, C. (eds) *Augmented Cognition. Human Cognition and Behavior. HCII 2020. Lecture Notes in Computer Science, 12197*, 316–334. (Springer, Cham). https://doi.org/10.1007/978-3-030-50439-7_22

Cannon-Bowers, J. A., and Salas, E. (2001). Reflections on shared cognition. *Journal of Organizational Behavior*, *22*, 195–202. doi: 10.1002/job.82

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-based cyber defense analysis. In *2012 IEEE International Multi-Disciplinary Conference on Cognitive*

Methods in situation. Awareness and Decision Support (New Orleans, LA. USA), 218–221. https://doi.org/10.1109/CogSIMA.2012.6188386

Chand, T., Li, M., Jamalabadi, H., Wagner, G., Lord, A., Alizadeh, S., Danyeli, L. V., Herrmann, L., Walter, M., & Sen, Z. D. (2020). Heart rate variability as an index of differential brain dynamics at rest and after acute stress induction. *Frontiers in neuroscience*, *14*, 645. https://doi.org/10.3389/fnins.2020.00645

Chang, C., & Glover, G. H. (2009). Effects of model-based physiological noise correction on default mode network anti-correlations and correlations. *NeuroImage*, *47*(4), 1448–1459. https://doi.org/10.1016/j.neuroimage.2009.05.012

Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). Sources of occupational stress and prevalence of burnout and clinical distress among US Air Force Cyber Warfare Operators (No. AFRL-SA-WP-TR-2013-0006). School of Aerospace Medicine, Wright-Patterson AFB, OH.

Charitoudi, K., & Blyth, A. (2023). A socio-technical approach to cyber risk management and impact assessment. *Journal of Information Security*, *4*, 33-41. http://dx.doi.org/10.4236/jis.2013.41005

Chen, A. C., Oathes, D. J., Chang, C., Bradley, T., Zhou, Z. W., Williams, L. M., Glover, G. H., Deisseroth, K., & Etkin, A. (2013). Causal interactions between fronto-parietal central executive and default-mode networks in humans. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(49), 19944–19949. https://doi.org/10.1073/pnas.1311772110

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cybersecurity: A systematic literature review. *Information & Computer Security*, *29*(5), 697–723. https://doi.org/10.1108/ICS-07-2020-0121

Christensen, J., Doczy, E., Durbin, M., Finomore, V., Funke, M., McKinley, R., Satterfield, K., Schmidt, R., Sidrow, K., & Traver, K. (2010). *Neuroergonomics deep dive literature review, volume 1: Neuroergonomics and cognitive state*. Air Force Research Laboratory, AFRL-RH-WP-TP-2011-0001, 1-58. Retrieved from [https://apps.dtic.mil/sti/tr/pdf/ADA536065.pdf]

Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum*, *37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Clore, G. L., & Huntsinger, J. R. (2007). How emotions inform judgment and regulate thought. *Trends in cognitive sciences*, *11*(9), 393–399. https://doi.org/10.1016/j.tics.2007.08.005

Cocchi, L., Halford, G. S., Zalesky, A., Harding, I. H., Ramm, B. J., Cutmore, T., Shum, D. H., & Mattingley, J. B. (2014). Complexity in relational processing predicts changes in functional brain network dynamics. *Cerebral cortex (New York, N.Y. : 1991)*, *24*(9), 2283–2296. https://doi.org/10.1093/cercor/bht075

Cocchi, L., Zalesky, A., Fornito, A., & Mattingley, J. B. (2013). Dynamic cooperation and competition between brain systems during cognitive control. *Trends in cognitive sciences*, *17*(10), 493–501. https://doi.org/10.1016/j.tics.2013.08.006

Cohen, J. D. (2017). Cognitive control: core constructs and current considerations. In *Egner, T. (ed) The Wiley handbook of cognitive control*, 3–28. Chichester, West Sussex, UK: John Wiley & Sons Ltd.

Cole, M. W., Yarkoni, T., Repovs, G., Anticevic, A., & Braver, T. S. (2012). Global connectivity of prefrontal cortex predicts cognitive control and intelligence. *The Journal of neuroscience : the official journal of the Society for Neuroscience*, *32*(26), 8988–8999. https://doi.org/10.1523/JNEUROSCI.0536-12.2012

Cooke, N. J., Gorman, J. C., Myers, C. W., & Duran, J. L. (2013). Interactive team cognition. *Cognitive Science*, *37*, 255–285. doi: 10.1111/cogs.12009

Dawson, C. (2023). Looking on the (b)right side of life: cognitive ability and miscalibrated financial expectations. *Personality and Social Psychology Bulletin*, *0*(0). https://doi.org/10.1177/01461672231209400

De Schotten, M. T., & Forkel, S. J. (2022). The emergent properties of the connected brain. *Science*, *378*(6619), 505-510. DOI: 10.1126/science.abq2591

De Witte, N. A., Sütterlin, S., Braet, C., & Mueller, S. C. (2016). Getting to the heart of emotion regulation in youth: the role of interoceptive sensitivity, heart rate variability, and parental psychopathology. *PloS one*, *11*(10), e0164615. https://doi.org/10.1371/journal.pone.0164615

Debashi, M., & Vickers, P. (2018). Sonification of network traffic flow for monitoring and situational awareness. *PloS one*, *13*(4), e0195948. https://doi.org/10.1371/journal.pone.0195948

DeCoster, J., Gallucci, M., Iselin, A.-M. R. (2011). Best practices for using median splits, artificial categorization, and their continuous alternatives. *Journal of Experimental Psychopathology*, 2(2), 197-209. doi:10.5127/jep.008310

Desender, K., Van Opstal, F., & Van den Bussche, E. (2014). Feeling the conflict: The crucial role of conflict experience in adaptation. *Psychological Science*, *25*(3), 675–683. doi:10.1177/0956797613511468

Desender, K., Vermeylen, L. & Verguts, T. (2022). Dynamic influences on static measures of metacognition. *Nature Communications*, *13*, 4208. https://doi.org/10.1038/s41467-022-31727-0

Doeller, C. F., Barry, C., & Burgess, N. (2010). Evidence for grid cells in a human memory network. *Nature*, *463*(7281), 657–661. https://doi.org/10.1038/nature08704

Dresler, M., Shirer, W. R., Konrad, B. N., Müller, N. C. J., Wagner, I. C., Fernández, G., Czisch, M., & Greicius, M. D. (2017). Mnemonic training reshapes brain networks to support superior memory. *Neuron*, *93*(5), 1227–1235.e6. https://doi.org/10.1016/j.neuron.2017.02.003

Duncan, J. (2013). The structure of cognition: attentional episodes in mind and brain. *Neuron*, *80*(1), 35–50. https://doi.org/10.1016/j.neuron.2013.09.015

Durso, F. T., Hackworth, C. A., Truitt, T. R., Crutchfield, J., Nikolic, D., & Manning, C. A. (1998). Situation awareness as a predictor of performance for en route air traffic controllers. *Air Traffic Control Quarterly*, *6*(1), 1–20.

Edgar, L., Jones, M. D., Jr, Harsy, B., Passiment, M., & Hauer, K. E. (2021). Better decision-making: shared mental models and the clinical competency committee. *Journal of graduate medical education*, *13*(2 Suppl), 51–58. https://doi.org/10.4300/JGME-D-20-00850.1

Efklides, A. (2008). Metacognition: defining its facets and levels of functioning in relation to self-regulation and co-regulation. *European Psychologist*, *13*(4), 277–287. https://doi.org/10.1027/1016-9040.13.4.277

Eichenbaum, H. (2014). Time cells in the hippocampus: a new dimension for mapping memories. *Nature reviews. Neuroscience*, *15*(11), 732–744. https://doi.org/10.1038/nrn3827

Ekstrom, A. D., Caplan, J. B., Ho, E., Shattuck, K., Fried, I., & Kahana, M. J. (2005). Human hippocampal theta activity during virtual navigation. *Hippocampus*, *15*(7), 881–889. doi:10.1002/hipo.20109

Emery, F. E. (1959). Characteristics of socio-technical systems. London: Tavistock Institute of Social Relations, Doc. 527.

Emery, F., & Thorsrud, E. (1976). *Democracy at work*. Canberra: Australian National University, Centre for Continuing Education.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In: *Proceedings of the Human Factors Society 32nd Annual Meeting, 32(2)*, 97–101. https://doi.org/10.1177/154193128803200221

Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Human Factors*, *37*(1), 65-84. https://doi.org/10.1518/001872095779049499

Endsley, M. R. (2020). The Divergence of Objective and Subjective Situation Awareness: A Meta-Analysis. *Journal of Cognitive Engineering and Decision Making*, *14*(1), 34-53. https://doi.org/10.1177/1555343419874248

Endsley, M. R. (2021). A systematic review and meta-analysis of direct objective measures of Situation Awareness: A comparison of SAGAT and SPAM. *Human Factors*, *63*(1), 124–150. https://doi.org/10.1177/0018720819875376

European Union Agency for Cybersecurity, Drogkaris, P., & Bourka, A. (2018). Cybersecurity culture guidelines – Behavioural aspects of cybersecurity, Drogkaris, P. (editor), Bourka, A.(editor), European Network and Information Security Agency. https://doi.org/10.2824/324042

European Union Agency for Cybersecurity, ENISA. (2022). *European Cybersecurity Skills Framework Role Profiles*. Available online at: [https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles] (accessed March 06, 2024).

Fabricius, W. V., & Schwanenflugel, P. J. (1994). The older child's theory of mind. In A. Demetriou & A. Efklides (Eds.), *Intelligence, mind, and reasoning: Structure and development*, 111–132. Amsterdam: Elsevier.

Faul, L., & LaBar, K. S. (2023). Mood-congruent memory revisited. *Psychological review*, *130*(6), 1421–1456. https://doi.org/10.1037/rev0000394

Firth, A. M., Ask, T. F., Sütterlin, S., & Lugo, R. G. (2022). The effect of heart rate variability biofeedback training on vagal tone in athletically talented secondary school students. *Sports (Basel, Switzerland)*, *10*(10), 146. https://doi.org/10.3390/sports10100146

Fisher, K. (2022). The role of gender in providing expert advice on cyber conflict and artificial intelligence for military personnel. *Frontiers in Big Data*, *5*, 992620. https://doi.org/10.3389/fdata.2022.992620

Flavell, J. H. (1979). Metacognition and cognitive monitoring: a new area of cognitive-developmental inquiry. *American Psychologist*, *34*(10), 906–911. https://doi.org/10.1037/0003-066X.34.10.906

Flavell, J. H., & Wellman, H. M. (1975). *Metamemory*. 1-66.

Fleming, S. M., & Lau, H. C. (2014). How to measure metacognition. *Frontiers in Human Neuroscience*, *8*, 443. https://doi.org/10.3389/fnhum.2014.00443

Fleur, D. S., Bredeweg, B., & van den Bos, W. (2021). Metacognition: ideas and insights from neuro- and educational sciences. *Npj Science Of Learning*, *6*, 13. https://doi.org/10.1038/s41539-021-00089-5

Forgas, J. P. (2017). Mood effects on cognition: Affective influences on the content and process of information processing and behavior. In *Jeon M. (ed.), Emotions and Affect in Human Factors and Human-Computer Interaction*, 89–122. Cambridge, MA: Academic Press.

Fox, M. D., Snyder, A. Z., Vincent, J. L., Corbetta, M., Van Essen, D. C., & Raichle, M. E. (2005). The human brain is intrinsically organized into dynamic, anticorrelated functional networks. *Proceedings of the National Academy of Sciences of the United States of America*, *102*(27), 9673–9678. https://doi.org/10.1073/pnas.0504136102

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Friedman, N. P., & Robbins, T. W. (2022). The role of prefrontal cortex in cognitive control and executive function. *Neuropsychopharmacology*, *47*, 72–89. https://doi.org/10.1038/s41386-021-01132-0

Friesen, M. A., White, S. V., & Byers, J. F. (2008). Chapter 34: Handoffs: implications for nurses. In R. G. Hughes (ed) *Patient Safety and Quality: An Evidence-Based Handbook for Nurses*, 285–332. Rockville, MD: Agency for Healthcare Research and Quality.

Fyhn, M., Hafting, T., Treves, A., Moser, M. B., & Moser, E. I. (2007). Hippocampal remapping and grid realignment in entorhinal cortex. *Nature*, *446*(7132), 190–194. https://doi.org/10.1038/nature05601

Fyhn, M., Molden, S., Witter, M. P., Moser, E. I., & Moser, M. B. (2004). Spatial representation in the entorhinal cortex. *Science (New York, N.Y.)*, *305*(5688), 1258–1264. https://doi.org/10.1126/science.1099901

Galvin, S. J., Podd, J. V., Drga, V., & Whitmore, J. (2003). Type 2 tasks in the theory of signal detectability: discrimination between correct and incorrect decisions. *Psychonomic bulletin & review*, *10*(4), 843–876. https://doi.org/10.3758/bf03196546

Gambetti, E., & Giusberti, F. (2012). The effect of anger and anxiety traits on investment decisions. *Journal of Economic Psychology*, *33*(6), 1059–1069. doi:10.1016/j.joep.2012.07.001

Geisler, F. C. M., Vennewald, N., Kubiak, T., Weber, H. (2010). The impact of heart rate variability on subjective well-being is mediated by emotion regulation. *Personality and Individual Differences*, *49*(7), 723–728.

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: a guide for non-statisticians. *International journal of endocrinology and metabolism*, *10*(2), 486–489. https://doi.org/10.5812/ijem.3505

Girardeau, G., & Zugaro, M. (2011). Hippocampal ripples and memory consolidation. *Current opinion in neurobiology*, *21*(3), 452–459. https://doi.org/10.1016/j.conb.2011.02.005

Golkar, A., Lonsdorf, T. B., Olsson, A., Lindstrom, K. M., Berrebi, J., Fransson, P., Schalling, M., Ingvar, M., & Öhman, A. (2012). Distinct contributions of the dorsolateral prefrontal and orbitofrontal cortex during emotion regulation. *PloS one*, *7*(11), e48107. https://doi.org/10.1371/journal.pone.0048107

Golosheykin, S., Grant, J. D., Novak, O. V., Heath, A. C., & Anokhin, A. P. (2017). Genetic influences on heart rate variability. International journal of psychophysiology : official journal of the International Organization of Psychophysiology, 115, 65–73. https://doi.org/10.1016/j.ijpsycho.2016.04.008

Gonzalez-Escamilla, G., Dörfel, D., Becke, M., Trefz, J., Bonanno, G. A., & Groppa, S. (2022). Associating flexible regulation of emotional expression with psychopathological symptoms. *Frontiers in behavioral neuroscience*, *16*, 924305. https://doi.org/10.3389/fnbeh.2022.924305

Good, D., & Yeganeh, B. (2012). Cognitive agility: adapting to real-time decision making at work. *OD Practitioner*, *44*(2), 13–17.

Good, D. J. (2009). Cognitive agility: A real-time adaptive capacity. *Academy of Management Annual Meeting*. Chicago, Illinois.

Goto, N., & Schaefer, A. (2017). Emotional Intensity. In *Zeigler-Hill, V., Shackelford, T. (eds) Encyclopedia of Personality and Individual Differences*, 1-9. Springer, Cham. https://doi.org/10.1007/978-3-319-28099-8_509-1

Gouveia, V. V., de Moura, H. M., de Oliveira, I. C. V., Ribeiro, M. G. C., Rezende, A. T., Brito, T. R. S. (2018). Emotional regulation questionnaire (ERQ): evidence of construct

validity and internal consistency. *Psico-USF*, *23*(3), 461–471. doi:10.1590/1413-82712018230306

Gratton, G., Cooper, P., Fabiani, M., Carter, C. S., & Karayanidis, F. (2018). Dynamics of cognitive control: Theoretical bases, paradigms, and a view for the future. *Psychophysiology*, *55*(3), e13016. https://doi.org/10.1111/psyp.13016

Greenlee, E. T., Funke, G. J., Warm, J. S., Sawyer, B. D., Finomore, V. S., Mancuso, V. F., Funke, M. E., & Matthews, G. (2016). Stress and workload profiles of network analysis: not all tasks are created equal. In *Nicholson, D. (ed) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing*, *501*. Springer, Cham. https://doi.org/10.1007/978-3-319-41932-9_13

Gross, J. J. (1998). The emerging field of emotion regulation: an integrative review. *Review of General Psychology*, *2*(3), 271-299. https://doi.org/10.1037/1089-2680.2.3.271

Guidetti, O. A., Speelman, C., & Bouhlas, P. (2023). A review of cyber vigilance tasks for network defense. *Frontiers in Neuroergonomics*, *4*, 1104873. https://doi.org/10.3389/fnrgo.2023.1104873

Gutzwiller, R., Dykstra, J., & Payne, B. (2020). Gaps and Opportunities in Situational Awareness for Cybersecurity. Digital Threats: Research and Practice, 1(3), 1–6. https://doi.org/10.1145/3384471

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

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). https://doi.org/10.1109/COGSIMA.2016.7497780

Hafting, T., Fyhn, M., Molden, S., Moser, M. B., & Moser, E. I. (2005). Microstructure of a spatial map in the entorhinal cortex. *Nature*, *436*(7052), 801–806. https://doi.org/10.1038/nature03721

Han, J., Waddington, G., Adams, R., Anson, J., & Liu, Y. (2016). Assessing proprioception: A critical review of methods. *Journal of sport and health science*, *5*(1), 80–90. https://doi.org/10.1016/j.jshs.2014.10.004

Hancock, P. A., Sawyer, B. D., & Stafford, S. (2015). The effects of display size on performance. *Ergonomics*, *58*(3), 337–354. https://doi.org/10.1080/00140139.2014.973914

Hansen, A. L., Johnsen, B. H., & Thayer, J. F. (2009). Relationship between heart rate variability and cognitive function during threat of shock. *Anxiety, Stress & Coping, 22*(1), 77–89. doi:10.1080/10615800802272251

Hansen, A. L., Johnsen, B. H., Thornton, D., Waage, L., & Thayer, J. F. (2007). Facets of psychopathy, heart rate variability and cognitive function. *Journal of personality disorders*, *21*(5), 568–582. https://doi.org/10.1521/pedi.2007.21.5.568

Hare, T. A., Camerer, C. F., & Rangel, A. (2009). Self-control in decision-making involves modulation of the vmPFC valuation system. *Science (New York, N.Y.)*, *324*(5927), 646–648. https://doi.org/10.1126/science.1168450

Hargreaves, E. L., Rao, G., Lee, I., and Knierim, J. J. (2005). Major dissociation between medial and lateral entorhinal input to dorsal hippocampus. *Science*, *308*, 1792–1794. https://doi.org/10.1126/science.1110449.

Hámornik, B. P., & Krasznay, C. (2018). A team-level perspective of human factors in cyber security: security operations centers. *Advances in Human Factors in Cybersecurity*, *593*, 224–236. doi:10.1007/978-3-319-60585-2_21

Henshel, D. S., Deckard, G. M., Lufkin, B., Buchler, N., Hoffman, B., Rajivan, P., & Collman, S. (2016). Predicting proficiency in cyber defense team exercises. *MILCOM 2016 - 2016 IEEE Military Communications Conference*, *2016*, 776-781 (Baltimore, MD, USA). doi: 10.1109/MILCOM.2016.7795423.

Hildebrandt, L. K., McCall, C., Engen, H. G., & Singer, T. (2016). Cognitive flexibility, heart rate variability, and resilience predict fine-grained regulation of arousal during prolonged threat. *Psychophysiology*, *53*(6), 880–890. https://doi.org/10.1111/psyp.12632

Hinde, K., White, G., & Armstrong, N. (2021). Wearable Devices Suitable for Monitoring Twenty Four Hour Heart Rate Variability in Military Populations. *Sensors* (Basel, Switzerland), *21*(4), 1061. https://doi.org/10.3390/s21041061

Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L., & Endert, A. (2010). Towards efficient collaboration in cyber security. *2010 International Symposium on Collaborative Technologies and Systems*, 489-498. https://doi.org/10.1109/CTS.2010.5478473

Hutchins, E., Cloppert, M. J., & Amin, R. M. (2010). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion Kill Chains. *Lockheed Martin Corporation*, 1-14.

ISC2 (2023). ISC2 Global Workforce Study. How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce. media.isc2.org, [https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e&hash=CE6762D811935593F5C04AAB49DF33DF]

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ. Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Iggena, D., Jeung, S., Maier, P. M., Ploner, C. J., Gramann, K., & Finke, C. (2023). Multisensory input modulates memory-guided spatial navigation in humans. *Communications biology*, *6*(1), 1167. https://doi.org/10.1038/s42003-023-05522-6

Jacob, P. Y., Poucet, B., Liberge, M., Save, E., & Sargolini, F. (2014). Vestibular control of entorhinal cortex activity in spatial navigation. *Frontiers in integrative neuroscience*, *8,* 38. https://doi.org/10.3389/fnint.2014.00038

Jariwala, S., Champion, M., Rajivan, P., & Cooke, N. J. (2012). Influence of team communication and coordination on the performance of teams at the iCTF competition. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *56*(1), 458-462. https://doi.org/10.1177/1071181312561044

Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., & Babar, M. A. (2022). Systematic literature review on Cyber Situational Awareness visualizations. *IEEE Access*, *10*, 57525-57554. Doi: 10.1109/ACCESS.2022.3178195

Johnson, C., Badger, M., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing, (SP 800-150), Gaithersburg, Maryland. https://doi.org/10.6028/NIST.SP.800-150.

Johnson, K. T., & Picard, R. W. (2020). Advancing neuroscience through wearable devices. Neuron, 108(1), 8–12. https://doi.org/10.1016/j.neuron.2020.09.030

Joint Task Force Transformation Initiative (JTFTI). (2012). Guide for Conducting Risk Assessments (SP 800-30, Rev. 1). NIST, Gaithersburg, Maryland, Technical Report, 2012. https://doi.org/10.6028/NIST.SP.800-53r4

Jøsok, Ø., Knox, B. J., Helkala, K., Wilson, K., Sütterlin, S., Lugo, R. G., & Ødegaard, T. (2017). Macrocognition applied to the hybrid space: team environment, functions and processes in cyber operations. In *Lecture Notes in Computer Science*. eds. D. D. Schmorrow and C. M. Fidopiastis, vol. 10285, 486–500. Cham: Springer. https://doi.org/10.1007/978-3-319-58625-0_35

Jøsok, Ø., 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: Schmorrow, D., Fidopiastis, C. (eds) *Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience. AC 2016. Lecture Notes in Computer Science()*, vol 9744, 178–188. Cham: Springer. https://doi.org/10.1007/978-3-319-39952-2_18

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

Kanwisher, N., & Wojciulik, E. (2000). Visual attention: insights from brain imaging. *Nature reviews. Neuroscience*, *1*(2), 91–100. https://doi.org/10.1038/35039043

Kaplan, A. D., Cruit, J., Endsley, M., Beers, S. M., Sawyer, B. D., & Hancock, P. A. (2021). The effects of virtual reality, augmented reality, and mixed reality as training enhancement methods: A meta-analysis. *Human factors*, *63*(4), 706–726. https://doi.org/10.1177/0018720820904229

Kelley, N. J., Gallucci, A., Riva, P., Romero Lauro, L. J., & Schmeichel, B. J. (2019). Stimulating self-regulation: A review of non-invasive brain stimulation studies of goal-directed behavior. *Frontiers in Behavioral Neuroscience*, *12*, 337. doi:10.3389/fnbeh.2018.00337

Kelly, J. E. (1978). A reappraisal of sociotechnical systems theory. *Human Relations*, *31*(12), 1069-1099. https://doi.org/10.1177/001872677803101204

Kerr, K. M., Agster, K. L., Furtak, S. C., & Burwell, R. D. (2007). Functional neuroanatomy of the parahippocampal region: the lateral and medial entorhinal areas. *Hippocampus*, *17*, 697–708. https://doi.org/10.1002/hipo.20315

Kim, C., Cilles, S. E., Johnson, N. F., & Gold, B. T. (2011). Domain general and domain preferential brain regions associated with different types of task switching: a meta-analysis. *Human brain mapping*, *33*(1), 130–142. https://doi.org/10.1002/hbm.21199

Kim, H. G., Cheon, E. J., Bai, D. S., Lee, Y. H., & Koo, B. H. (2018). Stress and heart rate variability: A meta-analysis and review of the literature. *Psychiatry investigation*, *15*(3), 235–245. https://doi.org/10.30773/pi.2017.08.17

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

Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019). Cognisance as a Human Factor in Military Cyber Defence Education. *IFAC-PapersOnLine*, *52*(19), 163–168. doi:10.1016/j.ifacol.2019.12.168

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 *C. Stephanidis (ed) HCII Posters 2017, 713*, 330–338 (Cham: Springer). https://doi.org/10.1007/978-3-319-58750-9_46

Koster, E. H., De Raedt, R., Goeleven, E., Franck, E., & Crombez, G. (2005). Mood-congruent attentional bias in dysphoria: maintained attention to and impaired disengagement from negative information. *Emotion (Washington, D.C.)*, *5*(4), 446–455. https://doi.org/10.1037/1528-3542.5.4.446

Koval, P., Ogrinz, B., Kuppens, P., Van den Bergh, O., Tuerlinckx, F., & Sütterlin, S. (2013). Affective instability in daily life is predicted by resting heart rate variability. *PloS one*, *8*(11), e81536. https://doi.org/10.1371/journal.pone.0081536

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (eds) *Cyberpower and National Security*, 24-42. University of Nebraska Press, Nebraska. Retrieved from [https://ndupress.ndu.edu].

Kuhrt, D., St. John, N. R., Bellmund, J. L. S., Kaplan, R., & Doeller, C. F. (2021). An immersive first-person navigation task for abstract knowledge acquisition. *Scientific Reports*, *11*(1). doi:10.1038/s41598-021-84599-7

Kullman, K., & Engel D. (2022). Interactive stereoscopically perceivable multidimensional data visualizations for cybersecurity. *Journal of Defence & Security Technologies*, *4*(3), 37-52. http://dx.doi.org/10.46713/jdst.004.03

Kullman, K., Asher, N. B., & Sample, C. (2019b). Operator impressions of 3D visualizations for cybersecurity analysts. In *T. Cruz, S. Paulo (ed) Proceedings of the 18th European*

Conference on Cyber Warfare and Security, ECCWS 2019. University of Coimbra, Portugal (Reading, UK: ACPI) 257–266.

Kullman, K., Buchanan, L., Komlodi, A., & Engel, D. (2020). Mental model mapping method for cybersecurity. In *A. Moallem (ed) HCI for Cybersecurity, Privacy and Trust. HCII 2020*, (Cham, Springer). doi: 10.1007/978-3-030-50309-3_30

Kullman, K., Cowley, J. A., & Ben-Asher, N. (2018). Enhancing cyber defense situational awareness using 3D visualizations. In *Proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018,* 369–378. National Defense University, Washington DC, USA (Washington DC: Academic Conferences and Publishing International Limited).

Kullman, K., Ryan, M., & Trossbach, L. (2019a). VR/MR supporting the future of defensive cyber operations. *IFAC-PapersOnLine*, *52*, 181–186. doi: 10.1016/j.ifacol.2019.12.093

Kwon, E. S., Kittaneh, A. A., Gerardo, G. M., Koenig, J., Thayer, J. F., & Williams, D. P. (2022). Resting heart rate variability, perceived emotion regulation, and low-risk drug use in college-aged adults: gender as a moderator. *Frontiers in psychiatry*, *13*, 885217. https://doi.org/10.3389/fpsyt.2022.885217

Laborde, S., & Mosley, E. (2016). Commentary: Heart rate variability and self-control-A meta-analysis. *Frontiers in psychology*, *7*, 653. https://doi.org/10.3389/fpsyg.2016.00653

Lande, N. M., Ask, T. F., Sætren, S. S., Lugo, R. G., & Sütterlin, S. (2023). The Role of Emotion Regulation for General Self-Efficacy in Adolescents Assessed Through Both Neurophysiological and Self-Reported Measures. *Psychology research and behavior management*, *16*, 3373–3383. https://doi.org/10.2147/PRBM.S406702

Leenen, L., & Meyer, T. (2021). Artificial Intelligence and Big Data Analytics in Support of Cyber Defense. *Research Anthology on Artificial Intelligence Applications in Security*. https://doi.org/10.4018/978-1-5225-8304-2.CH002.

Lif, P., Granasen, M., & Sommestad, T. (2017). Development and validation of technique to measure cyber situation awareness. In *2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, *2017*, 1-8 (London, UK). https://doi.org/10.1109/CyberSA.2017.8073388

Lif, P., Sommestad, T., & Granasen, D. (2018). Development and evaluation of information elements for simplified cyber-incident reports. In *2018 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, *2018*, 1-10 (Glasgow, UK). https://doi.org/10.1109/CyberSA.2018.8551402

Lif, P., Varga, S., Wedlin, M., Lindahl, D., & Persson, M. (2020). Evaluation of information elements in a cyber incident report. In *2020 IEEE European symposium on security and privacy workshops (EuroS&PW)*, *2020*, 17-26 (Genoa, Italy). https://doi.org/10.1109/EuroSPW51379.2020.00012

Liston, C., Chen, A. C., Zebley, B. D., Drysdale, A. T., Gordon, R., Leuchter, B., Voss, H. U., Casey, B. J., Etkin, A., & Dubin, M. J. (2014). Default mode network mechanisms of transcranial magnetic stimulation in depression. *Biological psychiatry*, *76*(7), 517–526. https://doi.org/10.1016/j.biopsych.2014.01.023

Livingston, J. A. (2003). *Metacognition: An Overview*. 1-7.

Livingstone, K. M., & Isaacowitz, D. M. (2015). Situation selection and modification for emotion regulation in younger and older adults. *Social psychological and personality science*, *6*(8), 904–910. https://doi.org/10.1177/1948550615593148

Lugo, R. G., & Sütterlin, S. (2018). Cyber officer profiles and performance factors. *Lecture Notes in Computer Science*, *10906*, 181–190. https://doi.org/10.1007/978-3-319-91122-9_16

Lugo, R. G., Firth-Clark, A., Knox, B. J., Jøsok, Ø., Helkala, K. M., & Sütterlin, S. (2019). Cognitive profiles and education of female Cyber Defence Operators. *Lecture Notes in Computer Science*, *11580,* 563-572. Doi. 10.1007/978-3-030-22419-6_40

Lugo, R., Kwei-Nahr, P., Jøsok, Ø., Knox, B. J., Helkala, K., & Sütterlin, S. (2017). Team workload demands influence on cyber detection performance. In *13th International Conference on Naturalistic Decision Making*, 223–225 (Bath, UK).

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

Lund, M. S. (2022). Øving på cybersikkerheit: ein casestudie av ei cybersikkerheitsøving. *Scandinavian Journal of Military Studies*, *5*, 244–256. doi: 10.31374/sjms.119

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Magnon, V., Vallet, G. T., Benson, A., Mermillod, M., Chausse, P., Lacroix, A., Bouillon-Minois, J. B., & Dutheil, F. (2022). Does heart rate variability predict better executive functioning? A systematic review and meta-analysis. *Cortex; a journal devoted to the*

study of the nervous system and behavior, *155*, 218–236. https://doi.org/10.1016/j.cortex.2022.07.008

Makin, T. R., & Orban de Xivry, J. J. (2019). Ten common statistical mistakes to watch out for when writing or reviewing a manuscript. *eLife*, *8*, e48175. https://doi.org/10.7554/eLife.48175

Marques, A. H., Silverman, M. N., & Sternberg, E. M. (2010). Evaluation of stress systems by applying noninvasive methodologies: measurements of neuroimmune biomarkers in the sweat, heart rate variability and salivary cortisol. *Neuroimmunomodulation*, *17*(3), 205–208. https://doi.org/10.1159/000258725

Mc Mahon, C. (2020). In defence of the human factor. *Frontiers in Psychology*, *11*, 1390. https://doi.org/10.3389/fpsyg.2020.01390

McCabe, J. A. (2015). Location, Location, Location! Demonstrating the Mnemonic Benefit of the Method of Loci. *Teaching of Psychology*, *42*(2), 169-173. https://doi.org/10.1177/0098628315573143

McCauley-Bell, P. R., & Crumpton, L. L. (1998). The human factors issues in Information Security: What are they and do they matter? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *42*(4), 439-443. https://doi.org/10.1177/154193129804200408

McChrystal, S., Collins, T., Silverman, D., & Fussell, C. (2016). *Teams of Teams: New Rules of Engagement for a Complex World*. Penguin, New York.

McCorry, L. K. (2007). Physiology of the autonomic nervous system. *American journal of pharmaceutical education*, *71*(4), 78. https://doi.org/10.5688/aj710478

McNeese, N. J., Demir, M., Cooke, N. J., & She, M. (2021). Team situation awareness and conflict: a study of human–machine teaming. *Journal of Cognitive Engineering and Decision Making*, *15*(2-3), 83-96. https://doi.org/10.1177/15553434211017354

Medaglia, J. D. (2019). Clarifying cognitive control and the controllable connectome. Wiley interdisciplinary reviews. *Cognitive science*, *10*(1), e1471. https://doi.org/10.1002/wcs.1471

Meessen, J., Sütterlin, S., Gauggel, S., & Forkmann, T. (2018). Learning by heart-the relationship between resting vagal tone and metacognitive judgments: a pilot study. *Cognitive processing*, *19*(4), 557–561. https://doi.org/10.1007/s10339-018-0865-6

Menon, V., & D'Esposito, M. (2022). The role of PFC networks in cognitive control and executive function. *Neuropsychopharmacology*, *47*, 90–103. doi: 10.1038/s41386-021-01152-w

Milardi, D., Bramanti, P., Milazzo, C., Finocchio, G., Arrigo, A., Santoro, G., Trimarchi, F., Quartarone, A., Anastasi, G., & Gaeta, M. (2015). Cortical and subcortical connections of the human claustrum revealed in vivo by constrained spherical deconvolution tractography. *Cerebral cortex (New York, N.Y. : 1991)*, *25*(2), 406–414. https://doi.org/10.1093/cercor/bht231

Min, J., Koenig, J., Nashiro, K., Yoo, H. J., Cho, C., Thayer, J. F., & Mather, M. (2023). Sex Differences in Neural Correlates of Emotion Regulation in Relation to Resting Heart Rate Variability. *Brain topography*, *36*(5), 698–709. https://doi.org/10.1007/s10548-023-00974-9

Miyake, A., Friedman, N. P., Emerson, M. J., Witzki, A. H., Howerter, A., & Wager, T. D. (2000). The unity and diversity of executive functions and their contributions to complex "frontal lobe" tasks: A latent variable analysis. *Cognitive Psychology*, *41*(1), 49–100. doi:10.1006/cogp.1999.0734

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS medicine*, *6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L. A., & PRISMA-P Group (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic reviews*, *4*(1), 1. https://doi.org/10.1186/2046-4053-4-1

Mohanty, A., & Sussman, T. J. (2013). Top-down modulation of attention by emotion. *Frontiers in human neuroscience*, *7*, 102. https://doi.org/10.3389/fnhum.2013.00102

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: concerns for psychiatry. *Current Psychiatry Reports*, *23*(4), 18. https://doi.org/10.1007/s11920-021-01228-w

Moon, J., Sasangohar, F., Son, C., & Peres, S. C. (2020). Cognition in Crisis Management Teams: An Integrative Analysis of Definitions. *Ergonomics*, 1–23. doi:10.1080/00140139.2020.1781936

Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*, *13*(11). Available at [https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/].

Moser, E. I., Kropff, E., & Moser, M. B. (2008). Place cells, grid cells, and the brain's spatial representation system. *Annual review of neuroscience*, *31*, 69–89. https://doi.org/10.1146/annurev.neuro.31.061307.090723

Moser, M. B., Rowland, D. C., & Moser, E. I. (2015). Place cells, grid cells, and memory. *Cold Spring Harbor perspectives in biology*, *7*(2), a021808. https://doi.org/10.1101/cshperspect.a021808

Nee, D. E. (2021). Integrative frontal-parietal dynamics supporting cognitive control. *eLife*, *10*, e57244. doi: 10.7554/eLife.57244

Nee, D. E., & D'Esposito, M. (2016). The hierarchical organization of the lateral prefrontal cortex. *eLife*, *5*, e12112. doi: 10.7554/eLife.12112

Nelson, T. O., & Narens, L. (1990). Metamemory: A Theoretical Framework and New Findings. In *Bower, G. (Ed.), The Psychology of Learning and Motivation: Advances in Research and Theory*, 125-173. Academic Press, New York. https://doi.org/10.1016/S0079-7421(08)60053-5

Nelson, T. O. & Narens, L. (1994). Why investigate metacognition. In *J. Metcalfe & A. P. Shimamura (eds.) Metacognition: Knowing About Knowing*, 1–25. MIT Press: MA.

Niehorster, D. C. (2021). Optic flow: a history. *i-Perception*, *12*(6), 20416695211055766. https://doi.org/10.1177/20416695211055766

NIST (1992). 1991 Annual Report of the Computer System Security and Privacy Advisory Board, National Institute of Standards and Technology (NIST), March 1992, p. 18.

O'Keefe, J., & Nadel, L. (1978). *The Hippocampus as a Cognitive Map*. Oxford: Clarendon.

Ochsner, K. N., Ray, R. D., Cooper, J. C., Robertson, E. R., Chopra, S., Gabrieli, J. D., & Gross, J. J. (2004). For better or for worse: neural systems supporting the cognitive down- and up-regulation of negative emotion. *NeuroImage*, *23*(2), 483–499. https://doi.org/10.1016/j.neuroimage.2004.06.030

Ofte, H. J., & Katsikas, S. (2023). Understanding situation awareness in SOCs, a systematic literature review. *Computers & Security*, *126*(C), 103069. https://doi.org/10.1016/j.cose.2022.103069

Okon-Singer, H., Hendler, T., Pessoa, L., & Shackman, A. J. (2015). The neurobiology of emotion-cognition interactions: fundamental questions and strategies for future research. *Frontiers in human neuroscience*, *9*, 58. https://doi.org/10.3389/fnhum.2015.00058

Oltsik, J. (2019). *The life and times of cybersecurity professionals*. Technical report, Enterprise Strategy Group (ESG), 1-42.

Omand, D. (2011). *Securing the State*. Oxford University Press: New York.

Osnes, B., Berrefjord, S. R., Poless, P. G., Sigrist, C., Koenig, J., & Sørensen, L. (2023). Low heart rate variability is associated with a negativity valence bias in interpreting ambiguous emotional expressions. *Emotion*, *23*(4), 1040–1047. https://doi.org/10.1037/emo0001123

Pagani, M., Pizzinelli, P., Bergamaschi, M., & Malliani, A. (1982). A positive feedback sympathetic pressor reflex during stretch of the thoracic aorta in conscious dogs. *Circulation research*, *50*(1), 125–132. https://doi.org/10.1161/01.res.50.1.125

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ (Clinical research ed.)*, *372*, n71. https://doi.org/10.1136/bmj.n71

Panikratova, Y. R., Vlasova, R. M., Akhutina, T. V., Korneev, A. A., Sinitsyn, V. E., & Pechenkova, E. V. (2020). Functional connectivity of the dorsolateral prefrontal cortex contributes to different components of executive functions. *International journal of psychophysiology : official journal of the International Organization of Psychophysiology*, 151, 70–79. https://doi.org/10.1016/j.ijpsycho.2020.02.013

Parasuraman, R. (1990). Event-related brain potentials and human factors research. In *J. W. Rohrbaugh, R. Parasuraman and R. Johnson (eds), Event-related Brain Potentials: Basic and Applied Issues*, 279–300. New York: Oxford University Press.

Parasuraman, R. (1998). *The Attentive Brain*. Cambridge, MA: MIT Press.

Parasuraman, R. (2003). Neuroergonomics: Research and practice. *Theoretical Issues in Ergonomics Science*, *4*(1-2), 5–20. https://doi.org/10.1080/14639220210199753

Parasuraman, R. (2011). Neuroergonomics: Brain, Cognition, and Performance at Work. *Current Directions in Psychological Science*, *20*(3), 181-186. https://doi.org/10.1177/0963721411409176

Parasuraman, R., & Riley, V. A. (1997). Humans and automation: use, misuse, disuse, abuse. *Human Factors*, *39*, 230–253.

Parasuraman, R., Greenwood, P. M., & Sunderland, T. (2002). The apolipoprotein E gene, attention, and brain function. *Neuropsychology*, *16*, 254–274.

Parasuraman, R., Mouloua, M., & Hilburn, B. (1999). Adaptive aiding and adaptive task allocation enhance human–machine interaction. In *M. Scerbo, M. Mouloua (eds), Automation Technology and Human Performance: Current Research and Trends*, 119–123. Mahwah, NJ: Erlbaum.

Parasuraman, R., Mouloua, M., & Molloy, R. (1996). Effects of adaptive task allocation on monitoring of automated systems. *Human Factors*, *38*, 665–679.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics*, *30*, 286–297.

Paschke, L. M., Dörfel, D., Steimke, R., Trempler, I., Magrabi, A., Ludwig, V. U., Schubert, T., Stelzel, C., & Walter, H. (2016). Individual differences in self-reported self-control predict successful emotion regulation. *Social Cognitive and Affective Neuroscience*, *11*(8), 1193–1204. doi:10.1093/scan/nsw036

Pasmore, W., Francis, C., Haldeman, J., & Shani, A. (1982). Sociotechnical systems: A North American reflection on empirical studies of the seventies. *Human Relations*, *35*(12), 1179-1204. https://doi.org/10.1177/001872678203501207

Patel, P. (2014). Defense against the dark arts (of Cyberspace) universities are offering graduate degrees in cybersecurity. *IEEE Spectrum*, *51*, 26-26. https://doi.org/10.1109/MSPEC.2014.6821610

Paul, K., & Pourtois, G. (2017). Mood congruent tuning of reward expectation in positive mood: evidence from FRN and theta modulations. *Social cognitive and affective neuroscience*, *12*(5), 765–774. https://doi.org/10.1093/scan/nsx010

Paulhus, D. L., Harms, P. D., Bruce, M. N., & Lysy, D. C. (2003). The over-claiming technique: measuring self-enhancement independent of ability. *Journal of Personality and Social Psychology*, 84(4) 890–904; doi: 10.1037/0022-3514.84.4.890

Payer, G., & Trossbach, L. (2015). The application of virtual reality for cyber information visualization and investigation. *Evolution of Cyber Technologies and Operations to 2035*, 71–90. doi:10.1007/978-3-319-23585-1_6

Petrosyan, A. (2023). *Estimated cost of cybercrime worldwide 2017-2028*. Statista. Available at [https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide].

Pinna, T., & Edwards, D. J. (2020). A systematic review of associations between interoception, vagal tone, and emotional regulation: potential applications for mental health, wellbeing, psychological flexibility, and chronic conditions. *Frontiers in Psychology*, *11*, 1792. https://doi.org/10.3389/fpsyg.2020.01792

Pobric, G., Chillingsworth, K., Mitchell, G., Smith, S., & Hulleman, J. (2021). Effects of transcranial electrical stimulation (tES) in Defence and security related tasks: meta-analysis of findings from healthy populations. In *Proceedings of NATO HFM-RSY-334 Symposium Applying Neuroscience to Performance: From Rehabilitation to Human Cognitive Augmentation*, 4 1-12.

Poth, C. H. (2021). Urgency forces stimulus-driven action by overcoming cognitive control. *eLife*, *10*, e73682. https://doi.org/10.7554/eLife.73682

Press, M. (1986). *Situation awareness: Let's get serious about the clue bird*. Unpublished manuscript.

Pu, J., Schmeichel, B. J., & Demaree, H. A. (2010). Cardiac vagal control predicts spontaneous regulation of negative emotional expression and subsequent cognitive performance. *Biological Psychology*, *84*, 531–540. doi:10.1016/j.biopsycho.2009.07.006

Questienne, L., Van Opstal, F., van Dijck, J.-P., & Gevers, W. (2018). Metacognition and cognitive control: behavioural adaptation requires conflict experience. *Quarterly Journal of Experimental Psychology*, *71*(2), 411–423. doi:10.1080/17470218.2016.1251473

Raichle, M. E., MacLeod, A. M., Snyder, A. Z., Powers, W. J., Gusnard, D. A., & Shulman, G. L. (2001). A default mode of brain function. *Proceedings of the National Academy of Sciences of the United States of America*, *98*(2), 676–682. https://doi.org/10.1073/pnas.98.2.676

Ray, S., & Brecht, M. (2016). Structural development and dorsoventral maturation of the medial entorhinal cortex. *eLife*, *5*, e13343. https://doi.org/10.7554/eLife.13343

Razza, L. B., De Smet, S., Cornelis, X., Nikolin, S., Pulopulos, M. M., De Raedt, R., Brunoni, A. R., & Vanderhasselt, M. A. (2024). Dose-dependent response of prefrontal transcranial direct current stimulation on the heart rate variability: An electric field modeling study. *Psychophysiology*, e14556. Advance online publication. https://doi.org/10.1111/psyp.14556

Reagan, M. D. (1967). Basic and applied research: a meaningful distinction?. *Science (New York, N.Y.)*, *155*(3768), 1383–1386. https://doi.org/10.1126/science.155.3768.1383

Reggente, N., Essoe, J. K. Y., Baek, H. Y., & Rissman, J. (2019). The method of loci in virtual reality: explicit binding of objects to spatial contexts enhances subsequent memory recall. *Journal of Cognitive Enhancement*, *4*, 12–30. https://doi.org/10.1007/s41465-019-00141-8

Rohr, M., Tarvainen, M., Miri, S., Güney, G., Vehkaoja, A., & Antink, C. (2024). An extensive quantitative analysis of the effects of errors in beat-to-beat intervals on all commonly used HRV parameters. *Scientific Reports*, *14*, 2498. https://doi.org/10.1038/s41598-023-50701-4

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 C2 Journal, 2(1), 1–30.

Salmon, P. M., Stanton, N. A., Walker, G. H., Baber, C., Jenkins, D. P., McMaster, R., & Young, M. S. (2008). What really is going on? Review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science*, *9*(4), 297–323. doi:10.1080/14639220701561775

Scerbo, M. W., Freeman, F. G., Mikulka, P. J., Parasuraman, R., Di Nocera, F., & Prinzel, L. J. (2001). The efficacy of psychophysiological measures for implementing adaptive technology, NASA TP-2001-211018 (Hampton, VA: NASA Langley Research Center).

Schinagl, S., Schoon, K., & Paans, R. (2015). A framework for designing a security operations centre (SOC). 48th Hawaii International Conference on System Sciences; IEEE, *2015*, 2253-2262. https://doi.org/10.1109/HICSS.2015.270

Schmaußer, M., Hoffmann, S., Raab, M., & Laborde, S. (2022). The effects of noninvasive brain stimulation on heart rate and heart rate variability: A systematic review and meta-analysis. *Journal of neuroscience research*, *100*(9), 1664–1694. https://doi.org/10.1002/jnr.25062

Schmidt, L., Tusche, A., Manoharan, N., Hutcherson, C., Hare, T., & Plassmann, H. (2018). Neuroanatomy of the vmPFC and dlPFC predicts individual differences in cognitive regulation during dietary self-control across regulation strategies. *The Journal of neuroscience : the official journal of the Society for Neuroscience*, *38*(25), 5799–5806. https://doi.org/10.1523/JNEUROSCI.3402-17.2018

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York, NY: John Wiley & Sons.

Schraw, G., & Dennison, R. S. (1994). Assessing Metacognitive Awareness. *Contemporary Educational Psychology*, *19*(4), 460–475. https://doi.org/10.1006/ceps.1994.1033

Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002

Schwerdtfeger, A. R., & Gerteis, A. K. (2014). The manifold effects of positive affect on heart rate variability in everyday life: distinguishing within-person and between-person associations. *Health psychology : official journal of the Division of Health Psychology, American Psychological Association*, *33*(9), 1065–1073. https://doi.org/10.1037/hea0000079

Sellers, J., Helton, W. S., Näswall, K., Funke, G. J., & Knott, B. A. (2014). Development of the Team Workload Questionnaire (TWLQ). *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *58*(1), 989-993. https://doi.org/10.1177/1541931214581207

Sharkov, G. (2016). From cybersecurity to collaborative resiliency. *SafeConfig '16: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*, *2016*, 3–9. (Vienna, Austria). https://doi.org/10.1145/2994475.2994484

Shi, H., Zhao, H., Liu, Y., Gao, W., & Dou, S. C. (2019). Systematic analysis of a military wearable device based on a multi-level fusion framework: research directions. Sensors (Basel, Switzerland), 19(12), 2651. https://doi.org/10.3390/s19122651

Shimamura, A. P. (2008). A neurocognitive approach to metacognitive monitoring and control. In *J. Dunlosky J., R. A. Bjork (eds.) Handbook of Metamemory and Memory*, 373–390. New York, NY: Psychology Press.

Silvers, J. A., & Guassi Moreira, J. F. (2019). Capacity and tendency: A neuroscientific framework for the study of emotion regulation. *Neuroscience letters*, *693*, 35–39. https://doi.org/10.1016/j.neulet.2017.09.017

Sklerov, M., Dayan, E., & Browner, N. (2019). Functional neuroimaging of the central autonomic network: recent developments and clinical implications. *Clinical autonomic research : official journal of the Clinical Autonomic Research Society*, *29*(6), 555–566. https://doi.org/10.1007/s10286-018-0577-0

Smirnov, D., Glerean, E., Lahnakoski, J. M., Salmi, J., Jääskeläinen, I. P., Sams, M., & Nummenmaa, L. (2014). Fronto-parietal network supports context-dependent speech

comprehension. *Neuropsychologia*, *63*, 293–303. https://doi.org/10.1016/j.neuropsychologia.2014.09.007

Spring, J. M., & Illari, P. (2021). Review of human decision-making during computer security incident analysis. *Digital Threats*, *2*(2), 2021. DOI: 10.1145/3427787.

Staheli, D., Mancuso, V., Harnasch, R., Fulcher, C., Chmielinski, M., Kearns, A., Kelly, S., & Vuksani, E. (2016). Collaborative data analysis and discovery for cyber security. In *SOUPS 2016: Twelfth Symposium on Usable Privacy and Security* (Denver, CO), 1-7.

Stahl, B. C. (2007). ETHICS, Morality and Critique: An Essay on Enid Mumford¡¯s Socio-Technical Approach. *Journal of the Association for Information Systems*, *8*(9), 479-490. DOI: 10.17705/1jais.00138

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., … Tetrick, L. E. (2015). Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Security & Privacy*, *13*(4), 20–29. doi:10.1109/msp.2015.71

Stimpfel, A. W., Sloane, D. M., & Aiken, L. H. (2012). The longer the shifts for hospital nurses, the higher the levels of burnout and patient dissatisfaction. *Health affairs (Project Hope)*, *31*(11), 2501–2509. https://doi.org/10.1377/hlthaff.2011.1377

Stuyck, H., Demeyer, F., Bratanov, C., Cleeremans, A., & Van den Bussche, E. (2023). Insight and non-insight problem solving: A heart rate variability study. *Quarterly Journal of Experimental Psychology*, *0*(0). https://doi.org/10.1177/17470218231202519

Sütterlin, S., Herbert, C., Schmitt, M., Kübler, A., & Vögele, C. (2011). Frames, decisions, and cardiac-autonomic control. *Social neuroscience*, *6*(2), 169–177. https://doi.org/10.1080/17470919.2010.495883

Sütterlin, S., Lugo, R., Ask, T., Veng, K., Eck, J., Fritschi, J., Özmen, M.-T., Bärreiter, B., & Knox, B. J. (2022). The Role of IT Background for Metacognitive Accuracy, Confidence and Overestimation of Deep Fake Recognition Skills. *In Schmorrow, D. D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2022. Lecture Notes in Computer Science()*, *13310*, 103-119. Springer, Cham. https://doi.org/10.1007/978-3-031-05457-0_9

Tamir, M., & Robinson, M. D. (2007). The happy spotlight: positive mood and selective attention to rewarding information. *Personality & social psychology bulletin*, *33*(8), 1124–1136. https://doi.org/10.1177/0146167207301030

Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology. (1996). Heart rate variability: standards of measurement, physiological interpretation and clinical use. *Circulation*, *93*(5), 1043–1065.

Taylor, N., Carroll, A., & Gifford, R. M. (2023). Five-day evaluation of the acceptability and comfort of wearable technology at four anatomical locations during military training. *BMJ military health*, e002524. *Advance online publication*. https://doi.org/10.1136/military-2023-002524

Taylor, N., Willman, A. S., Eager, M., & Gifford, R. M. (2024). Enhancing decision-making in the Armed Forces through wearable technology: what do commanders think?. *BMJ military health,* e002710. *Advance online publication*. https://doi.org/10.1136/military-2024-002710

Tiwari, R., Kumar, R., Malik, S., Raj, T., & Kumar, P. (2021). Analysis of heart rate variability and implication of different factors on heart rate variability. *Current cardiology reviews*, 17(5), e160721189770. https://doi.org/10.2174/1573403X16999201231203854

Thayer, J. F., & Lane, R. D. (2009). Claude Bernard and the heart-brain connection: further elaboration of a model of neurovisceral integration. *Neuroscience and biobehavioral reviews*, *33*(2), 81–88. https://doi.org/10.1016/j.neubiorev.2008.08.004

Tinde, T. G. (2022). *Cyber Threat Information Requirements for Strategic Decision-Making*. [Master Thesis, NTNU].

Tomes, C., Schram, B., & Orr, R. (2020). Relationships between heart rate variability, occupational performance, and fitness for tactical personnel: A systematic review. *Frontiers in public health*, *8*, 583336. https://doi.org/10.3389/fpubh.2020.583336

Toplak, M. E., West, R. F., & Stanovich, K. E. (2011). The Cognitive Reflection Test as a predictor of performance on heuristics-and-biases tasks. *Memory & cognition*, *39*(7), 1275–1289. https://doi.org/10.3758/s13421-011-0104-1

Torgerson, C. M., Irimia, A., Goh, S. Y., & Van Horn, J. D. (2015). The DTI connectivity of the human claustrum. *Human brain mapping*, *36*(3), 827–838. https://doi.org/10.1002/hbm.22667

Trent, S., Hoffman, R. R., Merritt, D., & Smith, S. (2019). Modelling the cognitive work of cyber protection teams. *The Cyber Defense Review*, *4*(1), 125-136.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., Lewin, S., … Straus,

S. E. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Annals of internal medicine*, *169*(7), 467–473. https://doi.org/10.7326/M18-0850

Trist, E. L., & Bamforth, K. (1951). Some social and psychological consequences of the long-wall method of coal-getting. *Human Relations*, *4*, 3-39.

Trist, E. L., Higgin, G., Murray, H., & Pollock, A. B. (1963). *Organizational choice*. London, Tavistock.

Tsaparlis, G. (2014). Cognitive demand. In *Gunstone, R. (ed), Encyclopedia of Science Education*, 1–4. Springer; Netherlands.

Ural, Ö., & Acartürk, C. (2021). Automatic detection of cyber security events from Turkish Twitter stream and newspaper data. In *Conference: 7th International Conference on Information Systems Security and Privacy*, 66-76. https://doi.org/10.5220/0010201600660076

Vaccaro, A. G., & Fleming, S. M. (2018). Thinking about thinking: A coordinate-based meta-analysis of neuroimaging studies of metacognitive judgements. *Brain and neuroscience advances*, *2*, 2398212818810591. https://doi.org/10.1177/2398212818810591

Varga, S., Brynielsson, J., & Franke, U. (2018). Information requirements for national level cyber situational awareness. In *2018 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM)*, 774–781 (Barcelona, Spain).

Veenman, M. V. J., & Elshout, J. J. (1999). Changes in the relation between cognitive and metacognitive skills during the acquisition of expertise. *European Journal of Psychology of Education, XIV*, 509–523

Veksler, V. D., Buchler, N., LaFleur, C. G., Yu, M. S., Lebiere, C., & Gonzalez, C. (2020). Cognitive models in cybersecurity: learning from expert analysts and predicting attacker behavior. *Frontiers in Psychology*, *11*, 1049. https://doi.org/10.3389/fpsyg.2020.01049

Vickerstaff, V., Omar, R. Z., & Ambler, G. (2019). Methods to adjust for multiple comparisons in the analysis and sample size calculation of randomised controlled trials with multiple primary outcomes. *BMC medical research methodology*, *19*(1), 129. https://doi.org/10.1186/s12874-019-0754-4

Volokhov, R. N., & Demaree, H. A. (2010). Spontaneous emotion regulation to positive and negative stimuli. *Brain and cognition*, *73*(1), 1–6. https://doi.org/10.1016/j.bandc.2009.10.015

Wang, X., Ding, X., Su, S., Li, Z., Riese, H., Thayer, J. F., Treiber, F., & Snieder, H. (2009). Genetic influences on heart rate variability at rest and during stress. *Psychophysiology*, *46*(3), 458–465. https://doi.org/10.1111/j.1469-8986.2009.00793.x

Watanabe, D. K., Pourmand, V., Lai, J., Park, G., Koenig, J., Wiley, C. R., Thayer, J. F., & Williams, D. P. (2023). Resting heart rate variability and emotion regulation difficulties: Comparing Asian Americans and European Americans. *International journal of psychophysiology : official journal of the International Organization of Psychophysiology*, *194*, 112258. https://doi.org/10.1016/j.ijpsycho.2023.112258

Watrous, A. J., Fried, I., & Ekstrom, A. D. (2011). Behavioral correlates of human hippocampal delta and theta oscillations during navigation. *Journal of Neurophysiology*, *105*(4), 1747–1755. doi:10.1152/jn.00921.2010

Watrous, A. J., Lee, D. J., Izadi, A., Gurkoff, G. G., Shahlaie, K., & Ekstrom, A. D. (2013). A comparative study of human and rat hippocampal low-frequency oscillations during spatial navigation. *Hippocampus*, *23*(8), 656–661. https://doi.org/10.1002/hipo.22124

Whitlock, J. R., & Moser, E. I. (2009). 7: Synaptic Plasticity and Spatial Representations in the Hippocampus. In M. S. Gazzaniga (ed) The Cognitive Neurosciences (4th ed), 109-127. The MIT Press: Cambridge, MA. https://doi.org/10.7551/mitpress/8029.003.0013

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security* (4th ed). Course Technology, Boston.

Willems, R. M., & Peelen, M. V. (2021). How context changes the neural basis of perception and language. *iScience*, *24*(5), 102392. https://doi.org/10.1016/j.isci.2021.102392

Williams, D. P., Cash, C., Rankin, C., Bernardi, A., Koenig, J., & Thayer, J. F. (2015). Resting heart rate variability predicts self-reported difficulties in emotion regulation: a focus on different facets of emotion regulation. *Frontiers in psychology, 6*, 261. https://doi.org/10.3389/fpsyg.2015.00261

Witter, M. P., Doan, T. P., Jacobsen, B., Nilssen, E. S., & Ohara, S. (2017). Architecture of the Entorhinal Cortex A Review of Entorhinal Anatomy in Rodents with Some Comparative Notes. *Frontiers in systems neuroscience*, *11*, 46. https://doi.org/10.3389/fnsys.2017.00046

Yoder, R. M., & Taube, J. S. (2014). The vestibular contribution to the head direction signal and navigation. *Frontiers in integrative neuroscience*, *8*, 32. https://doi.org/10.3389/fnint.2014.00032

Yufik, Y., & Malhotra, R. (2021). Situational understanding in the human and the machine. *Frontiers in systems neuroscience*, *15*, 786252. https://doi.org/10.3389/fnsys.2021.78625

Zahn, D., Adams, J., Krohn, J., Wenzel, M., Mann, C. G., Gomille, L. K., Jacobi-Scherbening, V., & Kubiak, T. (2016). Heart rate variability and self-control--A meta-analysis. *Biological psychology*, *115*, 9–26. https://doi.org/10.1016/j.biopsycho.2015.12.007

Zehnder, E., Torgersen, L., Ask, T. F., Knox, B. J., Morgernstern, H., Gaiser, J., Naudet, Y., Perez, A. G., & Stahl, C. (2024). Digital twins and extended reality for tailoring better adapted cybersecurity trainings in critical infrastructures. *Lecture Notes in Computer Science*, in press.

Zoto, E., Kowalski, S. J., Rojas, L., Alonso, E., & Mazaher, K. (2018). Using a socio-technical systems approach to design and support systems thinking in cyber security education. *CEUR Workshop Proceedings*, *2107*, 123-128.

Zwergal, A., Grabova, D., & Schöberl, F. (2024). Vestibular contribution to spatial orientation and navigation. *Current opinion in neurology*, 37(1), 52–58. https://doi.org/10.1097/WCO.0000000000001230

ISBN 978-82-326-8148-8 (printed ver.)
ISBN 978-82-326-8147-1 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU

Norwegian University of
Science and Technology