A Gamification Approach to Improving Interpersonal Situational Awareness in Cyber Defense

Torvald F. Ask[1,2,] Benjamin J. Knox[1,2,3] Ricardo G. Lugo[1,2], Lukas Hoffmann[4], Stefan Sütterlin[2,4]

[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] *Norwegian Armed Forces Cyber Defense, Norway*

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

Corresponding author

Torvald F. Ask
Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Gjøvik, Norway
Østfold University College
Faculty of Health, Welfare and Organization
Halden, Norway
Email: torvaldfask@gmail.com / torvalda@hiof.no

Abstract

In cyber threat situations, the establishment of a shared situational awareness as a basis for cyber defense decision-making results from adequate communication of a Recognized Cyber Picture (RCP). RCPs consist of actively selected information and have the goal of accurately presenting the severity and potential consequences of the situation. RCPs must be communicated between individuals, but also between organizations, and often from technical to non-/less technical personnel. The communication of RCPs is subject to many challenges that may affect the transfer of critical information between individuals. There are currently no common best practices for training communication for shared situational awareness among cyber defense personnel. The Orient, Locate, Bridge (OLB) model is a pedagogic tool to improve communication between individuals during a cyber threat situation. According to the model, an individual must apply meta-cognitive awareness (O), perspective taking (L), and communication skills (B) to successfully communicate the RCP. Gamification (applying game elements to non-game contexts) has shown promise as an approach to learning. We propose a novel OLB-based Gamification design to improve dyadic communication for shared situational awareness among (technical and non-technical) individuals during a cyber threat situation. The design includes the Gamification elements of narrative, scoring, feedback, and judgment of self. The proposed concept contributes to the educational development of cyber operators from both military and civilian organizations responsible for defending and securing digital infrastructure. This is achieved by combining the elements of a novel communication model with Gamification in a context in urgent need for educational input.

Keywords: Gamification, cyber defense education, shared situational awareness, cognitive cyber warfare, sociotechnical communication

Introduction

The formal recognition of the cyber domain as a digital battlefield (NATO Cooperative Cyber Defense Centre of Excellence, 2016) was an explicit response to the correlational effects of societal digitalization and an increase in the digital attack surface. It served as a call-to-arms for science-based cyber defense training and education in both civil and military sectors. NATO members and allies need to continually adapt to meet the defense and security vigilance demands required to form, protect and defend networks against existing and emerging cyber threats. These threats target the gray zone between peace and war to influence populations and divide opinion, undermine trust in societal institutions and exploit system vulnerabilities for disruption or espionage (Fitton, 2016; Gardner, 2021). The high rates of innovation and increased network- and technological interdependability that drive, and result from societal digitalization (Zanenga, 2014) increases the complexity of the Socio-Technical Systems (STSs) within which cyber security and cyberspace operations are conducted. In other words, digitalization leads to the expansion of cyberspace and an almost unmanageable cyber threat landscape that places demands on human cognition to adapt to survive.

Within organizations, cyber defense responsibilities are often divided among technical personnel (referred to as analysts or cyber operators; CyOs) who are tasked with detecting, analyzing, reporting and responding to cyber threats. Decision-makers ask critical 'so-what' questions based upon this reporting and assess the risk to mission before making time-critical decisions concerning available courses of action. Due to STS complexity, CyOs encounter many challenges spanning the cyber, physical, and social domains. When investigating a cyber threat situation, CyOs must navigate a technological threat-landscape operating at speeds that often are at odds with innate human cognitive abilities (Zachary et al., 2013). The information that can be extracted about the status of cyber threats is subject to high levels of uncertainty. Subsequently, CyOs must select (1) what information and (2) how to communicate it in a way that supports decision-making and ensures mission success (Jøsok et al., 2016; Knox et al., 2018). Communication problems have been identified as one of the major challenges facing personnel working within cyber defense (Agyepong et al., 2020; ENISA, 2018). There are, however, currently no common best practices for how these communication problems should be addressed in neither cyber defense training nor education (Ask et al., 2021a).

Current approaches, be they military or civilian, to training or explaining human behaviors that promote good cyber defense in organizations (e.g. awareness campaigns) have mostly been too simplistic and tend to blame end-users for failure to comply with target behaviors (ENISA, 2018; McMahon, 2020). The extensive reviews reported on by the European Union Agency For Network and Information Security (ENISA, 2018) suggest that policies and awareness campaigns alone are not sufficient to induce necessary behavioral change for cybersecurity, and that they sometimes are at odds with the productive goals of the organization. Moreover, personality models (e.g. Big 5) and models of behavior (e.g. Theory of Planned Behavior) are insufficient when trying to predict cybersecurity outcomes in the workplace because they ignore context and workplace demands. That said, some components of behavioral models such as 'self-efficacy' and 'coping' appear to be relevant predictors (ENISA, 2018). As noted by

ENISA, “Organizations should strive for adherence (active participation) rather than compliance - rapidly emerging threats require employees who are engaged and willing to step up” (ENISA, 2018; 4). Thus, educational approaches that engage humans at both the individual and group/organizational level, to actively pursue good cyber defense cognitions and behaviors, will arguably make for a resilient organization in the face of emerging cyber threats. Currently, there is a general lack of studies and interventions that simultaneously target cybersecurity performance at both the individual and group level (Ask et al., 2021a).

As the task-related cognitive challenges associated with cyber defense become increasingly complex (Jøsok et al., 2016; Zachary et al., 2013), and where outcomes are characterized by failure intolerance, one could argue that the need for carefully selected and cognition-based approaches to training and education increases with the complexity of these challenges. The threshold for group-level human cognitive performance is dependent on how well the processing-capabilities of the human brain matches the challenges of the group-task environment. Thus, approaches that simultaneously integrate knowledge about the brain with knowledge about the task-environment may be more efficient in training for optimal performance. Neuroergonomic approaches to training are neuro- and thus user-centric and can be implemented by (1) changing the working environment to fit the cognitive capabilities of humans, (2) training specific cognitive capabilities that better fit the working environment, or (3) a combination of the two. In the context of improving interpersonal communication for good cyber defense decision-making, one would have to apply methods that train a collection of specific human cognitive abilities (Jøsok et al., 2017; Knox et al., 2018) and in a sustainable way (ENISA, 2018). Gamification methods optimize for sustained and flexible learning (Howard-Jones & Demetriou, 2009; Lorenz et al., 2015) by hacking the human nervous system through controlling attentional focus (Howard-Jones et al., 2016) in a manner similar to video-games (Khoshnoud et al., 2020; Michailidis et al., 2018). This is necessary for continued engagement (Cowley et al., 2008; Howard-Jones et al., 2016) and the neuroplastic changes associated with learning (Cheng et al., 2020; Recanzone et al., 1992a, 1992b, 1993). We argue that utilizing gamification methods can serve as a neuroergonomic approach that targets the specific cognitive abilities needed for good cyber defense performance while making CyOs feel engaged with the processes and goals related to the outcome of the training.

The intervention design proposed in this paper is motivated to help CyOs involved in defensive cyberspace operations to improve knowledge transfer when communicating cyber threat information. Developing a training environment founded in gamification has the potential to fill this performance gap in socio-technical communication (Ask et al., 2021a; Knox et al., 2018) in cyber-hybrid contexts through a process that is neuroergonomically designed to improve engagement and change behavior. In the following sections, we will detail how gamification approaches can be utilized in training and education for cyber defense. First, we will give a brief overview of gamification mechanics and the considerations that must be met to train cognitive abilities for cyber defense. Then we will review the cognitive processes and abilities needed for achieving an interpersonal understanding of a cyber threat situation. This will be followed by the proposal of a gamification design for cyber team training that can be

utilized to target the specific cognitive abilities and processes implicated in successful communication for cyber defense.

Gamification Methods Used as an Educational Tool to Meet the Challenges of Cyber Defense Training.

Challenges arising from threats in the cyber domain can be urgent or of a delayed nature, and are often shared between organizations due to the interconnectedness between cyber assets. In the case of threats to military organizations (e.g. from nation-state-actors), they will likely have a strategic-level ambition. Research into Human Factors relating to cyber defense performance is beginning to gain traction in a field that has primarily been dominated by technological advancement (Gutzwiller et al., 2015). Of specific interest are cognitive aspects that can be improved through learning processes and interactions. This includes applied research designs aimed at cultivating the cognitive skills required to contend with varying challenges in the cyber threat landscape. For example, defensive cyber personnel must be able to identify and counter an adversary's intent and ability to a) operate under the threshold of 'war', and b) employ tactics that we may yet not be aware of or able to see. In cyber defense, the constantly changing nature of the cyberspace ecosystem leads to novelty, complexity, and uncertainty as well as opportunity (Johnsen, 2019). Consequently, there is a high demand for teaching concepts that explore ambiguity and challenge conventional methods that often fail to consider the implications of a changing cyber ecosystem.

Attempts to create training environments that can reduce risks to own organizational endeavors should focus on Generation X and Y relevant learning phenomenons as an alternative and enhancement to rote techniques designed for the baby boomers (Ong, 2013). For example, 'serious games' are designed to support acquisition and/or skill development (Loh and Yanyan Sheng, 2013), and certain video games encourage innate human pattern setting abilities as well as strategic thinking and the application of tactics founded in distributed knowledge (Gee, 2003). In training scenarios, these effects allow for learners to build adaptive skills as they enhance their current understanding of a situation by engaging in activities such as experimentation, extrapolation, and explantation (Ward et al., 2018). This may well hold some of the answers to how cyber-military training techniques can be modified to match adversaries that have already synchronized their information, cognitive, kinetic, cyber and special operations capabilities (House of Commons 2017; TRADOC, 2017).

Among game-based training approaches, gamification may serve as a neuroergonomic approach that can be easily modified to train the cognitive skills required for cyber defense. Gamification involves the incorporation of competition-, reward-, and ranking elements from video games such as points, leaderboards, and badges in non-game contexts with the aim to optimize learning through increased engagement (Rodrigues et al., 2019). As an approach to learning, gamification has shown very good effects concerning learner motivation and learning outcomes (Landers et al., 2015; Sailer et al., 2013) including those that involve incident management across different organizations (Harter, Schmidt, Killham, & Agrawal, 2009). For

gamification-based training methods to be efficacious in a threat landscape that is prone to rapid change (e.g. Johnson, 2019), one must include elements that specifically target skills that allow for flexible and agile adaptation of cognitive processes according to changing task-demands (Jøsok et al., 2016, 2017; Knox et al., 2017, 2018). One approach to scaffold adaptive skills is to focus on complexity preservation in training (Ward et al., 2018; p45). This requires learners to practice: 1) in varied contexts, 2) at boundaries of current knowledge and skills, 3) accessing knowledge when it is useful or needed, 4) anticipatory thinking, and consider the implications of the current situation for the future, and the alternative ways in which situations may evolve, 5) updating and re-configuring understanding on the fly, and 6) constantly juggling priorities and goal conflict resolution.

In sum, a gamification approach for cyber defense training must include elements that preserve the complexity needed to scaffold the adaptive skills needed to match situational change. This requires a good understanding of the different cognitive processes involved in achieving both an individual and shared situational understanding of a current cyber threat. The challenges associated with these processes often change according to the individuals that are involved in the acquisition and transfer of situational knowledge (Jøsok et al., 2016, 2017; Knox et al., 2017, 2018).

Achieving Shared Situational Awareness for Cyber Defense Decision-Making Rely on Having an Accurate Recognized Cyber Picture

During a cyber threat situation, cyber defense decisions must be grounded in an accurate situational understanding to achieve defensive goals. Cyber defense decision-making is often based on human-to-human communication, which requires communication partners to generate a common and overlapping situational understanding of the cyber threat (Ask et al., 2021a; Knox et al., 2018). Achieving a shared situational understanding can be subject to many challenges that span the cyber-physical domains (Jøsok et al., 2016, 2017), and will often require communication partners to apply a range of cognitive skills that will vary in effort and deliberation depending on how much their individual backgrounds differ from each other (Knox et al., 2018). For instance, when reporting on cyber threats, CyOs must establish a shared situational understanding with decision-makers that may be considered “non-technical”. Because a CyO’s understanding of a cyber threat situation rely on perceptual and sense-making processes that are based on having technical insight, the knowledge structures (mental models) they create to predict future situational states are not readily accessible, thus not immediately transferable nor actionable, to a potentially non-technical decision-maker (Jøsok et al., 2016, 2017; Knox et al., 2017, 2018). Consequently, CyOs and decision-makers operate at different levels of awareness which entail communicational challenges that may impede decision-making if critical information is lost. To fully understand how this potential gap in competence affects knowledge transfer, and how to design training elements to successfully bridge communication between CyOs and non/less-technical decision-makers, one must understand the processes involved in acquiring Situational Awareness (SA) for decision-making.

Situational Awareness for decision-making and performance

First proposed by Endsley (1988), SA is crucial in explaining decision-making and performance when operating in complex systems (Figure 1). SA is achieved through a series of three stages that rely on cognitive processes such as attention and working and long-term memory (Endsley, 1995). The first stage (Level 1 SA) encompasses basic perceptual processes (i.e. monitoring, cue detection, recognition) that then lead the operator to be aware of situational factors and their states, such as technical systems or other operators and their situation, location, and conditions. Awareness of situational factors then leads to the second stage (Level 2 SA) where previous experiences are integrated with current perceptions to form an understanding of how the current situation is influenced. The third stage (Level 3 SA) allows for understanding of current situations and its factors, and predicts possible future states of the environment, including those following the actions resulting from decision-making.

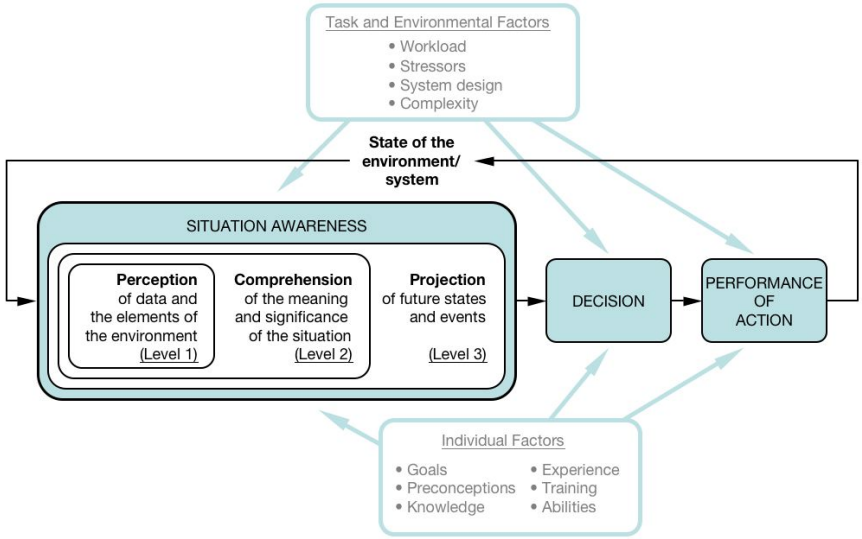

Figure 1: Relationship between Situational Awareness, decision-making, and performance of action and how these processes are influenced by individual and task and environmental factors. Figure adapted from Endsley (1995) by Dr. Peter Lankton, May 2007 (Public License).

SA separates itself from similar concepts such as situational assessment and understanding, situational assessment and sensemaking. Often interchanged with SA, situational assessment is the process used to achieve and sustain SA knowledge (Endsley, 1995) and situational understanding corresponds to Level 2 SA (Dostal, 2007). Sensemaking, on the other hand, has more temporal aspects. While SA is usually an instantaneous process with perception, comprehension and creating future prediction models, sensemaking is a more effortful action that focuses on creating an understanding of prior experiences through deliberation and integrating new information to explain outcomes (Klein et al., 2006).

Building on the framework of Endsley (1988), seven requirements have been suggested to achieve full Cyber Situation Awareness (CSA) for cyber defense (Barford et al., 2009). These requirements can be organized under Level 1-3 SA:

- Level 1 SA: (1) Awareness of the current situation, (2) awareness of the impact of the attack, (3) awareness of adversarial behavior, (4) awareness of the quality and trustworthiness of the CSA information.
- Level 2 SA: (5) Awareness of why and how the current situation is caused, (6) Awareness of how situations evolve.
- Level 3 SA: (7) Assessment of plausible outcomes.

To achieve CSA during a cyber threat situation, having an accurate Recognized Cyber Picture (RCP) is crucial. While general CSA can be considered as having awareness of the underlying state of a specific cyber environment at any given point in time, RCPs consist of actively selected and actionable information and is used to describe the actual circumstances of an incident or threat, e.g. the severity of (un)known effects, especially for individuals who are non/less-technical (Knox et al., 2018). Thus, a RCP is the visual or cognitive representation of cyber threat-related incidents and activities. An RCP that is created by a CyO and intended for a non/less-technical recipient must therefore be tailored to the recipient to achieve a shared CSA.

Organizational structures introduce challenges to RCP communication between CyOs and decision-makers

Organizations source their cyber security operations to internal or external Security Operation Centers (SOCs) which are organizational units and teams working around the clock to defend against cyber threats. SOCs typically form a hierarchical organizational structure with CyOs at the bottom and decision-makers further up in the hierarchical structure, where cyber threat information is 'pushed up' and decisions are 'pushed down' in the decision-making hierarchy (Ask et al., 2021a; Staheli et al., 2016). In this context, RCPs need to be shared and communicated across platforms and in differing modes. This asymmetry can be challenging for decision-making if mental models and priorities differ between the personnel occupying different hierarchical layers (Ask et al., 2021a). When attempting to communicate and share a RCP to a peer or to a member of the hierarchy there is an explicit need for mutual Perspective Taking and for acknowledging communication partner's needs. When this fails to be applied, critical information can get lost due to suboptimal communication flow leading to potentially dire consequences for mission assurance (Knox et al., 2018; Rosen et al., 2008). In a recent study surveying what information Swedish stakeholders (spanning national to local, and private to public actors including providers of critical infrastructure) perceived as needed to meet their RCP requirements, it was reported that none of the stakeholders listed awareness of adversarial behavior as important (Varga et al., 2018). This may suggest a blind-spot in different decision-making agents' mental models of what information is necessary to achieve CSA during a cyber threat situation. In line with their training, CyOs may treat cyber threats as a technical problem requiring technical problem solving. At some point, however, the threat will need to be understood and treated as an operational or a strategic dilemma. The findings of Varga et al. (2018) highlights an area where CyOs may face challenges when communicating RCPs to non-/less technical personnel and explicates the importance of being mindful of how a

communication partner's background and associated priorities affects their mental threat models and situational understanding (Ask et al., 2021a).

Irrespective of rank, communication partners are required to engage in a two-way process of locating and message framing to ensure that performance does not suffer as a cost of poor interaction. Already today, and as a matter of urgency going forward, non-technical military personnel in leadership positions require cyber-domain cognizance to support mission planning, operations and decision-making (Knox et al., 2018). Gaining this understanding demands trust in digital natives and effort to develop cyber-domain knowledge, skills and abilities. It requires engagement in learning, and knowledge transfer with younger soldiers/officers - often with less formal military competence - yet naturals in a digital-age able to contribute to and guide operational planning and/or strategic analysis (Crilly, 2021). As such, acknowledging a communication partner's needs and requirements can lead to more effective and closer aligned mental models in hierarchically challenged, complex, dynamic cyber-hybrid operating environments. Consequently, in this temporal, novel and digitally-driven context there is the opportunity to intervene with new combinations and perspectives on modes of education and training for improved outcomes in training tasks (Landers et al., 2015).

The ultimate goal of a RCP is to ensure enough shared CSA is achieved so that decision-making is born out of trust and understanding instead of authority, bias, or intuition driven by over-confidence. Taking an understanding approach that is founded upon accurate calibration between communication partners can minimize the risks of poor decision-making. Should a network intrusion occur, the severity and potential consequences need to be accurately presented via an RCP and accompanying brief. A cyber defense-associated STS may challenge RCP presentation due to (1) the interconnectedness between decision-making agents and between assets in both cyber and physical domains, (2) the uncertainty regarding the severity of threats and adversarial behaviors, impact of decisions, and the future state of assets, and (3) individual differences (e.g. technical competence, goals, priorities) between communication partners (Jøsok et al., 2016; Knox et al., 2018). Thus, to accurately relay their understanding through appropriate mode, method, and content of communication, CyOs may have to integrate SA from several domains in the STS.

Hierarchical Meta-Situational Awareness (HMSA)

To generate an actionable RCP, CyOs need to acquire SA at the level of the cyber domain (the CSA), and simultaneously integrate it with SA at the level of the social domain (Social SA; SSA; Kola et al., 2020) because they need to be aware of how social situational factors and challenges (different goals, priorities, knowledge, stresses) dictate how to tailor the RCP to their communication partner (Jøsok et al., 2016; Knox et al., 2018). To increase SSA performance, CyOs will need to understand, at some level, that they themselves are a system of internal (emotional and cognitive) states that vary between contexts. These internal states relate to how they understand and respond to different technical, physical, and social environments, including how their technical knowledge is constructed and how it may differ from other people's

knowledge. SA regarding interactions between one's internal states and the environment is achieved through a combination of complementary processes that are automatic, dispositional, and meta-cognitive and interoceptive. Situational Self-Awareness (SSeA) entails automatic processing of one's actions to internalized standards and serves to update an individual on the nature of their behavior in different contexts (Silvia & Duval, 2001). Dispositional Self-Awareness (DSA) entails the extent to which an individual is consciously reflecting over their own psychological processes and experiences and their relationship to others (Fenigstein et al., 1975; Trapnell & Campbell, 1999). Self-Other Distinctions (SOD) entails understanding other individuals' mental and emotional states and how they relate to- and differ from one's own, which requires interoceptive and meta-cognitive abilities (Steinbeis, 2016). Together, SSeA, DSA, and SOD allows an individual to understand their internal states, how they relate to each other, and how they relate to their interactions with the environment. Sometimes physical-domain assets are affected by cyber-domain threats which require Physical SA (PSA; Schauer et al., 2018), and subsequently, Hybrid SA (HSA; Schauer et al., 2018) to predict how decisions will affect cyber and physical systems based on the interconnectedness between physical and cyber assets.

To be consciously aware when monitoring and regulating the cognitive processing of situational elements to generate SA for increased SA-related performance is dependent on a meta-cognitive process called Meta-SA (MSA; Endsley, 2019; Sethumadhavan, 2011). We argue that being able to consciously transact knowledge between different domains of SA in an STS implies establishing a context-dependent hierarchy of SA (a MSA hereon referred to as Hierarchical MSA; HMSA; Figure 2), where various domain-specific social and technical forms of SA and MSA converge on STS-level HMSA at increased levels of hierarchical integration (Figure 2, a).

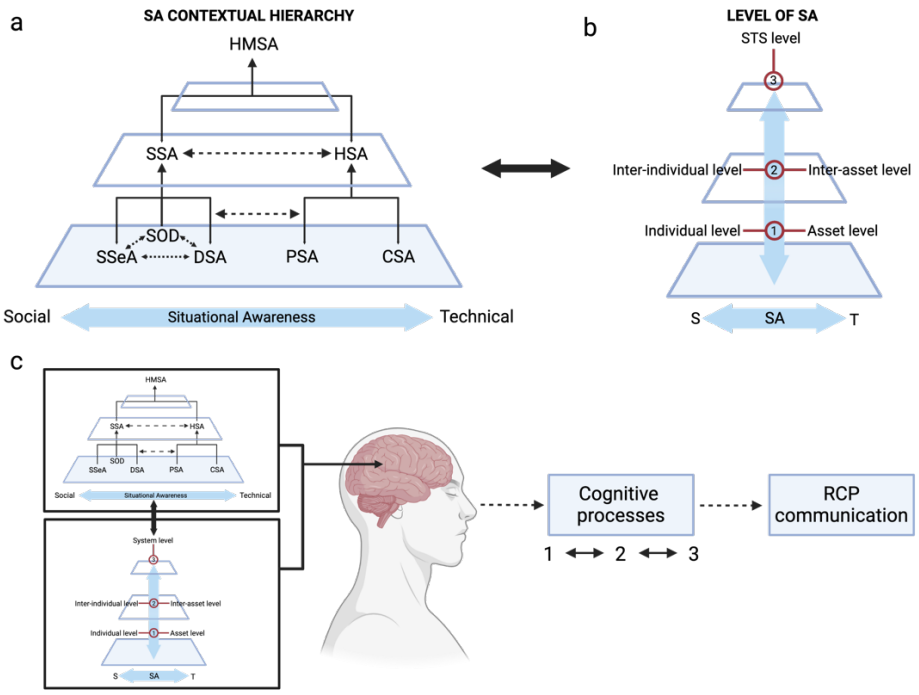

Figure 2: Hierarchical Meta-Situational Awareness (HMSA) from the CyOs perspective and how it relates to RCP communication. **a** HMSA shows the contextual hierarchy of SA in an STS. **b** The HMSA hierarchy can be

organized in SA levels according to the framework proposed by Endsley (1988). **c** Based on the HMSA, CyOs must apply various cognitive processes to generate the RCP. SA = Situational Awareness. SSA = Social Situational Awareness. HSA = Hybrid Situational Awareness. SOD = Self-Other Distinction. SSeA = Situational Self-Awareness. DSA = Dispositional Self-Awareness. PSA = Physical Situational Awareness. CSA = Cyber Situational Awareness. S = Social. T = Technical. 1 = Level 1 SA. 2 = Level 2 SA. 3 = Level 3 SA. Figure created with BioRender.com.

When organizing STS-level HMSA (Figure 2, b) under the level 1-3 framework proposed by Endsley (1988), Level 1 MSA entails establishing SA at the individual/self- (SSeA, DSA, SOD) and asset- (PSA and CSA) level and perceiving the elements that separate them as domains of awareness across a SA environment. Level 2 MSA entails understanding how individual-level and asset-level SA interact to form inter-individual (SSA) and inter-asset level (HSA) SA. Level 3 MSA entails acquiring the ability to predict STS-level future states (STS-level HMSA) based on integrating the understanding of how elements identified by inter-individual and inter-asset level SA influence each other in the STS. Thus, to facilitate a shared CSA between individuals, CyOs must mentally and flexibly transition between cyber and physical, and social and technical contexts, and at different levels of SA (Figure 2, c) when deciding how to communicate a RCP (Jøsok et al., 2016; Knox et al., 2018).

Implicit in HMSA is the notion that to share domain-specific SA at level 1 or level 2 in the HMSA hierarchy, SA at an above level is required, but to utilize an integrated SA at any level for RCP communication, having level 3 HMSA is required. This is because CyOs must understand and predict which and how elements identified in their HSA will change the state (e.g. strategic- and tactical-level goals) of a communication partner based on their SSA and how this affects the STS (Jøsok et al., 2016). As the CyO transitions from lower-to-higher levels in the HMSA hierarchy, the number of cognitive processes required to be successful at each level increases along with cognitive effort (Knox et al., 2017, 2018). Similarly, video games often include levels or stages at increasing difficulty, where the player must learn new skills and often combine them to succeed. Being aware of the different levels of HMSA could inform level design (difficulty) in gamification-based cyber defense training.

The information in the current and above sections can be summarized as follows: SA is required for decision-making to be successful (Endsley, 1988). Decision-making in cyber defense is based on human communication aimed to achieve a shared SA which requires RCPs to be accurate (Knox et al., 2018). RCP sharing is subject to challenges from multiple domains in the STS (Jøsok et al., 2016; Knox et al., 2018) which requires SA in each of these domains. MSA improves SA-performance but (by definition) requires both explicit knowledge of the cognitive processes involved in acquiring SA as well as the ability to willfully apply the cognitive skills involved in those processes (Endsley, 2019; Sethumadhavan, 2011). Thus, to improve and sustain defensive cyber operation mission performance it is necessary to train defensive cyber personnel in attaining HMSA-related cognitive skills.

Challenges may occur when attempting to apply HMSA in gamification design. The theoretical bodies of work implied in all the individual and social factors contributing to SA are vast, but what entails achieving HMSA for a given CyO will be specific to their immediate and extended

working environment (Ask et al., 2021a). Identifying core factors that are applicable across a broad range of working environments may be necessary for good gamification design.

All systems and their associated situations are reducible to a subset of systems and situations. This is also true for cognitive and situational factors affecting STS-related SA (e.g. technical competence allows for deeper SA in cyber systems, which at the extremes are reducible to the quantum level). In addition to being practically infeasible, trying to account for all systems/situations may cause loss of predictive power if the conclusion is that 'everything influences everything'. Operating from a purposefully limited set of systematic or situational elements while preserving complexity when incorporating gamification elements in training is ideal.

Knowing about HMSA may reveal when and how to adapt cognitive strategies to achieve communication goals. However, expecting cyber defense personnel to acquire deep knowledge of-, and to consciously apply- the various psychological constructs associated with all levels of HMSA is hardly neuroergonomic in training if this information is too condensed. Thus, requirements for knowledge-complexity at each level of difficulty in gamification-based training should be reduced to the minimum level needed for a) training adaptive cognitive agility to ensure mission success (Hutton et al., 2020; Ward et al., 2018), and b) easily allowing difficulty modifications according to trainee expertise to sustain motivation and engagement. Adapting the theoretical elements implicated in HMSA to a format that is practical and applicable for gamification can be challenging. An intuitive and simplified framework for identifying the cognitive processes required for achieving and utilizing SA at each context-dependent level may be required.

Communicating the RCP: The Hybrid Space framework and the Orient, Locate, Bridge process

The Hybrid Space (HS) framework (Figure 3, a) was proposed to readily illustrate the interconnectedness between the cyber and physical domains, and the tension between strategic and tactical goals in decision-making and action during defensive cyber operations (Jøsok et al., 2016). The HS framework can be used to understand the cognitive efforts implied in flexible context-shifting in the STS and how it relates to HMSA (Figure 3, b). Resulting from the cognitive challenges associated with context shifting, the HS shows how communication can get increasingly complex when relayed between agents that are located in different quadrants of the HS (Figure 3, c-d). Complexity can occur due to differences in priorities, workloads, and competencies (e.g. between a CyO that is oriented towards the cyber domain and decision-maker who is oriented towards action in the physical domain). Achieving HMSA for RCP communication requires knowledge of your own competencies and associated mental states, how they differ from your communication partner, and how to adjust Communication Style and message content (Knox et al., 2018). Communication across the HS between different individuals will thus require constant re-adjustment of message content and Communication Style, depending on who the communicated information is intended for (Knox et al., 2018).

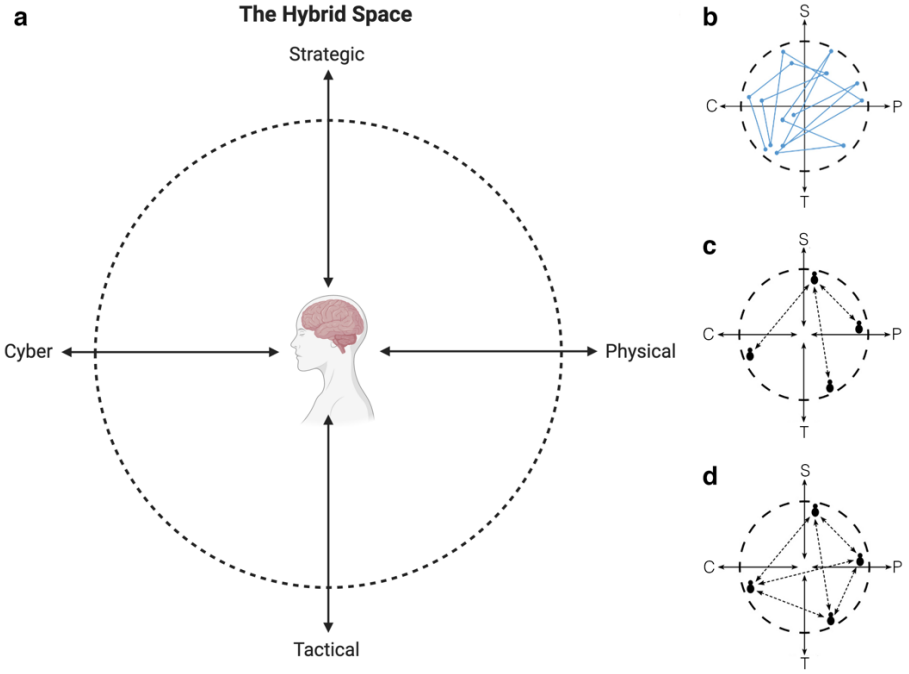

Figure 3: a The Hybrid Space framework (Jøsok et al., 2016, 2017). **b** Cognitive agility. **c** Hierarchical structure, complicated relations. **d** Hierarchical structure, complex relations. C = Cyber. S = Strategic. P = Physical. T = Tactical. Figure taken from (Ask et al., 2021b).

Based on the HS framework, an *Orient, Locate and Bridge* (OLB) model (Figure 4) was introduced to support socio-technical communication in cyber education (Knox et al., 2018).

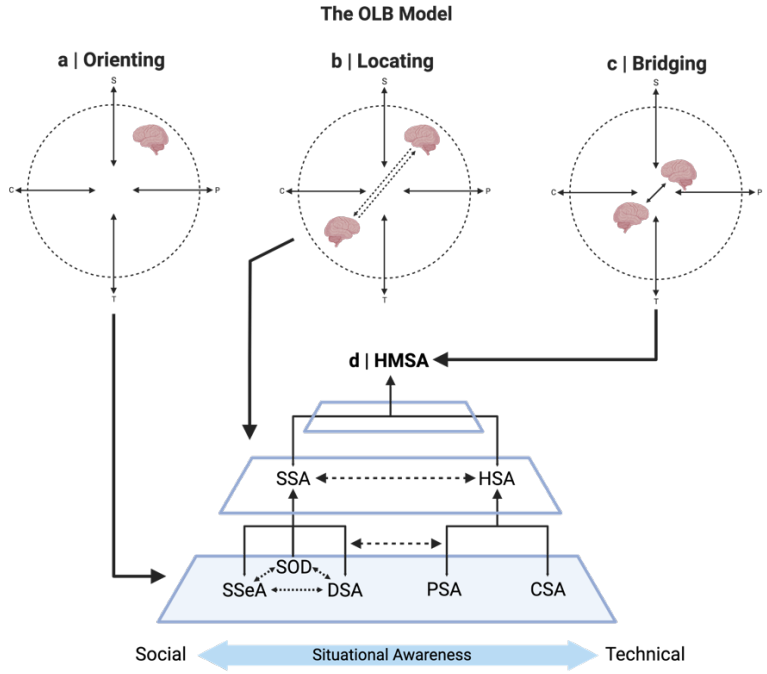

Figure 4: a-c The OLB model as a process of communicating across the Hybrid Space (Knox et al., 2018). **d** Each consecutive step in the OLB process is associated with SA at increasing levels in the HMSA hierarchy. S = strategic, T = tactical, P = physical, C = cyber. HMSA = Hierarchical Meta-Situational Awareness. SSA = Social Situational Awareness. HSA = Hybrid Situational Awareness. SOD = Self-Other Distinction. SSeA = Situational Self-Awareness. DSA = Dispositional Self-Awareness. PSA = Physical Situational Awareness. CSA = Cyber Situational Awareness. Figure created with BioRender.com.

The OLB model came from a cognitive engineering approach applied to communication activities in cyber defense, and describes the steps needed to achieve the HMSA needed for situation-specific successful communication in the HS. The model argues that communication partners attempting to co-construct a shared mental model should apply specific techniques to boost their shared CSA (Knox et al., 2018), which includes information-processing resources such as working memory, cognitive flexibility, Meta-Cognitive Awareness, and Perspective Taking (Morrow & Fischer, 2013).

In the context of HMSA for RCP communication, the *Orient* stage entails applying Meta-Cognitive Awareness to observe one's own internal states and location in the HS (e.g. orientation towards cyber), including how one's own CSA is organized in knowledge structures (Level 1 HMSA). The *Locate* stage entails using Perspective Taking to locate a communication partner in the HS (e.g. towards physical domain), including how their level of technical expertise differs from one's own, as well as their information needs, workload, goals, and priorities (Level 2 HMSA). The *Bridge* stage includes integrating the information from stage 1 and 2 (Level 3 HMSA) to regulate one's own cognitions and shape the flow and content of communication such that a shared CSA and mental models can be achieved (Knox et al., 2018). These and other cognitive skills and processes relevant for the OLB process will be discussed in more detail below under the 'Operationalization of Communicating the RCP'-section.

The Norwegian Defense Cyber Academy has taught and applied the OLB process to enhance future CyOs' communication skills. The OLB model argues that OLB processes can support improved dyadic and multi-domain grounded communication, better regulatory behavior, and cross cultural communication (Knox et al., 2018). To do this though, there is a requirement that participants are willing to engage in cognitively tough activities that require trainers to develop methods for conditioning, expectancies, goal-setting, and ensuring participant self-determination. These are psychological theories that have been found to be highly relevant to gamification (Landers et al., 2015; Landers 2014). Therefore, self-monitoring and self-regulatory processes that add to the already existing cognitive workload, and which require additional efforts to overcome existing habits, could be helped by gamification.

The OLB process helps in creating shared CSA through interdependent communication that helps solidify the Team SA as described by the Team SA Model (Endsley & Jones, 2001). This is done through four processes (Team SA requirements, devices, mechanisms, processes). Firstly, the CyOs are required to share their understanding and communicate information that is necessary (i.e. assessments and projections) for the team, and relaying information and updating task conditions and capabilities through communication devices (technical aspects) and modalities (verbal, non-verbal). This relies upon team members possessing shared mental models to assist in interpretation and creating prediction models. This is imperative for efficient communication and coordination of team members. Finally, Team SA is dependent on processes that require active engagement from team members that includes checking team performance, giving critical feedback, and being active in prioritizing and coordinating tasks,

and planning for multiple outcomes. Thus, Team SA model-associated processes can be facilitated in gamification by incorporating the OLB model.

Gamification Support to the OLB Process

Gamification can be utilized as a tool to unlock communication potential as it promotes higher levels of engagement, behavioral changes and stimulated innovation (Owen, 2017). In a military training context, inspiration can be drawn from the US Navy who implemented elements of game design, such as comprehensive narrative and varied feedback mechanisms, to great effect in a Flooding Control Trainer for recruit training. The reported results included a 50% decrease in decision-making errors, up to an 80% decrease in communication errors and SA improved by 50% (Hussain, 2009). Similar applied interventions that endeavor to scaffold and support the cognitive needs of junior and senior cyber-military personnel involved in defensive cyberspace operations could encourage engagement in mutually beneficial actions. Gamification-based training could include gamification elements aimed at getting participants to know themselves better for improved self-orientation in hybrid environments (Jøsok et al., 2016), Perspective Taking in order to locate and adapt to a communication partners' strengths or susceptibilities in order to bridge for grounded communication (Knox et al., 2018).

The OLB model describes the efficient communication of RCPs as a process requiring the engagement of conscious cognitive efforts, i.e., it comes with an increased cognitive workload. Perspective-taking and meta-cognition in a hybrid-space setting characterized by the need of cognitive agility pose particularly high cognitive demands, notwithstanding potential situational stress factors, and demand resource-intensive "cognitive readiness" (Fletcher, 2004). Particularly in highly complex situations (cognitive load) or particularly eventless periods of time (vigilance), self-regulatory skills are required to keep up the attentional levels needed for the pursuit of communicative tasks. Self-Regulation is highly motivation-dependent (Baumeister & Vohs, 2007), and social interaction requires cognitive processes draining motivational and self-regulatory resources (Finkel et al., 2006). Gamification has been shown to have enormous capabilities regarding the enhancement and maintenance of motivation and thus performance in highly demanding tasks (Sailer et al., 2013).

Effective communication in defensive cyberspace operations demands perspective-taking skills among communicating partners if they are to understand others' information needs and task demands in the form of mental workload. This Perspective Taking is influenced by momentary cognitive states and susceptibilities requiring communication partners to have developed Meta-Cognitive Awareness. When both partners' mental models are synchronously constructed this can support shared consciousness, and increased engagement leading to empowered execution (McChrystal, Collins, Fussell, & Silverman, 2015). One of the key goals of gamification is to increase 'engagement'. Therefore, by gamifying an OLB training programme designed to encourage shared mental models for increased engagement, it is possible that objective measures such as a) Perspective Taking, b) Communication Styles c) improved meta-cognition, and d) self-determination can be accelerated. This intervention targets the development of

specific psychological variables and uses them as tools to improve learning outcomes in dyadic communication scenarios.

The goal of this training intervention is to use gamification elements to improve human-to-human interaction. Thereby helping to ensure the accurate communication of RCPs and thus reduce security risks related to the human factor in cyber defense. For example: for a CyO to orient a peer, or someone in the hierarchical chain, with or without technical expertise, it will involve preparing and communicating the RCP. This communication should accurately present the severity and potential known or unknown consequences of the cyber situation and its impact upon mission assurance.

The game mechanics incorporated in this training intervention include: narrative, points, feedback, judgement of self, and dynamic difficulty adjustment:

- In this intervention, the Cyber-Task scenario will deliver the *Narrative* and is able to tie together the hybrid components of the task. The RCP is the visual or cognitive representation of cyber related incidents and activities tied to the mission. From a gamification perspective, understanding the RCP as a narrative opens space for it to be gamified in training environments.
- *Points* are given depending on objective or inter-subjective performance ratings conducted in real-time or with short delays.
- *Feedback* is given by game-partners (communication partners) and expert-judges. Score changes are immediately evident at the beginning of each new game cycle (i.e., communicative challenge).
- *Judgement of Self* (meta-cognition) is done via comparison of performance prediction and retrospective performance assessment, both in relation to external inter-subjective expert-ratings. Meta-cognitive accuracy is rewarded by points, irrespective of the task. The participant is rewarded for accurate recognition of their own performance.
- *Dynamic Difficulty Adjustment* (use of feedback loops to balance play) is incorporated as the communication partner can anticipate the abilities of the operator (and vice versa), read behaviors and make adjustments accordingly. This is incorporated to ensure that the game can be shaped so that each player has an optimal experience thus ensuring no loss of agency (Salen et al., 2004).

Operationalization of Communicating the RCP

To remain consistent with the theory presented in the OLB process (Figure 4), the following five individual traits that were identified will be measured: (1 Meta-Cognitive Awareness, (2 Perspective Taking, (3 Communication Styles, (4 Self-Regulation, (5 Motivational structures.

Meta-Cognitive Awareness

Meta-cognition refers to ‘thinking about thinking’ and includes the components knowledge of one’s abilities, SA, and behavioral regulation strategies. Individuals with high meta-cognitive

skills have more accurate and confident judgment of their own performance in relation to task demands and are better able to accurately describe their strengths, weaknesses, and their potential to improve. Meta-cognition is considered as having two dimensions: Meta-Cognitive Awareness and meta-cognitive regulation. Meta-cognition is necessary in all three phases of the OLB model. However, it was identified as a prerequisite for the *Orient* phase as an individual is required to have "awareness of factors influencing one's momentary mental state and ongoing cognitive processes" (Knox et al., 2018; 353).

Perspective Taking

Perspective Taking describes the tendency to spontaneously adopt the psychological point of view of others. This Perspective Taking is required to co-construct a shared mental model with communication partners and constitutes the *Locate* in the OLB model. This requires the operator to identify the communication partner in the STS, gaining information of the other person's SA by reflecting over their level of knowledge, skills, ability, and current mental state. Perspective taking can be manipulated through experimentation. By initially assessing levels of perspective taking, then passing incomplete information to participants and testing outcomes, and by qualitatively manipulating the information of participants (i.e. nonverbal vs. verbal; proximity: live vs. cyber).

Communication Styles

Communication skill is crucial to transfer of knowledge, and for decision-making. This skill, or skills, constitute the *Bridge* aspect in the OLB process. While meta-cognition relates to domain and skill knowledge, understanding how specific Communication Styles influence other participants could have great impact on decision-making in peers or command structures. This includes expressiveness and preciseness of communications, emotionality of the message, or using manipulation in communication. Communication can be manipulated at different levels during experimentation.

Self-Regulation

As a related concept to meta-cognition, Self-Regulation (SR) serves to regulate cognition. SR is defined as the regulation of cognition, emotions, behavior, and environment (Efklides, 2008). SR has been shown to contribute to performance across varying domains, particularly in sport (Toering et al., 2009) and academic achievement (Zimmerman, 1990).

Motivational structure (intrinsic/extrinsic)

Motivation is defined as 'a driving force responsible for the initiation, persistence, direction, and vigor of goal-directed behavior (Coleman, 2003), and includes the biological and achievement needs. Recent theories have been developed to include other aspects of motivation, intrinsic as well as extrinsic factors, and situational factors and is referred to as an 'organismic'

approach where individuals are involved proactively with their environment and feel connectedness, competence and autonomy (Deci & Ryan, 1985; Vallerand, 2007; Vallerand et al., 1987; Vallerand & Losier, 1999).

Design of an OLB-Based Gamification Approach to RCP Communication

In this section, we will use the information discussed in the previous sections to propose an OLB-based gamification approach (Figure 5) to RCP communication in STSs. The aim is to foster the (meta-)cognitive skills required for achieving HMSA to improve communication for CSA and Shared Mental Models.

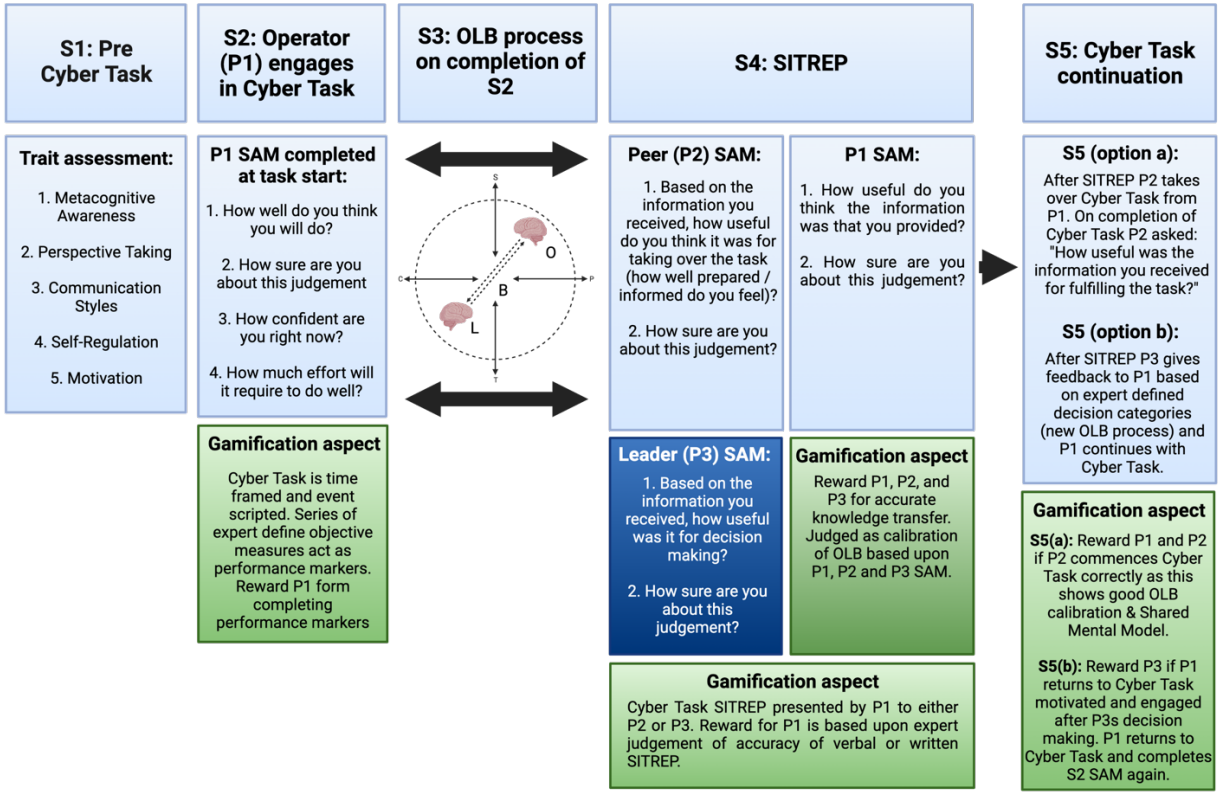

Figure 5: Step 1-5 of the game design (blue) including the gamification aspects (green). S1 will be done with validated questionnaires: e.g. MCAI (Schraw & Dennison, 1994), SRQ (Aubrey et al., 1994), REQ (Gross & John, 2003), IRI (Davis, 1983), CIS (de Vries et al., 2013), SIMS (Guay et al., 2002). S = Step (1-5). P = Participant (1, 2 & 3). SAM: Self-Assessment Mannequin (judgement of self; performance predictions and retrospective performance assessment). SITREP = Situational report. OLB = Orient, Locate, Bridge.

Step 1 (S1): Pre Cyber Task

Prior to the start of the intervention all participants complete a battery of trait questionnaires. The questionnaires assess traits influencing communication and decision-making styles with relatively high stability over time and situations. Amongst others, these questionnaires assess the operators' cognitive problem-solving style, ability to take others' perspective, belief in own capabilities, and typical Communication Styles. These trait variables have the potential to assist

with the interpretation of quantitative empirical findings and can potentially flag individuals with sub-optimal communication style, or more outlying trait tendencies.

Gamification mechanics: In Step 1 there are no gamification mechanics.

Step 2 (S2): Operator (P1) engages in Cyber Task

A collection of scenario based Cyber-Tasks with a variety of technical difficulty levels can be retrieved from a cyber range scenario database and implemented. The Cyber-Tasks are randomly allocated to cyber operator participants. There will be 'balancing' to match participant competence levels. The interdependent Cyber-Tasks are solved by a (single) CyO and involve processes such as penetration testing, attack / defense, capture-the-flag, malware forensics, and incident response. Before the CyO (P1) commences the Cyber Task he/she will answer a SAM relating to performance prediction/judgement of self.

Gamification mechanics: The initial *Judgement of Self* (SAM) occurs in this step as a performance prediction. However, points are awarded in S4 after the retrospective SAM. *Points* are awarded for Cyber-Task performance based on expert defined performance measures. In S2 the players are introduced to the *Narrative.*

Step 3 (S3): OLB process on completion of S2

After completing (coming as far as possible) the Cyber-Tasks within the designated time-frame, there is a requirement for dyadic communication. The RCP must be reported by the CyO (P1) following the OLB logic consisting of a perspective-taking adjustment of the given technical information under consideration of the psychosocial, tactical, strategic, and cyber-physical situational needs of the recipient. The information conveyed in Step 3 can be in verbal or written modality and constitutes a situational report (SITREP).

Gamification mechanics: the cognitive processes occurring during the OLB process are key functions to defining the outcome for the participants. As such, OLB supports and shapes the *Narrative*, and can be seen as a game component just without tangible reward. The reward comes in the form of *Points*, *Feedback* and *Judgement of Self* in S4.

Step 4 (S4): SITREP

The quality of the exchanged information will be assessed via quantitative and qualitative analysis of the exchanged SITREP by experts, including P1 or P3s perceived usefulness of the RCP as a reflection of the performance of the sender. There are two types of recipients of the SITREP:

- a peer-operator (P2) simulating a handover of tasks amongst equals, and
- a higher-ranking non/less-technical decision-maker (P3).

Gamification mechanics: S4 has three game mechanics: *Points*, *Narrative,* and *Expert Feedback.*

Step 5 (S5): Cyber Task continuation

The recipient (P2/P3) must also follow OLB logic. Depending on the desired goal of each intervention the recipient may be a participant in the experiment, or placed into the scenario as a manipulation (see Table 1).

a) Recipient as peer-operator (P2) participant: P2 task performance will be analyzed in context with the quality markers of the previous OLB-outcome (the expert SITREP analysis from S4) along with assessing the subjective benefits from the received SITREP (Self-Efficacy and entitlement to judge) for the subsequent task (assessed before and after engaging with the task).

b) Recipient as higher-ranking less/non-technical leader/decision-maker (P3) participant: P3 perceived SA and entitlement to judge will be assessed along with the leader's decision made in response to the SITREP. This response will be evaluated and scored for quality and degree of goal achievement (as defined by the guidelines of the scripted scenario).

Following the making of a (recorded) decision, P3 engages with the CyO and provides instructions and feedback regarding the work done and gives advice on future action (simulating that the same CyO (P1) would continue the task). This feedback will then be rated by P1 (who is the creator of the SITREP, but also receiver of the feedback).

Gamification mechanics: this final step involves *Points, Feedback, Narrative* and *Judgement of Self.*

HUMAN FACTOR (P1 manipulations)	**HUMAN FACTOR (P2 and P3 manipulations)**	**SITUATIONAL CONTEXT**
Time pressure	Conflicting information	Task demands/complex
Performance pressure	Expertise and pre-existing knowledge	Detrimentality of environmental conditions
Stress level / working memory load	Stress level / working memory load	Organisational deficit in cyber domain cognizance

Table 1. Dyadic factors for shared RCP: Manipulations (independent variables)

These independent variables represent several possibilities to choose from.

Step representation of gamification can be found in Table 2.

STEP (S)	APPROACH	SCORING
S1 (before)	Players are unaware of any conditioning and scoring but are shown a live scoreboard that is always present in players view (rankings manipulated by experimenters) but are told that a 'Champion' is declared at the end and their scores entered in database.	
S2	Completion of Cyber Task in technical terms.	(0-100 points, based on expert judgments' assessment of completion/advancement).
	Time pressure: Each task has several milestones.	For each milestone achieved players are rewarded with 10 points
	Working memory load (1-5 multiplier) Increased information through performance achievements (performance-related staircase algorithm).	
S3 & 4	Accurate transfer of knowledge.	Judged by observer (expert) on objective measures (max 100 points).
		Self–judgements of performance and meta-cognitive accuracy (controlled with self-assessments: S1 & S4) (-100 to 100 points).
S5	Reward OLB	(Max 100 points)
Extra Gamification aspect	Risk Taking	After judgement of performance from previous 4 rounds, P1 asked if he/she wants to cut time for more points (public ranking). (weighted scores x 100 points).

Table 2. Representation of the different steps in the gamified OLB process

SUMMARY

Communication efficiency is a crucial human factor in cyber defense and therefore a risk factor. The goal of human-to-human communication in cyber threat situations is to achieve a shared SA so that cyber defense decisions are based on having accurate information. RCPs are used to describe the actual circumstances of a cyber incident and are often communicated from technical to non/less-technical personnel. Formulating and communicating the RCP requires deliberate application of cognitive skills to integrate SA from both technical and social domains in the STS such that RCPs are actionable to the recipient. Currently there is some research, but

so far nothing has been applied in formal cyber defense education and training scenarios. Existing research models for efficient communication in cyber context, such as the OLB model, imply a high degree of self-regulation to avoid suboptimal performance between communicating partners. One of the best ways to increase self-regulation is to maximize motivation, and gamification is known to be a good neuroergonomic way to motivate, and may thus improve cyber defense performance through better modes of communication. This proposal suggests an intervention design for a peer-to-peer- and peer-to-rank dyadic communication situation that could be facilitated by a cyber range capability for training military personnel (and the wider cyber defense community).[1] It includes the gamification elements of a) narrative, b) scoring c) feedback d) judgment of self. Implementation should provide empirical data for further modification and validation.

Funding

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

[1] The Norwegian Cyber Range (NCR) is an arena for cybersecurity testing, training, and exercises: https://www.ntnu.no/ncr

References

Aubrey, L. L., Brown, J. M., & Miller, W. R. (1994). Psychometric properties of a selfregulation questionnaire (SRQ). *Alcohol. Clin. Exp. Res., 18*(2), 420–525.

Agyepong, E., et al. (2020). Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, *4*(3), 1- 28. DOI: 10.1080/23742917.2019.1698178

Ask, T. F., Lugo, R. G., Knox, B. J., & Sütterlin, S. (2021a). Human-human communication in cyber threat situations: A systematic review. In C. Stephanidis et al. (Eds.), *HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning, and Culture. HCII 2021. Lecture Notes in Computer Science*, 13096. Springer, Cham. https://doi.org/10.1007/978-3-030-90328-2_2

Ask, T. F., Sütterlin, S., Knox, B. J., & Lugo R. G. (2021b). Situational states influence on team workload demands in cyber defense exercise. In C. Stephanidis et al. (Eds.), *HCI International 2021 - Late Breaking Papers: Cognition, Inclusion, Learning, and Culture. HCII 2021. Lecture Notes in Computer Science*, 13096. Springer, Cham. https://doi.org/10.1007/978-3-030-90328-2_1

Barford, P., et al. (2009). Cyber SA: Situational awareness for cyber defense. *Cyber Situational Awareness*, 3–13. Doi:10.1007/978-1-4419-0140-8_1

Baumeister, R. F., & Vohs, K. D. (2007). Self-regulation, ego depletion, and motivation. *Social and personality psychology compass*, *1*(1), 115-128.

Cheng, Y., Zhang, Y., Wang, F., Jia, G., Zhou, J., Shan, Y., Sun, X., Yu, L., Merzenich, M. M., Recanzone, G. H., Yang, L., & Zhou, X. (2020). Reversal of age-related changes in cortical sound-azimuth selectivity with training. *Cereb Cortex*., *30*(3), 1768-1778. doi: 10.1093/cercor/bhz201.

Cowley, B., Charles, D., Black, M., & Hickey, R. (2008). Toward an understanding of flow in video games. *Computers in Entertainment*, *6*(2), 1. doi:10.1145/1371216.1371223

Crilly, M. (2021). Warfare in the post digital era. *Wavell Room: Contemporary British Military Thought.* Retrieved from: https://wavellroom.com/2021/10/05/warfare-in-the-post-digital-era/

Davis, M. H. (1983). Measuring individual differences in empathy: Evidence for a multidimensional approach. *Journal of Personality and Social Psychology, 44*(1), 113–126. https://doi.org/10.1037/0022-3514.44.1.113

de Vries, R. E., Bakker-Pieper, A., Konings, F. E., & Schouten, B. (2013). The communication styles inventory (CSI) a six-dimensional behavioral model of communication styles and its relation with personality. *Communication Research*, *40*(4), 506-532.

Deci, E. L., & Ryan, R. M. (1985). The general causality orientations scale: Self-determination in personality. *Journal of research in personality*, *19*(2), 109-134.

Dostal, B. C. (2007). Enhancing situational understanding through the employment of unmanned aerial vehicles. *Army Transformation Taking Shape ...Interim Brigade Combat Team Newsletter*, No. 01–18.

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

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. *Proceedings of the Human Factors Society annual meeting,* 32(2), 97-101.

Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Human factors*, *37*(1), 65-84.

Endsley, M. R. (2019). The divergence of objective and subjective situation awareness: A meta-analysis. *Journal of Cognitive Engineering and Decision Making, 155534341987424.* doi:10.1177/1555343419874248

Endsley, M. R. & Jones, W. M. (2001). A model of inter- and intrateam situation awareness: Implications for design, training and measurement. In M. McNeese, E. Salas & M. Endsley (Eds.), *New trends in cooperative activities: Understanding system dynamics in complex environments*. Santa Monica, CA: Human Factors and Ergonomics Society.

ENISA. (2018). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. *WP2018 O.3.3.2.*, 1-34. DOI: 10.2824/324042

Fenigstein, A., Scheier, M. F., & Buss, A. H. (1975). Public and private self-consciousness: Assessment and theory. *Journal of Counselling and Clinical Psychology*, *43*(4), 522–527. Doi: 10.1037/h0076760

Finkel, E. J., Campbell, W. K., Brunell, A. B., Dalton, A. N., Scarbeck, S. J., & Chartrand, T. L. (2006). High-maintenance interaction: Inefficient social coordination impairs self-regulation. *Journal of personality and social psychology*, *91*(3), 456.

Fitton, O. (2016). Cyber operations and gray zones: Challenges for NATO. *Connections: TQJ, 15*(2), 109-119.

Fletcher, J. D. (2004). *Cognitive readiness: Preparing for the unexpected*. Defence Technical Information Center, Institute for Defense Analysis. Alexandra, VA. Retrieved from: https://apps.dtic.mil/docs/citations/ADA458683.

Gardner, F. (2021, December 30). *What does future warfare look like? It's here already*. Retrieved from https://www.bbc.com/news/world-59755100

Gee, J. P. (2003). What video games have to teach us about learning and literacy. *Computers in Entertainment (CIE)*, *1*(1), 20-20.

Gross, J. J., & John, O. P. (2003). Individual differences in two emotion regulation processes: Implications for affect, relationships, and well-being. *Journal of Personality and Social Psychology*, *85*, 348-362.

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

Harter, J. K., Schmidt, F. L., Killham, E. A., & Agrawal, S. (2009). *Q12 meta-analysis: The relationship between engagement at work and organizational outcomes*. Omaha, NE: Gallup.

House of Commons. (2017). *Public administration and constitutional affairs committee. Lessons learned from the EU Referendum.* (Twelfth Report of Session 2016-2017). Retrieved from: https://publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/496.pdf

Howard-Jones, P. A., & Demetriou, S. (2009). Uncertainty and engagement with learning games. *Instruct. Sci., 37*, 519–536. 10.1007/s11251-008-9073-6

Howard-Jones, P. A., Jay, T., Mason, A., & Jones, H. (2016). Gamification of learning deactivates the default mode network. *Frontiers in psychology*, *6*, 1891. https://doi.org/10.3389/fpsyg.2015.01891

Hussain, T. S., Roberts, B., Menaker, E. S., Coleman, S. L., Centreville, V. A., Pounds, K., ... & Lee, J. (2009). Designing and developing effective training games for the US Navy. *The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC)*, *1*.

Hutton, R., Turner, P., & Jones, M. (2020, February 18). Cognitive agility & the thinking approach space. *Wavell Room: Contemporary British Military Thought*. Retrieved from: https://wavellroom.com/2020/02/18/cognitive-agility-the-thinking-approach-space/

Johnsen, R. (2019). *Cyber defence tactics. Defending our way of living, part II: Operations and Tactics*. IMT4213, NTNU.

Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., & Ward, P. (2016). Exploring the hybrid space. *International Conference on Augmented Cognition*, 178-188.

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: Schmorrow, D.D., Fidopiastis, C.M. (Eds.), *AC 2017. LNCS (LNAI)*, *10285*, 486–500. Springer, Cham. https://doi.org/10.1007/978-3-319-58625-0_35

Khoshnoud, S., Alvarez Igarzábal, F., & Wittmann, M. (2020). Peripheral-physiological and neural correlates of the flow experience while playing video games: a comprehensive review. *PeerJ, 8*, e10520. https://doi.org/10.7717/peerj.10520

Klein, G., Moon, B., & Hoffman, R. R. (2006). Making sense of sensemaking 1: Alternative perspectives. *IEEE Intelligent Systems*. *21*(4), 70–73. doi:10.1109/mis.2006.75

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.

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.), *HCI 2017. CCIS*, *713*, 330–338. Springer, Cham. https://doi.org/10.1007/978-3-319-58750-9_46

Kola, I., Jonker, C. M., & van Riemsdijk M. B. (2020). Who's That? - Social situation awareness for behaviour support agents. In L. Dennis, R. Bordini, & Y. Lespérance (Eds.), *Engineering Multi-Agent Systems. EMAS 2019. Lecture Notes in Computer Science*, *12058*. Springer, Cham. https://doi.org/10.1007/978-3-030-51417-4_7

Landers, R. N., Bauer, K. N., Callan, R. C., & Armstrong M. B. (2015). Psychological theory and the gamification of learning. In T. Reiners, & L. Wood (Eds), *Gamification in Education and Business*, 165-186, Springer, Cham.

Landers, R. N. (2014). Developing a theory of gamified learning: Linking serious games and gamification of learning. *Simulation & Gaming*, *45*(6), 752–768.

Lorenz, R. C., Gleich, T., Gallinat, J., & Kühn, S. (2015). Video game training and the reward system. *Frontiers in human neuroscience*, *9*, 40. https://doi.org/10.3389/fnhum.2015.00040

McChrystal, S. A., Collins, T., Fussell, C., & Silverman, D. (2015). *Team of teams: New rules of engagement for a complex world*. New York, NY: Penguin.

McMahon, C. (2020). In defence of the human factor. *Frontiers in Psychology*, *11*, 1390.

Michailidis, L., Balaguer-Ballester, E., & He, X. (2018). Flow and immersion in video games: The aftermath of a conceptual challenge. *Frontiers in Psychology*, *9*. doi:10.3389/fpsyg.2018.01682

NATO Cooperative Cyber Defense Centre of Excellence. (2016, July 9). NATO Recognizes cyberspace as a 'domain of operations' at Warsaw summit. *CCDCOE*. Retrieved from: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Ong, M. (2013). *Gamification and its effect on employee engagement and performance in a perceptual diagnosis task* (Master thesis, University of Canterbury, New Zealand). DOI: http://dx.doi.org/10.26021/5866

Owen, P. (2017). *How gamification can help your business engage in sustainability*. London England: Routledge. DOI: 10.4324/9781351275606

Recanzone, G. H., Merzenich, M. M., Jenkins, W. M., Grajski, K. A., & Dinse, H. R. (1992a). Topographic reorganization of the hand representation in cortical area 3b owl monkeys trained in a frequency-discrimination task. *J Neurophysio*l., *67*(5), 1031-56. doi: 10.1152/jn.1992.67.5.1031.

Recanzone, G. H., Merzenich, M. M., & Schreiner, C. E. (1992b). Changes in the distributed temporal response properties of SI cortical neurons reflect improvements in performance on a temporally based tactile discrimination task. *J Neurophysiol*., 67(5), 1071-91. doi: 10.1152/jn.1992.67.5.1071.

Recanzone, G. H., Schreiner, C. E., & Merzenich, M. M. (1993). Plasticity in the frequency representation of primary auditory cortex following discrimination training in adult owl monkeys. *J Neurosci*., 13(1), 87-103. doi: 10.1523/JNEUROSCI.13-01-00087.1993.

Rodrigues, L. F., Oliveira, A., & Rodrigues, H. (2019). Main gamification concepts: A systematic mapping study. *Heliyon*, *5*(7), e01993. https://doi.org/10.1016/j.heliyon.2019.e01993

Rosen, M. A., Fiore, S. M., Salas, E., Letsky, M., & Warner, N. (2008). Tightly coupling cognition: Understanding how communication and awareness drive coordination in teams. *International Journal of Command and Control*, *2*(1), 1–30.

Sailer, M., Hense, J., Mandl, J., & Klevers, M. (2013). Psychological perspectives on motivation through gamification. *Interaction Design and Architecture Journal*, (19), 28-37.

Salen, K., Tekinbaş, K. S., & Zimmerman, E. (2004). *Rules of play: Game design fundamentals*. MA, Cambridge: MIT press.

Schauer, S., Rainer, B., Museux, N., Faure, D., Hingant, J., Rodrigo, F. J. C., … & Lopez, S. Z. (2018). Conceptual framework for hybrid situational awareness in critical port infrastructures. *Lecture Notes in Computer Science*, 191–203. doi:10.1007/978-3-030-05849-4_15

Schraw, G., & Dennison, R. S. (1994). Assessing metacognitive awareness. *Contemp. Educ. Psychol.*, *19*(4), 460–475.

Sethumadhavan, A. (2011). Knowing what you know: The role of meta-situation awareness in predicting situation awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 55(1),* 360–364. doi:10.1177/1071181311551074

Silvia, P. J., & Duval, T. S. (2001). Objective self-awareness theory: recent progress and enduring problems. *Personality and Social Psychology Review*, *5*(3), 230–241. 10.1207/S15327957PSPR0503_4

Guay, F., Vallerand, R., & Blanchard, C. (2000). On the assessment of situational intrinsic and extrinsic motivation: The Situational Motivation Scale (SIMS). *Motivation and Emotion*, *24*, 175–213. doi:10.1023/A:1005614228250

Staheli, D., et al. (2016). Collaborative data analysis and discovery for cyber security. *Proceedings of the 12th Symposium on Usable Privacy and Security* (*SOUPS 2016): Twelfth Symposium on Usable Privacy and Security*. Denver, CO.

Steinbeis, N. (2016). The role of self-other distinction in understanding others' mental and emotional states: neurocognitive mechanisms in children and adults. *Philosophical*

transactions of the Royal Society of London. Series B, Biological sciences, *371*(1686), 20150074. https://doi.org/10.1098/rstb.2015.0074

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

TRADOC. (2017). An advanced engagement battlespace. Tactical, operational and strategic implications for the future operational environment. *Mad Scientist Initiative, Small Wars Journal*. Retrieved from: https://smallwarsjournal.com/jrnl/art/advanced-engagement-battlespace-tactical-operational-and-strategic-implications-future

Trapnell, P. D., & Campbell, J. D. (1999). Private self-consciousness and the five-factor model of personality: Distinguishing rumination from reflection. *Journal of Personality and Social Psychology, 76(2), 284–304.* doi:10.1037/0022-3514.76.2.284

Vallerand, R. J. (2007). Intrinsic and extrinsic motivation in sport and physical activity. *Handbook of sport psychology*, *3*, 59-83.

Vallerand, R. J., Deci, E. L., & Ryan, R. M. (1987). 12 intrinsic motivation in sport. *Exercise and sport sciences reviews*, *15*(1), 389-426.

Vallerand, R. J., & Losier, G. F. (1999). An integrative analysis of intrinsic and extrinsic motivation in sport. *Journal of applied sport psychology*, *11*(1), 142-169.

Varga, S., et al. (2018). Information requirements for national level cyber situational awareness. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, *2018*, 774-781, doi: 10.1109/ASONAM.2018.8508410.

Ward, P., Gore, J., Hutton, R., Conway, G. E., & Hoffman, R. R. (2018). Adaptive skill as the conditio sine qua non of expertise. *Journal of applied research in memory and cognition*, *7*(1), 35-50.

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

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

Zanenga, P. (2014). Knowledge eyes: Nature and emergence in society, culture, and economy. *2014 International Conference on Engineering, Technology and Innovation (ICE), 2014*, 1-6, doi: 10.1109/ICE.2014.6871618.