



A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects

SAGE Open
 January-March 2023: 1–12
 © The Author(s) 2023
 DOI: 10.1177/21582440231156367
journals.sagepub.com/home/sgo


Kaie Maennel¹ , Agnė Brilingaitė² , Linas Bukauskas², Aušrius Juozapavičius³, Benjamin James Knox^{4,5}, Ricardo Gregorio Lugo⁴, Olaf Maennel¹, Ginta Majore⁶, and Stefan Sütterlin^{4,7}

Abstract

Hands-on and practical learning has been key to cybersecurity education and training success. Cyber Defense Exercises (CDX) are a common approach to training, testing, and verifying technical and soft skills. However, full-scale CDX implementation is also an expensive training event. In order to advance such exercises to the next level, CDX organizers should further focus on educational, psychological, and cross-domain relationships. The paper discusses and proposes a multidimensional approach for CDX that balances cognitive, emotional, and social aspects critical for successful interdisciplinary learning. We share our experience incorporating knowledge from well-known psychology theories to CDX. We derive and describe seven elementary ingredients if a CDX is to meet the interdisciplinary and critical thinking needs of defensive cyberspace operations.

Keywords

cybersecurity, cyber defense exercise, interdisciplinary education, psychological safety, cognitive skills

Introduction

Cybersecurity education has been evolving over the last decades to respond to the increase in the demand for skilled cybersecurity professionals and the level of sophistication of cyberattacks. Hands-on and practical learning has been adopted by computer science, communication and engineering communities and is key to the successful education of the future workforce. Many cybersecurity exercises have been incorporated into educational and professional training paths. Such exercises range from a virtual computer or network assembly, quiz-based testing, capture-the-flag (CTF) gamified exercises to large-scale exercises. A Cyber Defense Exercise (CDX) is the most common approach to training, testing, and verifying professional skills at the highest preparedness tier for defensive cyberspace operations. However, it is also an expensive approach (Brilingaitė et al., 2020).

Given the many alternative cybersecurity training methods and providers, this article aims to present where the added value resides and what direction the CDX has to evolve to remain competitive and equal to the evolving technological and adversarial cyber-domain landscape.

Therefore, this work aims to reiterate the CDX execution quality and related components. We revisit the main principles of the CDX organization. However, we focus on CDX participants and soft skills as a foundation for advancement. Even if an exercise was designed purely as a technical skills assessment or for other purposes, such as testing processes and procedures, the non-technical

¹Tallinn University of Technology, Estonia

²Vilnius University, Lithuania

³General Jonas Žemaitis Military Academy of Lithuania, Vilnius, Lithuania

⁴Østfold University College, Norway

⁵Norwegian University of Science and Technology, Norway

⁶Vidzeme University of Applied Sciences, Valmiera, Latvia

⁷Albstadt-Sigmaringen University, Germany

*Ricardo Gregorio Lugo and Stefan Sütterlin is also affiliated to Tallinn University of Technology, Estonia; Kaie Maennel and Olaf Maennel is also affiliated to The University of Adelaide, Australia

Corresponding Author:

Kaie Maennel, Department of Software Sciences, School of Information Technology, Tallinn University of Technology, Ehitajate tee 5, Tallinn 19086, Estonia.

Email: kaie.maennel@taltech.ee



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of

the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

component should not be overlooked. Often the exercise organizers focus on technical, organizational, and strategic aspects, which are driven by the success metrics of other CDX stakeholders. For example, due to the expectations to achieve good scores from their organizations/leadership, the teams and their managers focus on the winning strategies (i.e., how to achieve good scores) instead of focusing on learning and collaborating during the preparation and execution. Due to differing stakeholder success metrics, the educational aspects for the training audience are forgotten. Thus, current exercises are not primarily designed with a holistic educational purpose and are criticized for lacking science-based teaching and training methods (Knox, Lugo, & Sütterlin, 2019). The participants should be at the center with planners asking:—*who* is learning, *what* are the expected lessons from each task or phase of the exercise, and *how* will performance and results be evaluated beyond purely technical ability?

We suggest a CDX design that adopts a multidimensional approach. One that demands the application of a wider cognitive repertoire and social-emotional aspects to encourage and expand interdisciplinary thinking (Spelt et al., 2017) in cyberspace operations. This can lead to higher digital literacy (Ng, 2012) among training audiences across competence levels. A critical reader might think—there is no time or need to focus on so-called “enjoyable” elements for participants, especially from the perspective of smaller nations and teams where they need to build interpersonal relationships and not only follow military-style command lines—these effects can bring eventually more positive effects when the teams face and mitigate real threats.

This paper aims to start the discussion and support the positions stated regarding the current status and how to advance a CDX by incorporating social, emotional, and cognitive aspects. We use experience gained from two larger CDXs, Locked Shields¹ (LS) and Amber Mist² (AM). We have been part of various CDXs and looked at these from the perspective of a smaller nation where multidisciplinary is a key factor. We present a multidimensional concept for developing and planning a CDX. The article derives seven ingredients that are elementary if a CDX is to meet the interdisciplinary and critical thinking needs of defensive cyberspace operations.

Research Design and Methodology

We apply theory-building as it provides a framework for analysis, facilitates the efficient development of the field, and is needed for the applicability to practical real-world problems (Gay & Weaver, 2011). As the mixed methods approach allows switching between inductive and deductive reasoning (Gay & Weaver, 2011), we consider this methodology relevant for the exploratory research of

novel aspects and developing the frameworks or approaches. This work contributes to the theory in two aspects: originality (incremental or revelatory) and utility (scientific or practical) (Corley & Gioia, 2011).

Overall, we follow the design and methodology, which contribute to providing practical knowledge and solutions that can support implementing innovative approaches in cybersecurity education, specifically in CDXs.

Context and Related Work

Types of CDXs

A multitude of variations of exercises that intend to improve cybersecurity exists—tabletops, CTFs, simulations, etc. (Ogee et al., 2015). This article focuses on more complex team-based and defense-oriented exercises with simulated opposing forces such as red (RT) and blue (BT) teams, respectively. The main learning objectives of these CDXs include advancing skills in network/system hardening and defense, incident response, communication, and teamwork (Brilingaitė et al., 2020). CDX structures have been adopted from confrontations, defense simulations with gamification elements or simulations of close-to-reality events. These exercises do not only focus on learning but can also be used for testing processes and procedures. Whether the primary purpose is learning or testing, if an exercise is not realistic, challenging, relevant, and addressing participants’ emotional, social, and cognitive needs, this can lead to a flawed assessment of outcomes and waste valuable resources.

CDXs From Multidisciplinary Aspects

There is an abundance of research on interdisciplinary educational approaches, generic and specific, for certain domains. The relevant research includes a multidimensional educational framework (Spelt et al., 2017) and six dimensions of expertise—Subject matter, Situational context, Interface tools, Expert identification, Communication, Information flow paths (Garrett et al., 2009). Some dimensions, such as communication expertise, self-awareness, and expert identification, might also be addressed through other methods, such as training and team development (Nyre-Yu, 2021). The multidisciplinary or multidimensional approach is emphasized for cybersecurity education (Berki et al., 2018; Blair et al., 2019; Omar et al., 2018; Tsado, 2019) to ensure curricular foundations for the multidisciplinary cybersecurity teams consisting of diverse cybersecurity experts. However, this is emphasized at the curricula level and appears not to be transferred to a CDX.

Recent academic literature about CDXs increasingly emphasizes quality and focuses on learning aspects (Brilingaitė et al., 2020; Chowdhury et al., 2022;

Hautamäki et al., 2019; Karjalainen et al., 2019, 2020; Maennel, 2020; Mäses et al., 2021; Seda et al., 2021). Also, an emphasis on the cognitive processes such as metacognition, self-regulation, coping strategies, communication, and shared mental modeling (e.g., Knox, Lugo, & Sütterlin, 2019) and various socio-cognitive aspects on course design level (e.g., Cruz & Simões, 2021) are emerging. However, the practical guides issued by various organizations, including Mitre, ANSSI, and ENISA, that discuss and provide guidance on how to organize a CDX mostly lack psychological and educational aspects. The incorporation of “behavioral aspects” starts to emerge, however, at a very high statement level.

Guidelines that tackle critical thinking aspects, interdisciplinary challenges, and a multidimensional approach combining technical “hard” and “soft” ingredients, that is, specific cognitive skills, emotional and social aspects (Illeris, 2016), and how these are addressed in a CDX, are not yet widely discussed.

CDXs From Social, Emotional, and Cognitive Aspects

In the following, we will discuss the social, emotional, and cognitive components based on the well-known theories relevant to the CDX context and build a foundation for incorporating and evaluating a CDX.

The Social Component: Psychological Safety. The term psychological safety (PS) describes a shared belief that the team is safe for interpersonal risk-taking where team members feel accepted and respected, that one will not be punished or humiliated for speaking up with ideas, questions, concerns, or mistakes (Kahn, 1990). A shared sense of PS in a team is a critical input to an effective learning system and predicts engagement in quality improvement work (A. Edmondson, 1999). Psychological safety is particularly needed in cross-disciplinary teams where status differences matter and members representing a particular area of responsibility may react defensively. Hierarchical teams, in general, may experience it challenging to secure psychological safety (Binyamin et al., 2018).

When implemented successfully, multiple empirical findings provide evidence that PS improves chances to successful organizational innovation (A. C. Edmondson, 2018). Teams are more likely to restructure, learn by trial and error, access and utilize available competencies by increased participation and engagement. A team with a high level of PS allows for cross-monitoring and makes problems apparent in an early stage, allowing for more proactive decision-making based on trust in competence rather than unambiguous empirical evidence. To reach a sufficient level of PS requires a leadership that is based on participatory or consultatory management—the empowerment of team members to participate in

decision-making or at least be consulted (A. C. Edmondson & Verdin, 2018).

Assessment of states of PS can be easily assessed via validated self-reports such as the Psychological Safety in the Workplace Questionnaire (PSWQ) (Carmeli et al., 2009). The use of the questionnaire allows for initial assessment as well as monitoring. It can point out areas where resources are neglected due to insufficient PS levels and thus point at necessary measures to be taken.

In the context of a CDX, PS can contribute to a lower risk of missing relevant signals and interpretations in following network monitoring and sensemaking, contributing to novel perspectives on given problems, expanding the repertoire of possible actions taken, and organizing roles and allocations of responsibilities more effectively in accordance with individual competencies. PS may also contribute to factors relevant to technical performance, such as intrinsic motivation via an increase in the sense of social relatedness (see Self-Determination Theory, SDT, for more details, Deci et al. (2017)). The particular relevance of PS in the CDX context is the very nature of problems posed in cyber defense, where available information and the repertoire of technically possible countermeasures are plentiful, but the problem’s nature as such remains to a high degree ambiguity. Ambiguous threats in cyber defense are characterized by a difficulty in attributing meaning to “gray” signals, to an increased risk of interpreting random signals as meaningful patterns, to lack of the ability to determine the outcomes and success probabilities of potential and technically feasible actions (Canham et al., 2022). Ambiguous threats are particularly prone to increase the likelihood of decision-making biases such as misinterpretations of statistical probabilities, and group think-based decision biases and other cognitive fallacies (Roberto et al., 2006). PS has the potential to increase the probability of available competencies allowing for a de-biasing of group decisions by questioning unarticulated belief systems, providing alternative viewpoints and challenging implicit assumptions or automatic tendencies.

The Emotional Component: Motivation by Self-Determination. Learning theories have long established the connection between motivation and learning outcomes. Where CDX participants are higher motivated, they will perform better, are less likely to give up, engage cognitively and generally invest more effort into collective or individual problem-solving. Particularly intrinsic motivation is crucial for positive learning effects and sustainable competence development. Intrinsic motivation refers to doing an activity for its inherent satisfaction rather than for some external and thus separable consequence such as a reward, fulfilling a formal requirement, or avoiding punishment (Reiss, 2004). Intrinsic

motivation is more sustainable than extrinsic motivation, which is based on rewards provided by others or the avoidance of negative consequences for oneself. It produces individual skill development and generally better learning outcomes. Efficient CDX should consider the requirements for developing intrinsic motivation early in designing an exercise. These requirements are laid out in the empirically well-supported Self-Determination Theory (Deci & Ryan, 1985). SDT states that intrinsic motivation results from fulfilling three basic psychological needs: autonomy, competence, and relatedness. In the context of CDX, autonomy refers to providing all participants with appropriate options and choices to make decisions and take risks in accordance with their level of expertise. This includes the freedom to communicate ideas, concerns and suggestions such as aberrant viewpoints or critical statements (see the connections to psychological safety) and a consultative or participatory leadership style. A maximal (but appropriate and responsible) level of autonomy strengthens intrinsic motivation. In contrast, a reduction to tasks requiring less reflective cognition and merely execution without any involvement in decision-making elements results in a decrease of intrinsic motivation and, thus, overall task engagement and resulting learning outcomes.

The second element SDT spells out as a requirement for intrinsic motivation is perceived competence. As humans have the need to experience their contribution as relevant and meaningful, positive, authentic, and accurate feedback is a highly relevant contributor to motivation. It is worth mentioning that feedback should always address the process and specific performance rather than unchangeable personality traits. Where both granular (task-specific) and cumulative feedback, that is, feedback over skill development over a longer period or substantial time span within an exercise, is given by authority and perceived as authentic, positive effects on motivation, task engagement, and thus learning outcomes are more likely. The effect of (positive) feedback is particularly strong where the feedback is unexpected and not part of a formal routine (Hattie & Timperley, 2007).

The third component of interest is the perceived relatedness (or: belongingness) of the individual with the task and the team. This includes the perception of following a shared goal with the team and being an appreciated and relevant member of it. This perception can be reached not only by feedback highlighting the relevance of a team member's contribution (regardless of formal rank and qualification) but also by the aforementioned participatory or consultative leadership style.

It appears evident that SDT shows close links with the aforementioned concept of psychological safety (PS), as both concepts require socially competent, that is,

prosocial, inclusive, and empathic leadership styles (Coetzee, 2019). Leadership with awareness of the pre-conditions of intrinsic motivation is thus a requirement for the full exploitation of team competencies over time and thus also in maximizing learning outcomes in CDX (Zeng et al., 2020).

The Cognitive Component: Slow Education for Cognitive Agility. Developing the social and emotional dimensions at the human operator level is necessary to govern the effects of own and adversarial cyber power. As cognitive performance in these dimensions combines with technical skills and digital competencies, the hypothetical outcome is a superior level of cyber domain cognizance. However, reaching this point is an effortful process that must begin in advance of a CDX and likely requires novel pedagogic methods combined with psychological techniques.

One approach that has been identified to improve cognitive performance among cyber operators is Slow Education (Knox, Lugo, Helkala, & Sütterlin, 2019). This non-standards-based method favors intellectual nuance over standardization and accountability common to traditional educational models. Just as in other domains of skill development, Slow Education in cyber education and training relies upon mentoring processes (Knox, Lugo, & Sütterlin, 2019) and re-thinking teaching methods in order to scaffold the essential cyber hard skills and the motivation to develop critical soft skills at individual and team levels. A higher overall domain cognizance can be understood as a contributing factor to intrinsic motivation to work on hard problems and mental resilience. The latter has been defined as a feature of what it takes for an individual to achieve the highest levels of proficiency (L. Ward et al., 2013).

Improving learners' cognitive repertoire through the integration of Slow Education techniques into a curriculum's pedagogic approach preceding a CDX can lead to improved PS, metacognitive skill orientation, and a better understanding of real-world events (Hannafin & Hannafin, 2010) by creating a deepening knowledge of the context of cyberspace operations. A pedagogic intervention of this kind can support the development of the cognitive strategies of self-regulation and reflective pondering, both of which correlate with cognitive agility. This is relevant for conducting cyberspace operations as cognitive agility is understood as an individual's metacognitive strategy proficiency to meet objectives with situational constraints (Turner et al., 2020).

The task characteristics of cyberspace operations require effective coordination to ease constraints between multiple agents and asset types (human, technical, tangible, and intangible) to deliver a performance edge. Building domain cognizance requires individuals to be

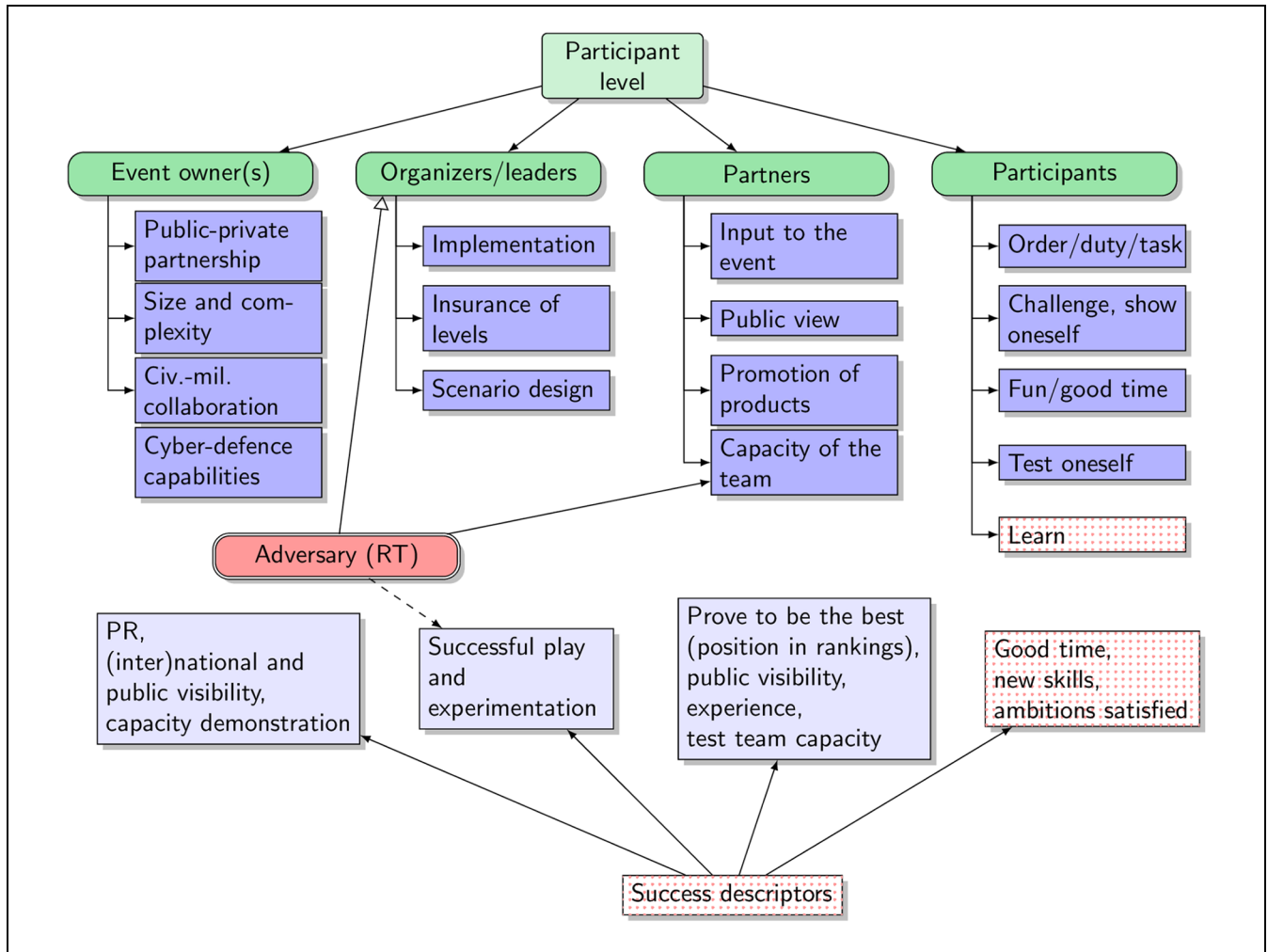


Figure 1. Goals and success from the perspective of various levels.

self-governing, open, flexible, and adaptable: the psychological characteristics of cognitive agility (Hutton & Turner, 2019).

The ability of cyber operators and cyber leaders/decision-makers to find, apply, and deploy the appropriate technological tools is reliant upon the sum of their individual cyber domain cognizance. Without it, maintenance of relevancy and communication of effects become challenged, leading to potential catastrophic miscalculations. As such, cognitive skill development, training, and testing during a CDX can be of particular use when dealing with geo-political factors, legal and ethical limitations/frames, strategic guidance, governance mechanisms, and risk analysis based on tactical, operational, and strategic cyber power effects. Improving critical self-reflection for more accurate measurement and monitoring of own and cyber-team performance relative to actual performance or learning rate (P. Ward et al., 2018) should be viewed as an essential training goal and

one that needs proactive academic investment. The use of retrospective-timeline analysis as a tool to encourage this cognitive process during a CDX can lead to adaptive performance. This occurs when metacognitive skills and reflective practice are facilitated immediately prior to, midst, and on completion of work (Fadde & Klein, 2010).

Discussion and Analysis

Stakeholder Perspectives—Emphasis to the Participants

At the center of a CDX are the participants. The organizers aim to ensure the participants leave the exercise having gained a valuable learning experience. However, many stakeholders are involved in a CDX, and success can be expressed and measured differently depending on their perspective. In Figure 1, we have depicted the

various stakeholder categories and their goals regarding a CDX. The goals range from international/multi-sector collaboration and advanced scenario design to testing oneself and having a good time (in AM 2018, nearly 90% of BT members marked the latter in a multi-choice question about their goals, and more than 90% said they came to learn). Therefore, the success of an event varies depending upon the stakeholder's perspectives, for example, successful play versus ambitions satisfied. Figure 1 distinguishes four stakeholder categories. Event owners focus on demonstrating public-private partnership, civilian-military collaboration, event scale and complexity, and joint cyber-defense capabilities. Organizers and leaders are responsible for the event implementation, supporting proper advancement levels and engaging and realistic scenarios. The red team (RT) *extends* the organizers' stakeholder category, as usually, it simulates adversaries based on the scenario design. But RT might have specific goals related to offensive activities. CDX partners (e.g., BTs, and entity representatives within other teams) provide input to the event, which might imply partner product promotion, impressive public view, or demonstration of the partner team's capacity. Finally, in CDX, individual participants follow the order, perform the duty, do tasks as a challenge or come to have a good time by self-testing. Therefore, success for owners and organizers might mean publicity and successful play, respectively. Partners could aim to make a good impression and gain experience. Individual participants provide positive feedback if they develop new skills or have satisfied ambitions because some identify the CDX as an opportunity to learn. The stakeholder goals may be competing, in some cases, they may be overlapping, and often they do not keep actual training audience needs in focus. Consequently, they may negatively impact participants' experience and thus need to be balanced and their impact considered from an emotional, social, and cognitive view.

Shortcomings in the Existing Approaches

The existing approaches where the multidimensional aspects, including multidisciplinary and soft skills, are ignored are insufficient and ineffective. We share experiences based on the authors' participation in CDXs, including LS and AM, and draw on multidisciplinary academic backgrounds to support our argument.

CDX and IT Curricula. A CDX brings together specialists (subject matter experts) from various IT domains—for example, system administrators, network analysts, and forensics experts, with experts from non-IT, but also inter-related domains, for example, legal, business, media. These experts may not have experienced a CDX

as part of their studies in their domain of interest and expertise. Specifically, computing curricula, where IT security is a critical element, do not provide a merged view of multidisciplinary competencies in cybersecurity.

CDX Lack of Educational Relationships. A CDX can be interpreted as a large-scale event that contains various teams (defending, offending, organizing, etc.), of which some may focus on defending (complex) systems allocated to them, while others may focus on attacking those systems, others maintaining the game infrastructure. It is often a team-based and competitive event focusing on time-to-fix or time-to-defend the problem or infrastructure. The setup is adopted from the Red versus Blue teams' "training" competition drills with extensive technical support capabilities, observer controllers, and simulation teams attached to the exercise. A CDX is often organized by large national or international organizations with relationships to defense or police forces and is vaguely supported by academia or applied education-sourced methodologies. For example, an objective driving the overall focus of a CDX is on incident reaction speed, that is, "Improving time management and prioritization." Often, such an objective is measured in time, for example, time to detect and time to mitigate. However, doing something fast does not necessarily mean doing it correctly. A time-constrained exercise design or unrealistic time pressure goals may prove instead to be an obstacle to learning and performance, for example, the wrong behavioral model is learned in the CDX and applied in real-life situations. The objective mentioned above should focus not only on time aspects but also on productive time usage, stress management, communication, and application of others, performance improvement, soft skills.

CDX Lack of Measurable Features, Especially for Soft Skills. Typically, the training objectives are defined at a high level, especially when talking about soft skills, for example, "improve team communication" or "improve inter-team collaboration," and measurements are not easy to carry out. Commonly used metrics are often simple technical ones, for example, time spent, number of attacks mitigated, service availability, and other individual timed actions. However, there should be a shift to measuring what we value as a qualitative result from inter-person and inter-group communication (Maennel, 2020). Therefore, if the training aims to foster team communication, we should start looking into communication patterns among team members, analyze the multitude of communication channels used, and if there are time delays or possible miscommunications, we should come to objective conclusions regarding why these happen.

Individual and Team/Group Formation. The cybersecurity environment is highly collaborative, involving many different roles and fluctuating team sizes. For very large-scale CDXs, teams are usually formed only a few weeks before the exercise and dissolve after the execution. Selection of team members with various capabilities, domain or system knowledge, and competencies is encouraged. The team and their communications need to be rebuilt each time the team (re)forms. However, refining the capabilities of an *ad-hoc* team would benefit primarily the partners and team leaders but not so much the individual participants. Team-based CDXs aim to create an active environment and provide teams, and individuals within teams, the opportunity to learn and (safely) practice their skills and strategies. An individual's domain-specific competence (or lack of competence) might cripple a team's performance. However, in many cases, teamwork can partially mitigate this negative occurrence. Group learning supports the development of critical thinking through discussion, clarification of ideas, and evaluation of others' ideas (Gokhale, 1995). Learning is seen as something that can be aided by experience, and in many cases, this is true. But practice does not make perfect, and it only makes it permanent. When a team fails, the reasons need to be understood. Group dynamics and group learning concepts play a crucial role in understanding this.

Competition Versus Learning. Often the larger exercises are seen as competitions, measurements, and assessments of skill. There can be a mismatch when technical participants perceive a CDX as a learning event, while managers and leaders may see it as a competition. While scoring can be a hygiene factor for skill improvement, it can also be (in a game-based learning context) a vital component for feedback. Even if scoring is anonymous, we could experience "informal" leaderboards emerging; thus, well-designed scoring methods that match learning objectives are critical. However, finding the relevant metrics for cognitive skills, and social and emotional elements is challenging.

Multidimensional Approach for a CDX

Reasons for a Different Approach

Multidisciplinary approaches in cybersecurity education have been talked about for many years, as they can facilitate critical and analytical thinking and good communication. Similar reasoning should expand to CDX.

How can we take a CDX to the next level to meet the demands of the digital era and multidisciplinary setting? Firstly, we need to address pedagogical and psychological fundamentals. What can we realistically teach with regards to advancing communication and other soft

skills, as well as addressing technical and transferable skills aspect? Will these interventions lead to improved actions and decision-making when implementing them into daily routines after the exercise is completed?

Learning can be viewed as three interrelated dimensions: content, incentive, and interaction, that is, the content to be learned involves the cognitive part of the learning, the mobilization of energy involving the emotional part of the learning, and interactions with the environment involving the social part of the learning (Illeris, 2016; Spelt et al., 2017), respectively. As a CDX is a simulation and involves certain elements of gamification, the principles of mechanics, dynamics, and emotions (i.e., Mechanics, Dynamics and Emotions [MDE] framework) apply (Robson et al., 2015) and support cognitive-emotional viewpoints (Mullins & Sabherwal, 2020). CDXs offer the perfect training ground for developing skills in all these dimensions, with a significant learning impact. For example, responding to a cyber critical incident can involve combining cognitive strategies (technical skills of hardening networks or monitoring networks and contributing to writing situation reports), emotional appraisals (fearing the possibility of human losses when mitigating attack on critical infrastructures), and social interactions (being part of the team).

Multidimensional Approach Focusing on Social, Emotional, and Cognitive Aspects

Building upon existing research (Illeris, 2016; Spelt et al., 2017), it is possible to adopt a multidimensional approach to a CDX. This task requires combining a developed cognitive repertoire with emotional and social dimensions. In addition, as a CDX often brings together varying competence levels, we need to understand and appreciate different learning foci. For example, a novice may struggle with applying individual technical skills in more complex incident response processes, while experts who have mastered content (cognitive) aspects may focus on social aspects, for example, building strong individual connections with team members. Thus, for a novice, there may be the need for a technical coach to support skill development, while the expert might prefer the availability of a socializing space for informal bonding. When we look at the feedback from a CDX (several years of AM execution), we can see trends covering cognitive, social, and emotional aspects. The most frequent items Liked and Disliked are categorized and presented in Figure 2. For example, *Environment* is an umbrella for a cozy atmosphere, organization, timely information, and coffee breaks. These factors support the psychological safety of the CDX participants. Coziness means time to reflect on the stressful and intense gameplay and the possibility to share insights with other participants. The

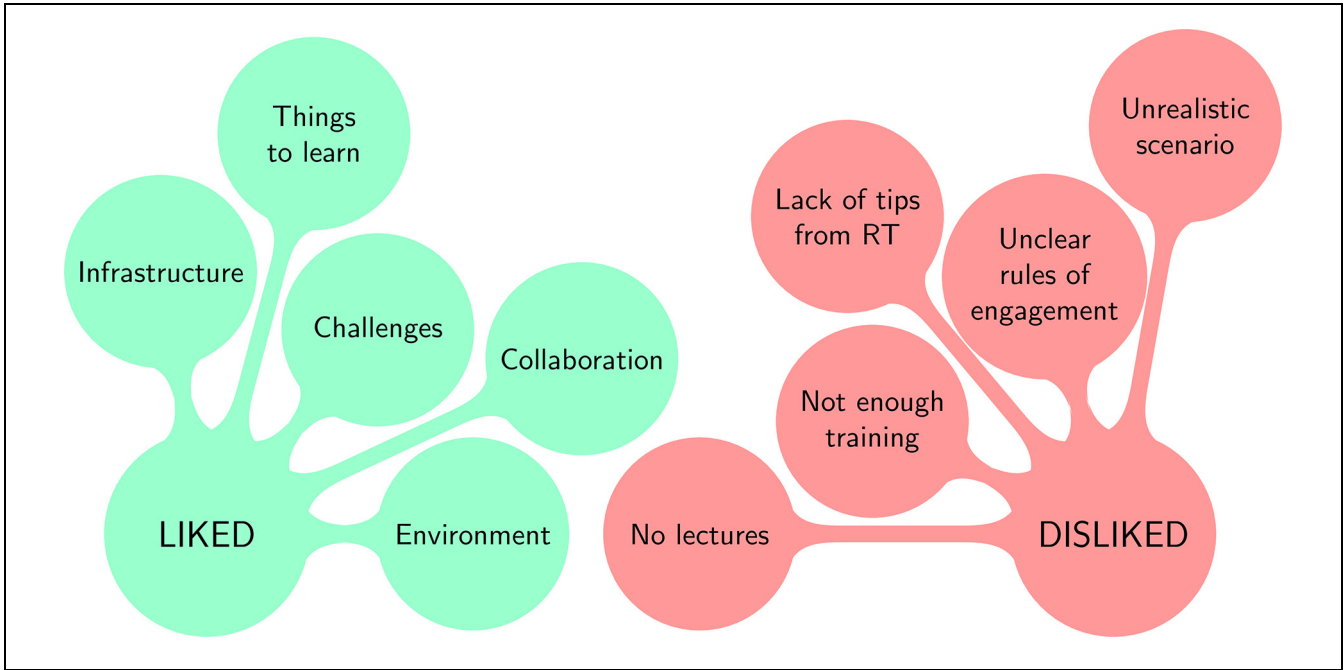


Figure 2. Likes and dislikes of CDX participants from Amber Mist CDX.

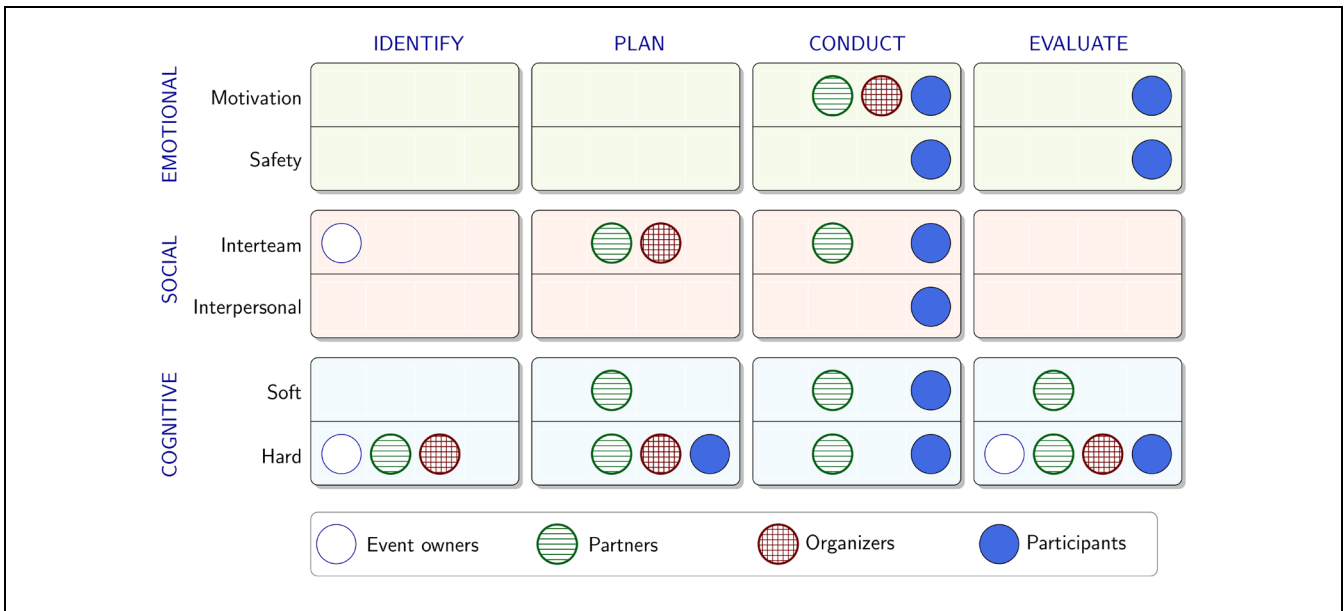


Figure 3. Current multidimensional view to CDX.

category *Collaboration* includes collaboration within and across teams and communication enabled by coffee time and rules allowing/suggesting to reach other blue teams. As for *Unclear rules* or *Not enough training*, participants felt uncomfortable due to the information lack or differences between the rules of the game and routine procedures, which led to some personal confusion. The social

and emotional needs seem to dominate the feedback even though most trainees came to learn as reported in the feedback.

The key activities are depicted in a multidimensional approach (see Figure 3) that needs to span across stakeholders’ goals and be incorporated within the CDX’s life cycle. The figure shows team involvement in CDX

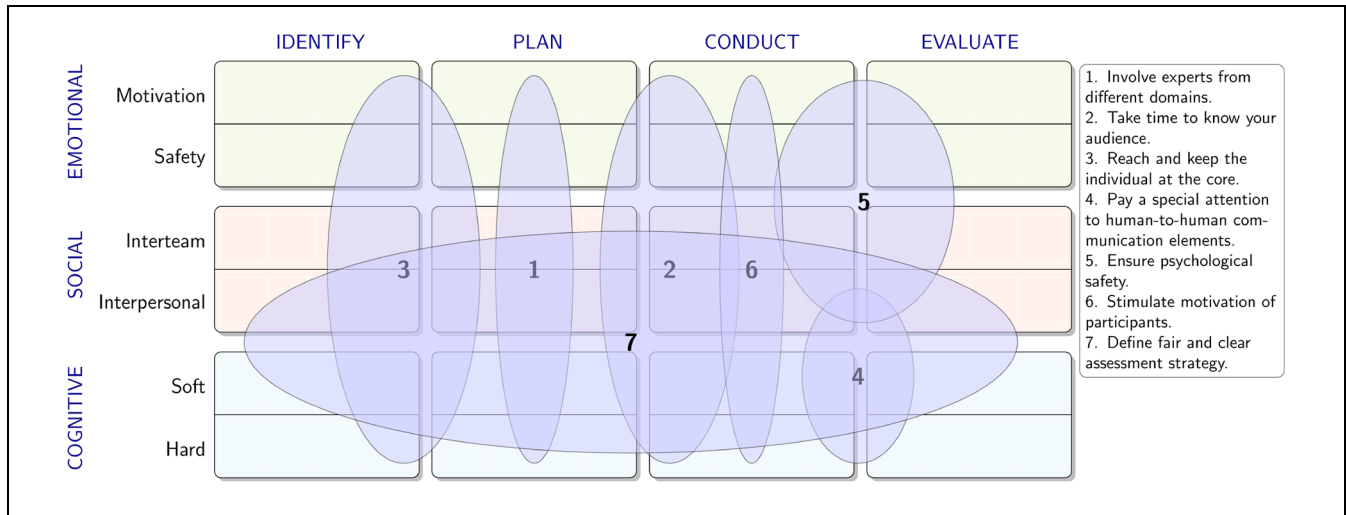


Figure 4. Mapping the ingredients to the multidimensional approach for a successful CDX.

activities related to cognitive, social, and emotional dimensions with exercise planning phases as circles. For example, in the Identify phase, event owners emphasize event objectives like fostering international communication (i.e., Social—Inter-team sub-dimension) or resilience against attacks from the technical perspective (i.e., Cognitive—Hard sub-dimension). Typically, the latter is a center for organizers and partners in this CDX phase. In the Conduct phase, the participant focus spans from Cognitive to Emotional due to a complex scenario, stress factors, and personal objectives.

While the organizers may not necessarily be in of control the participants' emotional, social, and cognitive aspects and rather it is a responsibility of the participants and teams and their representatives, the CDX owner(s) and organizers/leaders should emphasize and provide guidance how to achieve/strengthen these elements throughout the CDX life cycle. Using the multidimensional approach and balancing three dimensions (emotional, social, and cognitive) would support expertise levels (Garrett et al., 2009) building from novices to experts and from individual to team level.

Putting in Practice: Ingredients for Incorporating Social, Emotional, and Cognitive Aspects to CDX

CDXs should go beyond technical cybersecurity objectives. The planning of a CDX requires a multidimensional approach and significant consideration for the training audience and their broader emotional, social, and cognitive needs. Therefore, in order to support interdisciplinary critical thinking and expertise development while incorporating social, emotional, and cognitive access, we suggest the following *ingredients* for CDX organizers to keep in mind. In Figure 4, we map the

recommendations onto the same space of skills and CDX phases as in Figure 3. However, with numbered ellipses, we highlight essential ingredients to be used that span over dimensions independently of the CDX teams involved.

Involve Experts From Different Domains. Research (Bell et al., 2011) has shown repeatedly that diversity in disciplines and degrees of expertise increase a group's performance. Cross-domain communication is more demanding, but trains participants in perspective-taking and makes them more efficient in building situational awareness. Behavioral and cognitive scientists may contribute with insights regarding perceived difficulty, decision-making and communication processes, and defining human-factor-related learning outcomes.

Take Time to Know Your Audience. Emotional, cognitive, and social elements need to be balanced and adjusted based on the skill level of the training audience. Technical attack modeling and non-technical dimensions introduced to offer wider learning opportunities should be tailored to ensure competencies and expectations are met.

Reach and Keep the Individual at the Core. Organizers should be aware of the various and differing objectives and motivations, that the stakeholders bring with them. Taking these various demands into account, facilitates communication, cooperation, and overall motivation, resulting in improved learning outcomes.

Pay a Special Attention to Human-to-Human Communication Elements. *Ad-hoc* built teams of experts who are not familiar with each other, and particularly teams

containing explicitly or implicitly a strong hierarchical gradient, perform less efficiently. Organizers should give all participants the opportunity to communicate, even though only briefly, and become acquainted outside of the testing/training conditions. Even brief “ice-breaker” events have been shown to improve cooperation in complex problems through a facilitated and more open exchange of potentially critical information.

Ensure Psychological Safety. One of the strongest single predictors of team performance is “psychological safety.” This concept describes a group’s positive attitude toward the expression of individual opinions, even if they deviate from the majority or can not yet be supported by data or backed by formal qualifications. Questioning, criticizing, and expressing doubts at an early stage of a problem and regardless of the formal hierarchical position, provide the team with additional information, more effective exploitation of actually available competencies from within the team, and increases the probability of pro-active decisions. An atmosphere in which deviant perspectives and ways of thinking are more likely are those led by leaders showing a consultative leadership style (rather than an authoritarian or laissez-faire style), are typically characterized by cultural and hierarchical diversity, and include persons with diverse backgrounds in terms of expertise levels.

Stimulate Motivation of Participants. Motivation is a crucial success factor for sustainable learning. While gamification is a popular method to increase motivation, the factors contributing to gamification-induced motivation should be considered in order to maximize the effects. Three factors should be fulfilled: Relatedness means that the individual perceives his/her own goals as being at least partially overlapping with the group’s goal. Appreciation of effort by an important figure can contribute to this impression. The factor of competence means that a challenge is designed to create an individually demanding but manageable skill-challenge-ratio. Finally, participants should be placed in an autonomy-supportive environment, with the possibility to choose their actions and take responsibility for them. With these three factors given, the probability of sustained positive motivation to perform increases, and so do the quantity and quality of the learning outcomes.

Define Fair and Clear Assessment Strategy. Appropriate assessment strategies can assist learning outcomes. In traditional settings, *post-hoc* data collection or pre-post comparisons suffer from hindsight bias, and valuable information with relevance for the course of action gets lost. Therefore, brief and minimally invasive assessments of mental states, decision-making or perceived situational states (risk assessments, options on the table and

their perceived consequences) can contribute to a better understanding of the causal relationships of observed outcomes. Quick single self-assessment items can replace time-consuming questionnaires and provide a better temporal resolution of the obtained data and observations.

Assessment of the training audiences’ preparation phase prior to exercise start should be factored in, and one single After-Action Review (AAR) at the exercise end may not be sufficient to capture multiple dimensions of learning.

Conclusion

The CDX is a valued and critical component of cybersecurity education in academic and professional settings; however, these are not realized to the full potential in the current format. Due to the challenges of multidisciplinary cybersecurity, the CDX needs to cater to various individuals and teams to foster diverse skill development. To achieve this, we need to think beyond technical aspects. We deep-dived at the cognitive, social, and emotional aspects (Illeris, 2016) and analyzed these specifically in the CDX context. Based on this analysis, we derived seven ingredients that ensure the best combination to foster successful participation and learning in a CDX and keep the individuals and teams at the core. This balanced approach would help bring the CDX from the primarily technical training focus to the next level, where emotional, social, and cognitive learning needs are also addressed, catered for, and measured as performance indicators. Even though this paper used an example of a large CDX, the same approach can be used for other types of cybersecurity exercises, for example, tabletops, CTFs, and simulations.

Acknowledgments

The authors of the paper would like to express their gratitude to the organizers, participants, and the evaluation team of the international cybersecurity exercises Amber Mist 2018–2021 for the opportunity to gather the data.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding


The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The “Advancing Human Performance in Cybersecurity,” ADVANCES, benefits from nearly €1 million grant from Iceland, Liechtenstein, and Norway through the EEA Grants. The aim of the project is to advance the


performance of cybersecurity specialists by personalizing the competence development path and risk assessment. Project contract with the Research Council of Lithuania (LMTLT) No is S-BMT-21-6 (LT08-2-LMT-K-01-051).

Ethics Statement

Ethics approval was not required for this study as the research does not involve animal and human experiments.

ORCID iDs

Kaie Maennel  <https://orcid.org/0000-0002-3886-9532>

Agnė Brilingaitė  <https://orcid.org/0000-0001-9768-4258>

Notes

1. <https://ccdcoc.org/exercises/locked-shields>
2. https://www.nksc.lt/doc/en/NKSC_2019_EN.pdf

References

- Bell, S. T., Villado, A. J., Lukasik, M. A., Belau, L., & Briggs, A. L. (2011). Getting specific about demographic diversity variable and team performance relationships: A meta-analysis. *Journal of Management*, *37*(3), 709–743.
- Berki, E., Valtanen, J., Chaudhary, S., & Li, L. (2018). The need for multi-disciplinary approaches and multi-level knowledge for cybersecurity professionals. In E. Berki, J. Valtanen, S. Chaudhary, & L. Li (Eds.), *Multidisciplinary perspectives on human capital and information technology professionals* (pp. 72–94). IGI Global.
- Binyamin, G., Friedman, A., & Carmeli, A. (2018). Reciprocal care in hierarchical exchange: Implications for psychological safety and innovative behaviors at work. *Psychology of Aesthetics Creativity and the Arts*, *12*(1), 79–88. <https://doi.org/10.1037/aca0000129>
- Blair, J. R. S., Hall, A. O., & Sobieski, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer*, *52*(3), 58–66. <https://doi.org/10.1109/MC.2018.2884190>
- Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, *88*, 101607. <https://doi.org/10.1016/j.cose.2019.101607>
- Canham, M., Sütterlin, S., Ask, T. F., Knox, B. J., Glenister, L., & Lugo, R. (2022). Ambiguous self-induced disinformation (ASID) attacks: Weaponizing a cognitive deficiency. *Journal of Information Warfare*, *21*(3), 43–58.
- Carmeli, A., Brueller, D., & Dutton, J. E. (2009). Learning behaviours in the workplace: The role of high-quality interpersonal relationships and psychological safety. *Systems Research and Behavioral Science*, *26*(1), 81–98. <https://doi.org/10.1002/sres.932>
- Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A Delphi method-based study. *Computers & Security*, *113*, 102551. <https://doi.org/10.1016/j.cose.2021.102551>
- Coetzee, M. (2019). Organisational climate conditions of psychological safety as thriving mechanism in digital workspaces. In M. Coetzee (Ed.), *Thriving in digital workspaces* (pp. 311–327). Springer.
- Corley, K. G., & Gioia, D. A. (2011). Building theory about theory building: What constitutes a theoretical contribution? *Academy of Management Review*, *36*(1), 12–32. <https://doi.org/10.5465/amr.2009.0486>
- Cruz, T., & Simões, P. (2021). Down the rabbit hole: Fostering active learning through guided exploration of a scada cyber range. *Applied Sciences*, *11*(20), 9509.
- Deci, E. L., Olafsen, A. H., & Ryan, R. M. (2017). Self-determination theory in work organizations: The state of a science. *Annual Review of Organizational Psychology and Organizational Behavior*, *4*, 19–43. <https://doi.org/10.1146/annurev-orgpsych-032516-113108>
- Deci, E. L., & Ryan, R. M. (1985). The general causality orientations scale: Self-determination in personality. *Journal of Research in Personality*, *19*(2), 109–134. [https://doi.org/10.1016/0092-6566\(85\)90023-6](https://doi.org/10.1016/0092-6566(85)90023-6)
- Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, *44*(2), 350–383.
- Edmondson, A. C. (2018). *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. John Wiley & Sons.
- Edmondson, A. C., & Verdin, P. J. (2018). The strategic imperative of psychological safety and organizational error management. In J. Hagen (Ed.), *How could this happen?* (pp. 81–104). Springer.
- Fadde, P. J., & Klein, G. A. (2010). Deliberate performance: Accelerating expertise in natural settings. *Performance Improvement*, *49*(9), 5–14. <https://doi.org/10.1002/pfi.20175>
- Garrett, S. K., Caldwell, B. S., Harris, E. C., & Gonzalez, M. C. (2009). Six dimensions of expertise: A more comprehensive definition of cognitive expertise for team coordination. *Theoretical Issues in Ergonomics Science*, *10*(2), 93–105. <https://doi.org/10.1080/14639220802059190>
- Gay, B., & Weaver, S. (2011). Theory building and paradigms: A primer on the nuances of theory construction. *American International Journal of Contemporary Research*, *1*(2), 24–32.
- Gokhale, A. A. (1995). Collaborative learning enhances critical thinking. *Journal of Technology Education*, *7*(1), 22–30. <https://doi.org/10.21061/jte.v7i1.a.2>
- Hannafin, M. J., & Hannafin, K. M. (2010). Cognition and student-centered, web-based learning: Issues and implications for research and theory. In J. Spector, D. Ifenthaler, P. Isaias, Kinshuk, & D. Sampson (Eds.), *Learning and instruction in the digital age* (pp. 11–23). Springer.
- Hattie, J., & Timperley, H. (2007). The power of feedback. *Review of Educational Research*, *77*(1), 81–112. <https://doi.org/10.3102/003465430298487>
- Hautamäki, J., Karjalainen, M., Hämäläinen, T., & Häkkinen, P. (2019). *Cyber security exercise: Literature review to pedagogical methodology*. INTED Proceedings 2019.
- Hutton, R., & Turner, P. (2019). *Cognitive agility: Providing the performance edge*. Retrieved February 11, 2023, from <https://wavellroom.com/2019/07/09/cognitive-agility-providing-a-performance-edge/>
- Illeris, K. (2016). *How we learn: Learning and non-learning in school and beyond*. Routledge.

- Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal*, 33(4), 692–724. <https://doi.org/10.5465/256287>
- Karjalainen, M., Kokkonen, T., & Puuska, S. (2019, June 17–19). *Pedagogical aspects of cyber security exercises* [Conference session]. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden. <https://doi.org/10.1109/EuroSPW.2019.00018>
- Karjalainen, M., Puuska, S., & Kokkonen, T. (2020). *Measuring learning in a cyber security exercise* [Conference session]. 2020 12th International Conference on Education Technology and Computers, London, United Kingdom. <https://doi.org/10.1145/3436756.3437046>
- Knox, B. J., Lugo, R. G., Helkala, K., & Sütterlin, S. (2019). Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower. *International Journal of Cyber Warfare and Terrorism*, 9(1), 48–66. <https://doi.org/10.4018/IJCWT.2019010104>
- Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019). Cognisance as a human factor in military cyber defence education. *IFAC-PapersOnLine*, 52(19), 163–168. <https://doi.org/10.1016/j.ifacol.2019.12.168>
- Maennel, K. (2020, September 7–11). *Learning analytics perspective: Evidencing learning from digital datasets in cybersecurity exercises* [Conference session]. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy. <https://doi.org/10.1109/EuroSPW51379.2020.00013>
- Mäses, S., Maennel, K., Toussaint, M., & Rosa, V. (2021, September 6–10). *Success factors for designing a cybersecurity exercise on the example of incident response*. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Vienna, Austria. <https://doi.org/10.1109/EuroSPW54576.2021.00033>
- Mullins, J. K., & Sabherwal, R. (2020). Gamification: A cognitive-emotional view. *Journal of Business Research*, 106, 304–314. <https://doi.org/10.1016/j.jbusres.2018.09.023>
- Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59(3), 1065–1078. <https://doi.org/10.1016/j.compedu.2012.04.016>
- Nyre-Yu, M. (2021). *Identifying expertise gaps in cyber incident response: Cyber defender needs vs. technological development* [Conference session]. 54th Hawaii International Conference on System Sciences. <https://doi.org/10.24251/HICSS.2021.242>
- Ogee, A., Gavrilas, R., Trimintzios, P., Stavropoulos, V., & Zacharis, A. (2015). *The 2015 report on national and international cyber security exercises: Survey, analysis and recommendations*. ENISA.
- Omar, T., Venkatesan, S., & Amamra, A. (2018). *Development of undergraduate interdisciplinary cybersecurity program: A literature survey* [Conference session]. 2018 ASEE Annual Conference & Exposition. <https://doi.org/10.18260/1-2-30331>
- Reiss, S. (2004). Multifaceted nature of intrinsic motivation: The theory of 16 basic desires. *Review of General Psychology*, 8(3), 179–193. <https://doi.org/10.1037/1089-2680.8.3.179>
- Roberto, M. A., Bohmer, R. M., & Edmondson, A. C. (2006). Facing ambiguous threats. *Harvard Business Review*, 84(11), 106–157.
- Robson, K., Plangger, K., Kietzmann, J. H., McCarthy, I., & Pitt, L. (2015). Is it all a game? understanding the principles of gamification. *Business Horizons*, 58(4), 411–420. <https://doi.org/10.1016/j.bushor.2015.03.006>
- Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2021, October 13–16). *Reinforcing cybersecurity hands-on training with adaptive learning* [Conference session]. 2021 IEEE Frontiers in Education Conference (FIE), Lincoln, NE, United States. <https://doi.org/10.1109/FIE49875.2021.9637252>
- Spelt, E. J. H., Luning, P. A., van Boekel, M. A. J. S., & Mulder, M. (2017). A multidimensional approach to examine student interdisciplinary learning in science and engineering in higher education. *European Journal of Engineering Education*, 42(6), 761–774. <https://doi.org/10.1080/03043797.2016.1224228>
- Tsado, L. (2019). Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach. *Journal of Cybersecurity Education, Research and Practice*, 2019(1), 4.
- Turner, G. R., Novakovic-Agopian, T., Kornblith, E., Adnan, A., Madore, M., Chen, A. J. W., & D'Esposito, M. (2020). Goal-oriented attention self-regulation (goals) training in older adults. *Aging & Mental Health*, 24(3), 464–473. <https://doi.org/10.1080/13607863.2018.1534080>
- Ward, L., Grudnoff, L., Brooker, B., & Simpson, M. (2013). Teacher preparation to proficiency and beyond: Exploring the landscape. *Asia Pacific Journal of Education*, 33(1), 68–80. <https://doi.org/10.1080/02188791.2012.751896>
- Ward, P., Gore, J., Hutton, R., Conway, G. E., & Hoffman, R. R. (2018). Adaptive skill as the *conditio sine qua non* of expertise. *Journal of Applied Research in Memory and Cognition*, 7(1), 35–50. <https://doi.org/10.1016/j.jarmac.2018.01.009>
- Zeng, H., Zhao, L., & Zhao, Y. (2020). Inclusive leadership and taking-charge behavior: Roles of psychological safety and thriving at work. *Frontiers in Psychology*, 11, 62. <https://doi.org/10.3389/fpsyg.2020.00062>