frontiers | Frontiers in Education

TYPE Review
PUBLISHED 20 June 2023
DOI 10.3389/feduc.2023.988043

OPEN ACCESS

EDITED BY
Mohammed Saqr,
University of Eastern Finland, Finland

REVIEWED BY
Hooman Alavizadeh,
The University of Sydney, Australia
Isabel Azevedo,
Polytechnic Institute of Porto, Portugal
Aritran Piplai,
University of Maryland, Baltimore County, United States

*CORRESPONDENCE
Torvald F. Ask
✉ torvaldfask@gmail.com

RECEIVED 06 July 2022
ACCEPTED 31 May 2023
PUBLISHED 20 June 2023

CITATION
Ask TF, Knox BJ, Lugo RG, Hoffmann L and Sütterlin S (2023) Gamification as a neuroergonomic approach to improving interpersonal situational awareness in cyber defense.
Front. Educ. 8:988043.
doi: 10.3389/feduc.2023.988043

Gamification as a neuroergonomic approach to improving interpersonal situational awareness in cyber defense

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

[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, Lillehammer, Norway, [4]Estonian Maritime Academy of Tallinn University of Technology, Tallinn, Estonia, [5]Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany, [6]Centre for Digital Forensics and Cybersecurity, Tallinn University of Technology, Tallinn, Estonia

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, neuroergonomics

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; Masakowski and Blatny, 2023). 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 cybersecurity and cyberspace operations are conducted. In other words, digitalization leads to the expansion of cyberspace and an almost unmanageable cyber threat landscape that places demand 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) 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, cyber operators encounter many challenges spanning the cyber, physical, and social domains. When investigating a cyber threat situation, cyber operators must navigate a technological threat-landscape operating at speeds that often are at odds with innate human cognitive abilities (Zachary and Miller, 2013). The information that can be extracted about the status of cyber threats is subject to high levels of uncertainty. Subsequently, when reporting on cyber threats, cyber operators must select (1) what information to communicate 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). In practice, this means that cyber threat information is filtered by cyber operators before reaching decision-makers and clients (Jøsok et al., 2017) through processes based on how the cyber operators understand their information needs and decision-making priorities (Ahrend et al., 2016; Staheli et al., 2016; Ask et al., 2021a). This process of filtering information in combination with the technical competence of decision-makers serve as potential bottlenecks to successfully communicating critical and actionable cyber threat information (Jøsok et al., 2016, 2017). Good cyber defense decisions are therefore based on human-to-human communication. Inadequate communication has been identified as one of the major challenges facing personnel working within cyber defense (ENISA, 2018; Agyepong et al., 2020). The consequence of inadequate communication is inadequate cyber defense. 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 to training or explaining human behaviors that promote good cyber defense in have arguably been too simplistic to improve cyber defense (ENISA, 2018). Widely established approaches such as awareness campaigns and policy-making 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. For instance, personality models such as the Big 5 and models of behavior such as Theory of Planned Behavior are insufficient when trying to predict cybersecurity outcomes in the workplace, arguably due to ignoring 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; pp. 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. With the exception of very recent suggestions for holistic intervention approaches (Pirta-Dreimane et al., 2022; Schaberreiter et al., 2022), 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 (Zachary and Miller, 2013; Jøsok et al., 2016), 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 information processing-capabilities of the individual 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 in cybersecurity working environments. This makes the case for the application of neuroergonomic approaches, which applies knowledge about the brain in real-world settings (Parasuraman and Rizzo, 2008). Neuroergonomic approaches to training are neuro- and thus user-centric and can be implemented by (1) changing the working environment to fit the cognitive processing capabilities of humans, (2) training specific cognitive capabilities that improves adaptability to the working environment, or (3) a combination of the two. In the context of neuroergonomically improving situational awareness and interpersonal communication for good cyber defense decision-making, both working environment-based interventions (Debashi and Vickers, 2018; Kullman et al., 2018; Ask et al., 2023a) and methods that train a collection of specific human cognitive abilities have been suggested (Knox et al., 2018, 2021; Jøsok et al., 2019). For instance, a 3D mixed reality representation of network topology and activity, at a scale that allows encoding of cyber threat information through the spatial navigation senses, resulted in better dyadic communication and situational understanding during a simulated network attack (Ask et al., 2023a). However, training must be conducted in a sustainable way to ensure lasting changes in behavior (ENISA, 2018).

Gamification methods optimize for sustained and flexible learning (Howard-Jones and 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 (Michailidis et al., 2018; Khoshnoud et al., 2020). This is necessary for continued engagement (Cowley et al., 2008; Howard-Jones et al., 2016) and the neuroplastic changes associated with learning (Recanzone et al., 1992a,b, 1993; Cheng et al., 2020). A recent review suggested that gamification methods may be a promising approach to

improve cybersecurity performance in employees (Sharif and Ameen, 2021). In line with this suggestion, through optimization of focus, information encoding, and learning, we argue that utilizing gamification methods can serve as a neuroergonomic approach for targeting specific cognitive abilities needed for good cyber defense performance while making cyber operators 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 cyber operators 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 (Knox et al., 2018; Ask et al., 2021a) in cyber-hybrid contexts through a process that is neuroergonomically designed to improve engagement and change behavior. While user engagement and motivation is central to all well-applied gamification approaches, the proposed intervention is evidence-based by targeting the training of specific adaptive cognitive skills that has been identified as relevant for communication and performance in cyber threat situations (self-regulation, perspective taking, and metacognition, discussed in later sections; Jøsok et al., 2016, 2017, 2019; Knox et al., 2017, 2018, 2021; Lugo and Sütterlin, 2018; Ask et al., 2021a,b, 2023b; Sütterlin et al., 2022, 2023). This is achieved by incorporating existing approaches designed for communication in cyber threat situations (Knox et al., 2018) that have received neuroergonomic support (Ask et al., 2023b). This separates our approach from other gamification approaches aimed at improving situational awareness and performance in cybersecurity, as they do not explicitly focus on training these cognitive skills (e.g., Fink et al., 2013; Wolfenden, 2019; Qusa and Tarazi, 2021; Sharif and Ameen, 2021; Wu et al., 2021; Brady and M'manga, 2022; Broholm et al., 2022; Jelo and Helebrandt, 2022; Matovu et al., 2022). 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 to human factors research are human cognitive processes and skills 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 (see "the new reality of cyber war" by Farwell and Rohozinski, 2012). 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 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 is becoming increasingly popular as a method for training in cybersecurity-relevant settings (e.g., Fink et al., 2013; Sharif and Ameen, 2021), and 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 (Sailer et al., 2013; Landers et al., 2015) including those that involve incident management across different organizations (Harter et al., 2009), and among students learning about cyberattacks (Matovu et al., 2022). For gamification-based training methods to be efficacious in a threat landscape that is prone to rapid change (e.g., Johnsen, 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; pp. 45). 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, 2019; Knox et al., 2017, 2018; Lugo and Sütterlin, 2018; Sütterlin et al., 2022, 2023; Ask et al., 2023b).

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 (Knox et al., 2018; Ask et al., 2021a). 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, cyber operators must establish a shared situational understanding with decision-makers that may be considered "non-technical." Because a cyber operator'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, cyber operators 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 cyber operators 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 1A). The formal definition for SA is "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). 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 (SA Level 1) 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 (SA Level 2) where previous experiences are integrated with current perceptions to form an understanding of how the current situation is influenced. The third stage (SA Level 3) 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.

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 SA Level 2 (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).

The SA model by Endsley (1988) is the most commonly used model for SA in cybersecurity contexts (Ofte and Katsikas, 2022). Building on the framework of Endsley (1988), seven requirements have been suggested to achieve full Cyber SA (CSA) for cyber defense (Barford et al., 2009). During a cyber threat situation, these requirements can be organized under SA Level 1–3 (Figure 1B):

- SA Level 1 will entail perceiving indicators of compromise: (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.
- SA Level 2 will entail understanding what kind of threat one is faced with based on the indicators of compromise (e.g., if the threat is directed, and whether it is automated): (5) Awareness of why and how the current situation is caused, (6) Awareness of how situations evolve.
- SA Level 3: (7) Assessment of plausible outcomes.

In the original paper (Barford et al., 2009), impact of the attack was originally proposed to be at level two, how situations evolve at level three, and plausible future outcomes at level two. However, the description provided for each criteria suggests that the organization in Figure 1B is more appropriate if arranging them according to what information one would need to possess to achieve each criterion. For instance, impact assessment would in many cases be a precursor to understanding the attack path, thus an information requirement for understanding "why and how the current situation is caused." Assessment of plausible future outcomes is described as the phase where actual predictions are made, while having an awareness about how situations evolve is more about situation tracking, according to Barford et al. (2009). Thus, awareness of how situations evolve would be an information requirement for (hence a precursor to) being able to make predictions at succeeding windows of time.

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

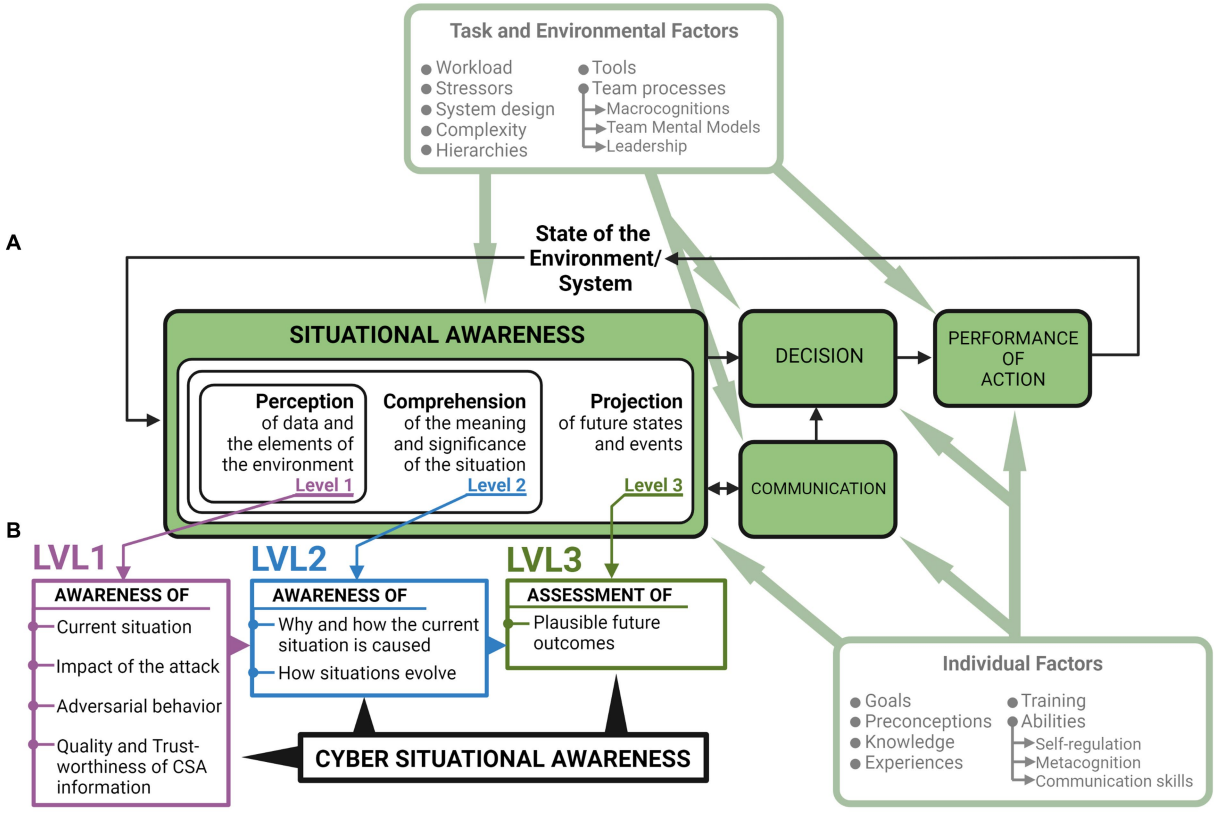

FIGURE 1
Situational awareness and suggested requirements for achieving cyber situational awareness. **(A)** The three stages of situational awareness (Endsley, 1988). "Communication" has been added to the model to account for the separation between analysts and decision-makers in security operation centers (Knox et al., 2018; Ask et al., 2021a). The arrows are bidirectional to indicate that SA influences and is influenced by communication. Figure adapted with modifications from Endsley (1995) and Lankton (2007). **(B)** The seven requirements for cyber situational awareness proposed by Barford et al. (2009). The requirements have been organized under the SA model according to which of them would be prerequisites for progressing through each level of SA. Figure modified from Ask et al. (2023a).

et al., 2018). Thus, a RCP is the visual or cognitive representation of cyber threat-related incidents and activities, which by itself does constitute CSA but is nevertheless an important contributor toward establishing CSA (Alavizadeh et al., 2022). An RCP that is created by a cyber operator and intended for a non/less-technical recipient must therefore be tailored to the recipient to achieve a shared CSA (Ahrend et al., 2016; Staheli et al., 2016).

Organizational structures introduce challenges to RCP communication between cyber operators 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 cyber operators 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 (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 the 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 (Rosen et al., 2008; Knox et al., 2018). 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, cyber operators 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) highlight an area where cyber operators 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). In short, to accurately relay their understanding through appropriate mode, method, and content of communication, cyber operators may have to integrate information from several domains in the STS when communicating RCPs.

Communicating the RCP: the hybrid space framework and the orient, locate, bridge process

The Hybrid Space (HS) framework (Figure 2A) 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 (Figure 2B). 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 (Figures 2C,D). Complexity can occur due to differences in priorities, workloads, and competencies (e.g., between a cyber operator that is oriented towards the cyber domain and a decision-maker who is oriented toward action in the physical domain). Achieving SA 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).

Based on the HS framework, an *Orient, Locate and Bridge* (OLB) model (Figures 2E–G) was introduced to support socio-technical communication in cyber education (Knox et al., 2018). The OLB model came from a cognitive engineering approach applied to communication activities in cyber defense, and describes the steps 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, metacognitive awareness, and perspective taking (Morrow and Fischer, 2013).

In the context of RCP communication, the *Orient* stage entails applying metacognitive awareness to observe one's own internal states and location in the HS (e.g., orientation toward cyber), including how one's own CSA is organized in knowledge structures. The *Locate* stage entails using perspective taking to locate a communication partner in the HS (e.g., toward physical domain), including how their level of technical expertise differs from one's own, as well as their information needs, workload, goals, and priorities. The *Bridge* stage includes integrating the information from OLB stage 1 and 2 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 cyber operators' 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, 2014; Landers et al., 2015). 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 and Jones, 2001). This is done through four processes (Team SA requirements, devices, mechanisms, processes). Firstly, the cyber operators are required to share their understanding and communicate information that is necessary (i.e., assessments and projections) for the team, and relaying

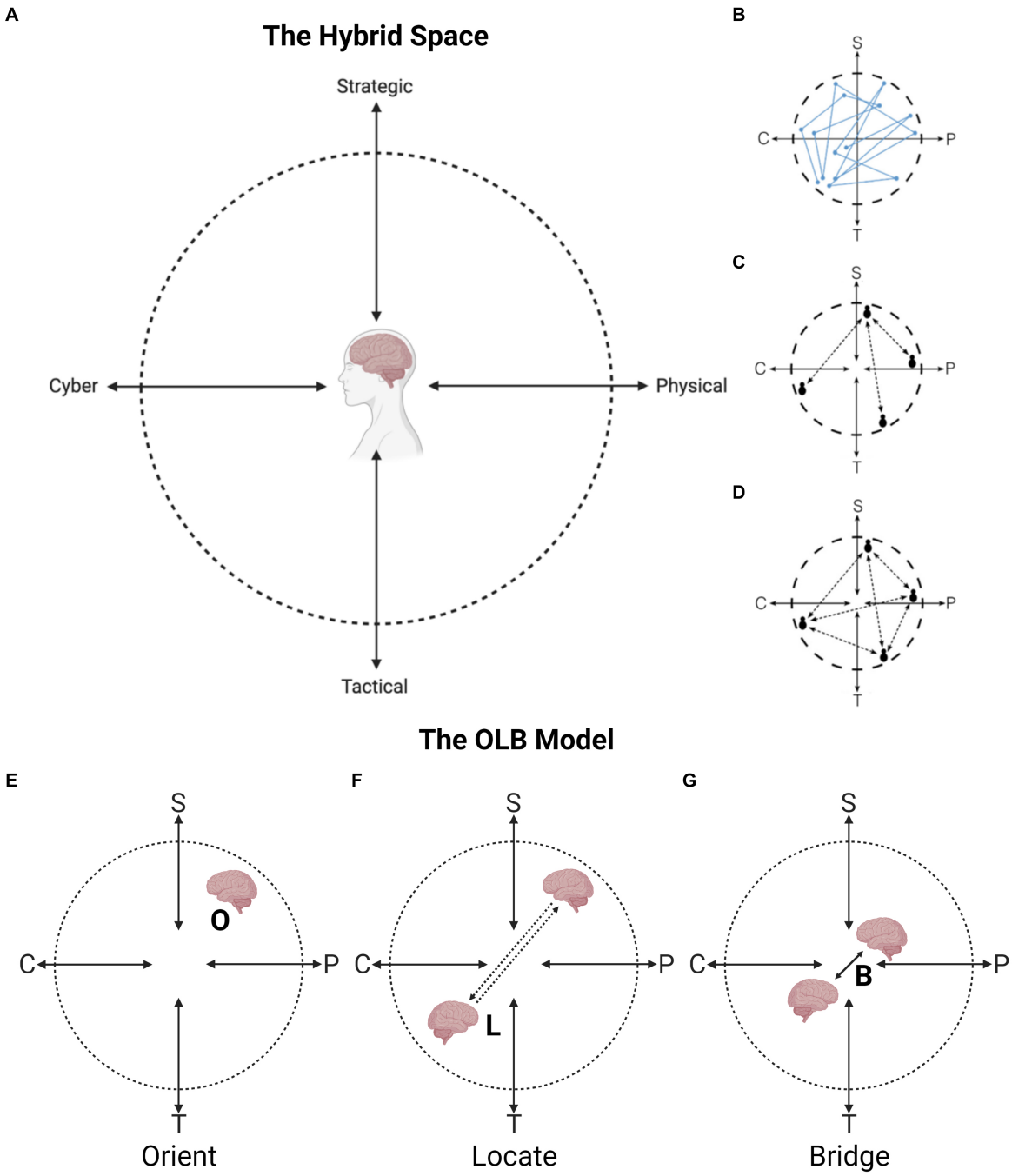

FIGURE 2
(A) The Hybrid Space framework (Jøsok et al., 2016, 2017). **(B)** Cognitive agility. **(C)** Hierarchical structure, complicated relations. **(D)** Hierarchical structure, complex relations. **(E–G)** The Orient, Locate, Bridge model as a process of communicating across the Hybrid Space (Knox et al., 2018). **(E)** Orient. **(F)** Locate. **(G)** Bridge. C=Cyber. S=Strategic. P=Physical. T=Tactical. Figure adapted from Ask et al. (2021a).

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 mechanics should relate to RCP communication. For example: for a cyber operator 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 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.

The game mechanics incorporated in this training intervention include narrative, points, feedback, judgment 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).
- Judgment of Self (metacognition) is done *via* comparison of performance prediction and retrospective performance assessment, both in relation to external inter-subjective expert-ratings. Metacognitive 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).

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 et al., 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 metacognition 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 and 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 metacognitive awareness. When both partners' mental models are synchronously constructed this can support shared consciousness, and increased engagement leading to empowered execution (McChrystal et al., 2015). One of the key goals of gamification is to increase 'engagement'. Therefore, by gamifying an OLB training program 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 metacognition, 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.

Operationalization of communicating the RCP

To remain consistent with the theory presented in the OLB process (Figures 2E–G), the following five individual traits that were identified will be measured: (1) metacognitive awareness, (2) perspective taking, (3) communication styles, (4) self-regulation, (5) motivational structures, as well as (6) CSA.

Metacognitive awareness

Metacognition 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 (Flavell, 1979; Efklides, 2008). Metacognitive abilities have been identified as important for SA in several contexts (Sethumadhavan, 2011; Endsley, 2020) including CSA for cybersecurity (Sütterlin et al., 2022; Ask et al., 2023b). Metacognition is considered as having two dimensions: Metacognitive awareness and metacognitive regulation. Metacognition 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; pp. 353). We provided neuroergonomic support for the OLB model in a recent study of cyber cadets participating in a defensive cyber engineering exercise (Ask et al., 2023b). We found that neurophysiological indicators (e.g., Brunoni et al., 2013; Nikolin et al., 2017; Chand et al., 2020; Schmaußer et al., 2022) of activity in brain regions relevant for metacognition (Fleur et al., 2021) was associated with self-report measures of how demanding team communication was, and CSA-related prospective metacognitive judgments (Ask et al., 2023b).

Perspective taking

Perspective taking describes the tendency to spontaneously adopt the psychological point of view of others. How the human brain interprets language depends on the context the language is occurring in Willems and Peelen (2021). To communicate efficiently, one must understand the context within which a communication partner is interpreting the communicated information. Contexts are represented mentally and may vary between individuals in the HS depending on their current priorities (Jøsok et al., 2016). Consequently, perspective taking is required to co-construct a shared mental model with communication partners and constitutes the *Locate* stage in the OLB model (Knox et al., 2018). 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 metacognition 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 metacognition, self-regulation serves to regulate cognition. Self-regulation is defined as the regulation of cognition, emotions, behavior, and environment (Efklides, 2008). Self-regulation has been shown to contribute to performance across varying domains, particularly in sport (Toering et al., 2009) and academic achievement (Zimmerman, 1990), as well as in cybersecurity (Knox et al., 2017; Jøsok et al., 2019; Knox et al., 2021; Ask et al., 2023b).

Motivational structure

Motivation is defined as 'a driving force responsible for the initiation, persistence, direction, and vigor of goal-directed behavior (Colman, 2006), 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 and Ryan, 1985; Vallerand et al., 1987; Vallerand and Losier, 1999; Vallerand, 2007). While gamification improves learning and motivation, the effect depends on the people and context where it is applied (Hamari et al., 2014). For instance, a recent study reported that a gamification intervention aimed at improving cybersecurity awareness among computer science students had an effect on learning outcomes but did not have an effect on attitudes and willingness for continued cybersecurity learning (Wu et al., 2021). Similarly, when using game-based learning to teach high school students about cybersecurity, it was found that males enjoyed the approach more than females (Jin et al., 2018). This suggests that there may be demographic-dependent aspects to consider when designing gamification approaches. Another study that used gamification to teach students about cyberattacks found that students were more engaged by a sense of achievement and knowledge acquisition rather than the entertaining and winning aspects of the gamification approach (Matovu et al., 2022). Thus, knowing whether users are motivated by growth or competition is important when designing gamified mechanics for intrinsic and extrinsic motivation.

From a neuroergonomic perspective, a task is intrinsically motivating when the brain is able to predict reward from the feedback of being engaged in the task itself (Di Domenico and Ryan, 2017). Consequently, what is crucial for gamification approaches to facilitate engagement is the inclusion of elements that relate game mechanics to an incentive structure that is relevant for target users. For our purposes, this requires knowing which aspects of being a cyber operator that motivates the individual. There is not much literature on what motivate cyber operators to choose their profession, a profession which entails high cognitive load and stress, although aspects of forensics work such as being "the one to find the needle in the haystack" with respect to uncovering cyber threats has been reported (Staheli et al., 2016). Aside from valuing technical and forensic competence, this could indicate that cyber operators are motivated by a high need for achievement (McClelland et al., 1953; see Yang et al., 2015 for a study on the relationship between need for achievement, motivation, and reactions to stress) as well as a high need for cognition (effortful cognitive activity; Cacioppo and Petty, 1982). Thus, the intrinsic motivations to be captured by gamification mechanics may be the sense of achievement from solving challenging and relevant tasks. Whether this is a correct assumption needs further investigation.

Cyber situational awareness

In addition to qualitative evaluations by experts or mentors, it is necessary to evaluate the outcomes of the gamification approach through objective, independent and quantitative measures that are not subject to human bias. Such measures should preferably capture multiple CSA elements in order to assess how successful

communication was. Performance metrics are lacking for human cyber operators (Agyepong et al., 2020). This includes measures of CSA as most studies on SA in SOC teams only utilize indirect measures of CSA (Ofte and Katsikas, 2022). There is still a need to understand what SA means for human cyber operators and methods to objectively measure it in ways that are useful for cybersecurity (Gutzwiller et al., 2020). A questionnaire has been proposed to measure CSA in cyber operators (Lif et al., 2017). This questionnaire employs multiple measurements; it asks cyber operators to draw a graph that illustrates network topology and activity during a cyberattack, including sources, IP addresses, attack paths, and so on. The questionnaire also asks cyber operators to indicate confidence in their descriptions, what kind of incident it was, the vulnerability that was exploited, if attacks were directed and/or automatic, where in the kill chain the attack is, the reason behind the attack, which system(s) are under attack, which actions should be taken, and to rate how critical the system is, how severe the attack is, and how urgent it is to take action (Lif et al., 2017). Several of these questions cover the CSA requirements forwarded by Barford et al. (2009). In studies utilizing expert validation of the CSA questionnaire during cyber defense exercises (Lif et al., 2018, 2020), it was found that when teams incorporated a higher number of the questionnaire items in their incident reports, it resulted in higher independent quality ratings of the report (Lif et al., 2018). When participants were asked to rate the relevance of the items on a scale from 1 (low) to 7 (high), the average rating was 4.3 (Lif et al., 2018), and 4.1 (Lif et al., 2020), which the authors interpreted as promising but also as an indication of need for further development of the questionnaire (Lif et al., 2018, 2020).

In a previous study, we used the CSA questionnaire developed by Lif et al. (2017) as a method for measuring cyber cadets' CSA while they were participating in a defensive cyber operations exercise (Ask et al., 2023b). We found that the accuracy of prospective metacognitive judgments of CSA acquisition was associated with both neurophysiological and self-report indicators of self-regulation and metacognitive capacity, and that individuals with higher metacognitive accuracy had more accurate CSA scores (Ask et al., 2023b). As metacognition is related to objective SA (Endsley, 2020), our findings (Ask et al., 2023b) provide some neurocognitive validation of the CSA questionnaire.

Given the need for cyber operators to tailor their RCPs to the information needs of their clients (Ahren et al., 2016; Staheli et al., 2016), one could argue that the CSA questionnaire (Lif et al., 2017) is missing some qualitative items that explicitly asks "what is the consequence of the attack for the daily operations of your client's organization?" and "what information is important for your client in order for them to make cyber defense decisions that ensures that their organization can maintain its productivity?." Answering these questions requires that cyber operators take the priorities of their clients into consideration when navigating their own CSA, which is a form of perspective-taking relevant for OLB-ing. Furthermore, asking cyber operators in an open-ended question to briefly, but specifically, describe the activity they have observed may provide some additional insight into their CSA (Ask et al., 2023a) in ways not currently captured by the CSA questionnaire proposed by Lif et al. (2017). In sum, with further development, the CSA questionnaire can be useful as a basis for objectively operationalizing the CSA following RCP communication.

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 3) to RCP communication in STSs. The aim is to foster the (meta-)cognitive skills required for improving communication for CSA and shared mental models.

Step 1: 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. Among 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: operator 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 task is chosen and tailored based upon advanced knowledge of the participants (e.g., skill, experience, leader level), gained through dialog with those who have requested the training. 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) cyber operator and involve processes such as penetration testing, attack/defense, capture-the-flag, malware forensics, and incident response. Before the cyber operator (P1) commences the Cyber Task he/she will answer a quantitative *Judgment of Self* questionnaire (SAM) relating to performance prediction/judgment of self.

Gamification mechanics: the initial 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: 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 cyber operator (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 S3 can be in

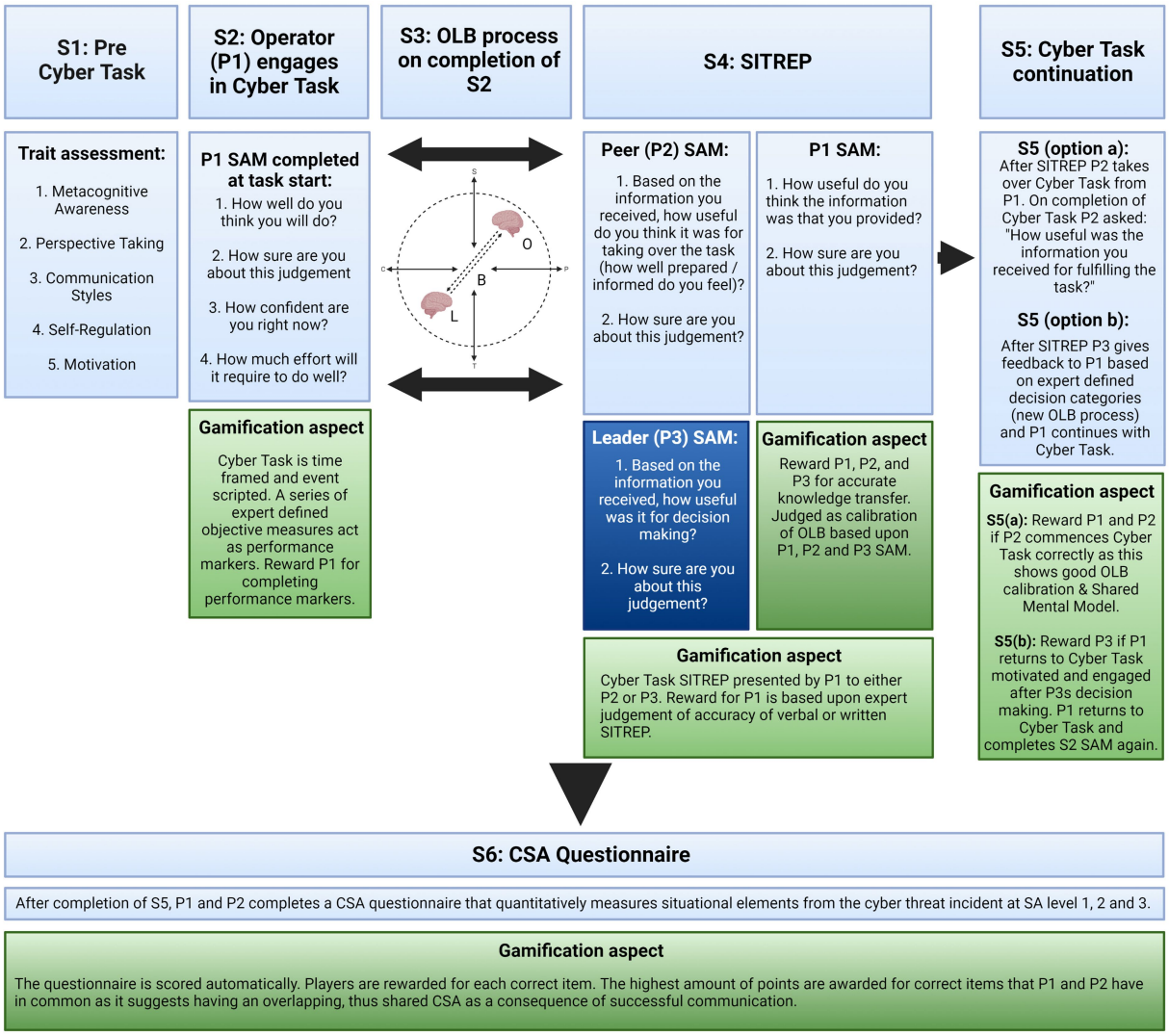

FIGURE 3
Step 1–6 of the game design (blue) including the gamification aspects (green). S1 will be done with validated questionnaires: e.g., MCAI (Schraw and Dennison, 1994), SRQ (Aubrey et al., 1994), REQ (Gross and John, 2003), IRI (Davis, 1983), CIS (De Vries et al., 2013), SIMS (Guay et al., 2000), CSA questionnaire for analysts (Lif et al., 2017). S=Step (1–6). P=Participant (1, 2 & 3). SAM, Self-Assessment Mannequin (judgment of self; performance predictions and retrospective performance assessment); SITREP, Situational report; OLB, Orient, Locate, Bridge; CSA, Cyber situational awareness.

verbal or written modality and constitutes a situational report (SITREP).

In the process from S2 through S3, P1 will make some progress (dependent upon skills, experience, and so on) in accordance with S2. Any hand-over (OLB) to P2 (S3) would be technical and moderated dependent upon P2's skill, knowledge, and status (and so on) as a cyber operator but would (or should) likely include some guidance to the expected or suspected operational impact of the cyberattack (e.g., ransomware) - if only to deliver an 'urgency' read out to P2. Any P1 OLB-ing with P3 could and should include more of the 'guidance' regarding the expected or suspected operational impact of the ransomware on the business/mission. This is the case even if the information is as much as; "this could take days to resolve if I am working alone." Technical information can be included for P3 for context if only to emphasize the severity or lack of current understanding, but too much technical information will baffle and potentially irritate, confuse, and/or obfuscate the real issue for P3, which is that of strategic impact.

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 *Judgment of Self* in S4.

Step 4: SITREP

The quality of the exchanged information will be assessed *via* 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 among 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: 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 cyber operator and provides instructions and feedback regarding the work done and gives advice on future action (simulating that the same cyber operator (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 step involves Points, Feedback, Narrative and Judgment of Self.

Step 6: CSA questionnaire

After completion of the gamification scenario, P1 and P2 complete a quantitative CSA questionnaire that contains items targeting SA at level 1, 2, and 3. Each player is rewarded for every item that is correctly answered. The highest number of points are awarded for correct items that P1 and P2 have in common. Having correct items in common suggests overlapping CSA and that RCP communication has been successful, thus, S6 ensures further gamification of efficient communication. The questionnaire is scored automatically and is independent of human expert/mentor ratings.

Gamification mechanics: this final step involves *Points*.

Considerations for difficulty adjustments

A critical, and beneficial aspect of the proposed gamification method is the ability to adjust difficulty. This will ensure that training can start off simple but become progressively harder as users develop their skills and knowledge. There are multiple ways to address this both within and between gamification sessions. One way to address this issue within a single gamification session is to design the gamification process to gradually incorporate CSA information elements at each SA level, such that the initial situational understanding that is to be communicated is based on SA level 1 elements, and then SA level 2 and SA level 3, as the participants cycles through the gamification steps. This will allow users to gradually develop the complexity of their situational knowledge. Another way of adjusting difficulty within a single session is to impose time constraints (as indicated in Table 2). Adjusting difficulty between gamification sessions would entail adjusting how much technical and information complexity that is included in the scenario in a given session. In other words, how many CSA elements that are included as critical for achieving an accurate CSA. This could also be achieved by selecting scenarios with more or less complexity. One important point that is worth re-emphasizing is that it is the cyber operator's task to reduce the complexity of the communicated information according to the understanding and needs of the decision-maker. Thus, there is an aspect of within-session complexity (hence difficulty) reduction that is dependent on how well P1 applies the OLB process when communicating the RCP.

Suggestions for validation of the gamification approach

While the combination of human rater and objective CSA measurements will ensure that there are ways for independently assessing the success of RCP communication that are intrinsic to the gamification approach, it may be necessary to perform additional validation procedures that are extrinsic to the suggested approach. One such approach is by utilizing comparative evaluation techniques. For example, basing the cyber threat scenario applied in the gamification method on existing scenarios that are used in cyber ranges would allow for including individuals (e.g., red teamers) that

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

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	Organizational deficit in cyber domain cognizance

These independent variables represent several possibilities to choose from. Step representation of gamification can be found in Table 2.

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

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–judgments of performance and meta-cognitive accuracy (controlled with self-assessments: S1 & S4) (−100 to 100 points).
S5	Reward OLB	(Max 100 points)
S6	CSA questionnaire measuring elements of SA level 1, 2, and 3.	Scored automatically. Points for each correct CSA item. Double points for correct items that P1 and P2 have in common (max 100 points).
Extra gamification aspect	Risk taking	After judgment 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).

are familiar with the ground truth of that scenario as external observers doing independent scoring. When validating the utility of their CSA questionnaire for incident reporting, Lif et al. (2018) utilized expert ratings (white team) where raters had a predefined scoring sheet for incident report quality that was developed independently of the CSA questionnaire. There was no direct overlap in the information items in the CSA questionnaire and the expert scoring sheet, allowing for correlational analysis of the relationship between them (Lif et al., 2018). We suggest that a similar approach can be adopted for comparative assessments to validate the gamification approach.

It is also necessary to incorporate user validation of the gamification process to ensure that it is engaging in a way that stimulates sustained learning. Thus, initial applications of the gamification method should include asking users if they found the gamification process engaging and motivating, which aspects of the approach they found the most and least engaging, if they would like to continue to use the approach for learning, if they have suggestions for improvement, if they found the scenarios to be realistic, and so on. This should be combined with standardized motivational measures such as those assessing need for achievement (McClelland et al., 1953), need for cognition (Cacioppo and Petty, 1982), and need for competition (Bugten et al., 2021). It is also important to assess whether there are gender differences in how engaging the gamification approach is (Jin et al., 2018).

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 which should include surveying target users about whether they are motivated to continue using the gamification approach, what elements (if any) they found motivational, and if they have any suggestions to improve engagement.

Author contributions

BK conceptualized the main ideas of the paper. TA wrote the main parts of the manuscript. BK, RL, SS, and LH contributed with

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

theoretical background. All authors contributed with review and editing of the manuscript and all authors approved of the final draft.

Funding

This research was funded by the Norwegian Research Council (#302941).

Acknowledgments

A preprint of this article is available at PsyArXiv preprints (Ask et al., 2021c; 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

References

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. (2020). Challenges and performance metrics for security operations center analysts: a systematic review. *J. Cyber Secur. 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*. London, UK: Data Analytics and Assessment (CyberSA).

Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., Welch, I., Camtepe, S. A., et al. (2022). A survey on cyber situation awareness systems: framework, techniques, and insights. *ACM Comput. Surv.* 55, 1–37. doi: 10.1145/3530809

Ask, T. F., Knox, B. J., Lugo, R. G., Helgetun, I., and Sütterlin, S. (2023b). Neurophysiological and emotional influences on team communication and metacognitive cyber situational awareness during a cyber engineering exercise. *Front. Hum. Neurosci.* 16:1092056. doi: 10.3389/fnhum.2022.1092056

Ask, T. F., Knox, B. J., Lugo, R., Hoffmann, L., and Sütterlin, S. (2021c). A gamification approach to improving interpersonal situational awareness in cyber defense. *PsyArXiv* 2021, 2–18. doi: 10.31234/osf.io/c95kw

Ask, T. F., Kullman, K., Sütterlin, S., Knox, B. J., Engel, D., and Lugo, R. G. (2023a). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *Front. Big Data* 6:1042783. doi: 10.3389/fdata.2023.1042783

Ask, T. F., Lugo, R. G., Knox, B. J., and Sütterlin, S.. (2021a). Human-human communication in cyber threat situations: a systematic review. In C. Stephanidis, Harris, D., Li, W. C., Schmorrow, D. D., Fidopiastis, C. M., and Antona, M.. *HCI international 2021–late breaking papers: cognition, inclusion, learning, and culture. HCII 2021 lecture notes in computer science*. Cham: Springer, p. 13096.

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 C. Stephanidis, Fidopiastis, C. M., and Antona, M.. *HCI international 2021–late breaking papers: cognition, inclusion, learning, and culture. HCII 2021. Lecture notes in computer science*. Springer, Cham, p. 13096.

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

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.

Baumeister, R. F., and Vohs, K. D. (2007). Self-regulation, ego depletion, and motivation. *Soc. Personal. Psychol. Compass* 1, 115–128. doi: 10.1111/j.1751-9004.2007.00001.x

Brady, C., and M'manga, A.. (2022). Gamification of cyber security training–EnsureSecure. In: *2022 IEEE international conference on e-business engineering (ICEBE)*, (Bournemouth, United Kingdom. pp. 7–12.

Broholm, R., Christensen, M., and Sørensen, L. T.. (2022). *Exploring Gamification elements to enhance user motivation in a cyber security learning platform through focus group interviews*. In: 2022 IEEE European symposium on security and privacy workshops (EuroS&PW), Genoa, Italy. pp. 470–476.

Brunoni, A. R., Vanderhasselt, M. A., Boggio, P. S., Fregni, F., Dantas, E. M., Mill, J. G., et al. (2013). 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

Bugten, J. B., Lugo, R. G., and Steptoe, K. (2021). Validation of the need for competing inventory. *Front. Psychol.* 12:721903. doi: 10.3389/fpsyg.2021.721903

Cacioppo, J. T., and Petty, R. E. (1982). The need for cognition. *J. Pers. Soc. Psychol.* 42, 116–131. doi: 10.1037/0022-3514.42.1.116

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

Cheng, Y., Zhang, Y., Wang, F., Jia, G., Zhou, J., Shan, Y., et al. (2020). Reversal of age-related changes in cortical sound-azimuth selectivity with training. *Cereb. Cortex* 30, 1768–1778. doi: 10.1093/cercor/bhz201

Colman, A. M. (2006). Motivation. In *Dictionary of psychology (2nd ed.)*. Oxford, N.Y.: Oxford University Press.

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

Crilly, M. (2021). *Warfare in the post digital era*. Wavell Room: Contemporary British Military Thought. Available at: 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. *J. Pers. Soc. Psychol.* 44, 113–126. doi: 10.1037/0022-3514.44.1.113

De Vries, R. E., Bakker-Pieper, A., Konings, F. E., and Schouten, B. (2013). The communication styles inventory (CSI) a six-dimensional behavioral model of communication styles and its relation with personality. *Commun. Res.* 40, 506–532. doi: 10.1177/009365021141357

Debashi, M., and Vickers, P. (2018). Sonification of network traffic flow for monitoring and situational awareness. *PLoS One* 13:e0195948. doi: 10.1371/journal.pone.0195948

Deci, E. L., and Ryan, R. M. (1985). The general causality orientations scale: self-determination in personality. *J. Res. Pers.* 19, 109–134.

Di Domenico, S. I., and Ryan, R. M. (2017). The emerging neuroscience of intrinsic motivation: a new frontier in self-determination research. *Front. Hum. Neurosci.* 11:145. doi: 10.3389/fnhum.2017.00145

Dostal, B. C. (2007). *Enhancing situational understanding through the employment of unmanned aerial vehicles*. Army Transformation Taking Shape. Interim Brigade Combat Team Newsletter, pp. 1–18.

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

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. *Proc. Hum. Factors Soc. Annu. Meet.* 32, 97–101.

Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Hum. Factors* 37, 65–84.

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

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

ENISA (2018). Cybersecurity culture guidelines: behavioural aspects of cybersecurity. *WP2018* 2, 1–34. doi: 10.2824/324042

Farwell, J. P., and Rohozinski, R. (2012). The new reality of cyber war. *Survival* 54, 107–120. doi: 10.1080/00396338.2012.709391

Fink, G., Best, D., Manz, D., Popovsky, V., and Endicott-Popovsky, B. (2013). Gamification for Measuring Cyber Security Situational Awareness. In *Foundations of Augmented Cognition*. AC 2013. Lecture Notes in Computer Science(), vol 8027. Schmorrow, D.D., Fidopiastis, C.M. (eds) (Springer, Berlin, Heidelberg).

Finkel, E. J., Campbell, W. K., Brunell, A. B., Dalton, A. N., Scarbeck, S. J., and Chartrand, T. L. (2006). High-maintenance interaction: inefficient social coordination impairs self-regulation. *J. Pers. Soc. Psychol.* 91:456. doi: 10.1037/0022-3514.91.3.456

Fitton, O. (2016). Cyber operations and gray zones: challenges for NATO. *Connections* 15, 109–119. doi: 10.11610/Connections.15.2.08

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

Fletcher, J. D. (2004). Cognitive readiness: preparing for the unexpected. Defence technical information center, institute for defense analysis. Alexandra, VA. Available at: https://apps.dtic.mil/docs/citations/ADA458683.

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

Gardner, F. (2021). *What does future warfare look like? It's here already*. Available at: https://www.bbc.com/news/world-59755100 (Accessed April 21 2023).

Gee, J. P. (2003). What video games have to teach us about learning and literacy. *Comput. Entertain.* 1:20. doi: 10.1145/950566.950595

Gross, J. J., and John, O. P. (2003). Individual differences in two emotion regulation processes: implications for affect, relationships, and well-being. *J. Pers. Soc. Psychol.* 85, 348–362. doi: 10.1037/0022-3514.85.2.348

Guay, F., Vallerand, R., and Blanchard, C. (2000). On the assessment of situational intrinsic and extrinsic motivation: the situational motivation scale (SIMS). *Motiv. Emot.* 24, 175–213. doi: 10.1023/A:1005614228250

Gutzwiller, R. S., Dykstra, J., and Payne, B. (2020). Gaps and opportunities in situational awareness for Cybersecurity. *Digit. Threats* 1:18. doi: 10.1145/3384471

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., and Hancock, P. A. (2015). The human factors of cyber network defense. *Proc. Hum. Fact. Ergon. Soc. Ann. Meet.* 59, 322–326. doi: 10.1177/1541931215591067

Hamari, J., Koivisto, J., and Sarsa, H. (2014). Does Gamification work?-a literature review of empirical studies on Gamification. *HICSS* 14, 3025–3034. doi: 10.1109/HICSS.2014.377

Harter, J. K., Schmidt, F. L., Killham, E. A., and 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)*. Available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmpubadm/496/496.pdf.

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

Howard-Jones, P. A., Jay, T., Mason, A., and Jones, H. (2016). Gamification of learning deactivates the default mode network. *Front. Psychol.* 6:1891. doi: 10.3389/fpsyg.2015.01891

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

Jelo, M., and Helebrandt, P.. (2022). *Gamification of cyber ranges in cybersecurity education*. In: 20th International Conference on Emerging eLearning Technologies and Applications (ICETA), Stary Smokovec, Slovakia, pp. 280–285.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., and White, J. (2018). Evaluation of game-based learning in Cybersecurity education for high school students. *J. Educ. Learn.* 12:150. doi: 10.11591/edulearn.v12i1.7736

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., and Ward, P. (2016). *Exploring the hybrid space*. International Conference on Augmented Cognition, pp. 178–188.

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 *Lecture Notes in Computer Science*. eds. D. D. Schmorrow and C. M. Fidopiastis, vol. *10285* (Cham: Springer), 486–500.

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

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

Klein, G., Moon, B., and Hoffman, R. R. (2006). Making sense of sensemaking 1: alternative perspectives. *IEEE Intell. Syst.* 21, 70–73. doi: 10.1109/mis.2006.75

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., and Sütterlin, S. (2021). Slow education and cognitive agility: improving military cyber cadet cognitive performance for better governance of Cyberpower. In *I. Management Association, Research anthology on military and defense applications, utilization, education, and ethics*, pp. 1–21. IGI Global.

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 *HCII Posters 2017*. ed. C. Stephanidis, vol. *713* (Cham: Springer), 330–338.

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: Academic Conferences and Publishing International Limited, 369–378.

Landers, R. N. (2014). Developing a theory of gamified learning: linking serious games and gamification of learning. *Simul. Gaming* 45, 752–768. doi: 10.1177/1046878114563660

Landers, R. N., Bauer, K. N., Callan, R. C., and Armstrong, M. B. (2015). "Psychological theory and the gamification of learning" in *Gamification in education and business*. eds. T. Reiners and L. Wood (Cham: Springer), 165–186.

Lankton, P. (2007). *Endsley's model of situational awareness*. Avalable 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.

Lif, P., Sommestad, T., and Granasen, D. (2018). *Development and evaluation of information elements for simplified cyber-incident reports*. 2018 international conference on cyber situational awareness, Data Analytics And Assessment (Cyber SA).

Lif, P., Varga, S., Wedlin, M., Lindahl, D., and Persson, M.. (2020). *Evaluation of information elements in a cyber incident report*. In: 2020 IEEE European symposium on security and privacy workshops (EuroS&PW).

Loh, C. S., and Sheng, Y. (2013). Performance metrics for serious games: Will the (real) expert please step forward? *Proceedings of CGAMES'2013 USA*. doi: 10.1109/cgames.2013.6632633

Lorenz, R. C., Gleich, T., Gallinat, J., and Kühn, S. (2015). Video game training and the reward system. *Front. Hum. Neurosci.* 9:40. doi: 10.3389/fnhum.2015.00040

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

Masakowski, Y. R., and Blatny, J. M.. (2023). *Mitigating and responding to cognitive warfare*. STO Technical Report RDP, STO-TR-HFM-ET-356.

Matovu, R., Nwokeji, J. C., Holmes, T., and Rahman, T. (2022). *Teaching and learning Cybersecurity awareness with Gamification in smaller universities and colleges*. In: 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 1–9.

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

McClelland, D. C., Atkinson, J. W., Clark, R. A., and Lowell, E. L. (1953). *The achievement motive*. New York: Appleton-Century-Crofts.

McMahon, C. (2020). In defence of the human factor. *Front. Psychol.* 11:1390. doi: 10.3389/fpsyg.2020.01390

Michailidis, L., Balaguer-Ballester, E., and He, X. (2018). Flow and immersion in video games: the aftermath of a conceptual challenge. *Front. Psychol.* 9:1682. doi: 10.3389/fpsyg.2018.01682

Morrow, D. G., and Fischer, U. M. (2013). "Communication in socio-technical systems" in *The Oxford handbook of cognitive engineering*. eds. J. D. Lee and A. Kirlik (New York: Oxford University Press), 178–199.

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

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

Ofte, H. J., and Katsikas, S. (2022). Understanding Situation Awareness in SOCs, A Systematic Literature Review. *Computers & Security* 103069. doi: 10.1016/j.cose.2022.103069

Ong, M. (2013). *Gamification and its effect on employee engagement and performance in a perceptual diagnosis task (master thesis)*. New Zealand: University of Canterbury.

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

Parasuraman, R., and Rizzo, M. (2008). "Introduction to neuroergonomics" in *Neuroergonomics: The brain at work*. eds. R. Parasurman and M. Rizzo (New York: Oxford University Press), 3–12.

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., et al. (2022). Application of intervention mapping in cybersecurity education design. *Front. Educ.* 7:998335. doi: 10.3389/feduc.2022.998335

Qusa, H., and Tarazi, J. (2021). *Cyber-Hero: a Gamification framework for cyber security awareness for high schools students*. In 2021 IEEE 11th annual computing and communication workshop and conference (CCWC). pp. 677–682.

Recanzone, G. H., Merzenich, M. M., Jenkins, W. M., Grajski, K. A., and Dinse, H. R. (1992a). Topographic reorganization of the hand representation in cortical area 3b owl monkeys trained in a frequency-discrimination task. *J. Neurophysiol.* 67, 1031–1056. doi: 10.1152/jn.1992.67.5.1031

Recanzone, G. H., Merzenich, M. M., and 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, 1071–1091. doi: 10.1152/jn.1992.67.5.1071

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

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

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

Sailer, M., Hense, J., Mandl, J., and Klevers, M. (2013). Psychological perspectives on motivation through gamification. *Interact. Des. Archit. J.* 19, 28–37. doi: 10.55612/s-5002-019-002

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

Schaberreiter, T., Röning, J., Quirchmayr, G., Kupfersberger, V., Wills, C., Bregonzio, M., et al. (2022). "A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: the CS-AWARE project" in *Challenges in Cybersecurity and privacy-the European research landscape*. eds. J. B. Bernabe and A. Skarmeta (Denmark: River Publishers), 149–180.

Schmaußer, M., Hoffmann, S., Raab, M., and Laborde, S. (2022). The effects of noninvasive brain stimulation on heart rate and heart rate variability: A systematic review and meta-analysis. *J. Neurosci. Res.* 100, 1664–1694. doi: 10.1002/jnr.25062

Schraw, G., and Dennison, R. S. (1994). Assessing metacognitive awareness. *Contemp. Educ. Psychol.* 19, 460–475. doi: 10.1006/ceps.1994.1033

Sethumadhavan, A. (2011). Knowing what you know: the role of meta-situation awareness in predicting situation awareness. *Proc. Hum. Factors Ergon. Soc. Ann. Meet.* 55, 360–364. doi: 10.1177/1071181311551074

Sharif, K. H., and Ameen, S. Y. (2021). *A review on Gamification for information security training*. In: 2021 international conference of modern trends in information and communication technology industry (MTICTI), Yemen, Sana'a, pp. 1–8.

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.

Sütterlin, S., Ask, T. F., Mägerle, S., Glöckler, S., Wolf, L., Schray, J., et al. (2023). *Individual deep fake recognition skills are affected by viewers' political orientation, agreement with content and device used*. Lecture Notes in Computer Science.

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, vol. *13310* (Cham: Springer)

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

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

Vallerand, R. J. (2007). "Intrinsic and extrinsic motivation in sport and physical activity" in *Handbook of Sport Psychology*. eds. G. Tenenbaum and R. C. Eklund, vol. 3, 59–83. doi: 10.1002/9781118270011.ch3

Vallerand, R. J., Deci, E. L., and Ryan, R. M. (1987). 12 intrinsic motivation in sport. *Exerc. Sport Sci. Rev.* 15, 389–426.

Vallerand, R. J., and Losier, G. F. (1999). An integrative analysis of intrinsic and extrinsic motivation in sport. *J. Appl. Sport Psychol.* 11, 142–169.

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, pp. 774–781.

Ward, P., Gore, J., Hutton, R., Conway, G. E., and Hoffman, R. R. (2018). Adaptive skill as the conditio sine qua non of expertise. *J. Appl. Res. Mem. Cogn.* 7, 35–50. doi: 10.1016/j.jarmac.2018.01.009

Willems, R. M., and Peelen, M. V. (2021). How context changes the neural basis of perception and language. *iScience* 24:102392. doi: 10.1016/j.isci.2021.102392

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Comput. Fraud Secur.* 2019, 9–12. doi: 10.1016/S1361-3723(19)30052-1

Wu, T., Tien, K.-Y., Hsu, W.-C., and Wen, F.-H. (2021). Assessing the effects of Gamification on enhancing information security awareness knowledge. *Appl. Sci.* 11:9266. doi: 10.3390/app11199266

Yang, F., Ramsay, J. E., Schultheiss, O. C., and Pang, J. S. (2015). Need for achievement moderates the effect of motive-relevant challenge on salivary cortisol changes. *Motiv. Emot.* 39, 321–334. doi: 10.1007/s11031-014-9465-7

Zachary, W., and Miller, A. R.. (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*. In: 2014 international conference on engineering, technology and innovation (ICE). pp. 1–6.

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