Pedagogical Aspects of Cyber Security Exercises

Mika Karjalainen, Tero Kokkonen, Samir Puuska
Institute of Information Technology
JAMK University of Applied Sciences
Jyväskylä, Finland
email: {mika.karjalainen, tero.kokkonen, samir.puuska}@jamk.fi

***Abstract*—Cyber security exercises (CSE) are complex learning experiences aimed at developing expert knowledge and competence through simulation. In this paper we examine pedagogical issues relating to CES, from exercise design to training results and evaluation. In addition, we present a Deliberate Practice - oriented view on expert and competence development for CSEs. We use data gathered from multiple CSE cases, where we have collected field notes, observations, questionnaire results, and other documentary data while organizing these training events.**

Based on our observations and analysis, integrating pedagogical knowledge and focus with each phase in the CSE lifecycle, i.e. planning, implementation, and feedback phases, the training effectiveness can be improved. We also note that CSE evaluation requires systematic measurements of change ranging from customer experience to organizational change. We also outline avenues for further work relating to various aspects of expert knowledge development and training evaluation in the context of CSEs.

***Index Terms*—cyber security exercise, expert performance, collaborative simulation, simulation pedagogy**

I. Introduction

Cyber security exercises (CSE) are increasingly seen as an important part of personnel training in both commercial and governmental contexts. At present, there exist a gap in research as to how these live exercises should be organized around competence development.

In this paper we present a competence development oriented view on CSE lifecycle, and examine how different components of an exercise could benefit from targeted learning outcomes. We also outline common challenges that often present themselves during various parts of the exercise lifecycle.

JAMK University of Applied Sciences has operated cyber security research, training and development center JYVSECTEC (Jyväskylä Security Technology) since 2011 [1]. JYVSECTEC has conducted the Finland's national cyber security exercise annually since 2013 [2] and, in addition, a large number of different types of CSEs for authorities and companies with critical infrastructure. The Ministry of Defence of Finland announced JYVSECTEC cyber range as a national range in the European Defence Agency's Cyber Range project [3]. Typical number of participants in a national exercise is between 100 to 150 people. Commercial companies operating in critical infrastructure sectors are often exercising with their partners or subcontractors. These exercises typically involve 50 to 100 people. SMEs with their partners usually have 10 – 30 participants in live exercises. When Capture-the-Flag or digital forensics and incident response exercises are held, there are normally 10 to 20 participants. In the past 8 years approximately 1,500 people have participated in the exercise sessions at JYVSECTEC. The data for this multiple-case design comes from documentary data, field notes, observations, and questionnaire results the authors have collected from organizing live CSEs at JYVSECTEC.

The aim of this research is to gain more detailed understanding of the pedagogical principles when using the CSE as a method to educate individuals and organizations to understand the cyber domain. For understanding the overall complexity of cyber domain, the need for CSEs has increased rapidly [4], [5]. Many countries have built up their cyber range facilities, and the latest projects have been aimed to interconnect the existing ranges for arranging mutual exercises between countries [6].

Traditionally, the field of engineering education emphasizes the need of training to learn and apply it in practice. Therefore, in engineering education different types of learning environments simulating real operating environments or facilities have been used as a learning tool for decades. In the field of ICT, information network laboratories and project-based learning environments have been widely used especially in applied software engineering. The current cyber security environment has brought new challenges to teaching. By using traditional teaching environments, it has been possible to teach the areas of expertise that the cyber security expert needs in necessary detail. However, the current environment requires a more holistic approach that integrates discrete skills and fosters understanding of the whole landscape, so that the importance of cause-and-effect relationships in the whole cyber context are understood. From the point of pedagogical frameworks, research related to simulation environments has been made especially in the applied health simulation teaching [7]–[9]. These studies are also applicable to cyber security teaching, but further need for applied research, especially of using cyber range as simulation environment, is obvious.

Lehto et al. [10] highlighted that in the research of cyber security the human factor is missing almost completely in the current literature. The importance of human sciences in technology developmental and cross-disciplinary cyber security issues research is still very limitedly understood. Thus, this research is focused specifically to the pedagogical factors of CSEs, and developing more detailed understanding on how the CSEs should be utilized in cyber security skills education.

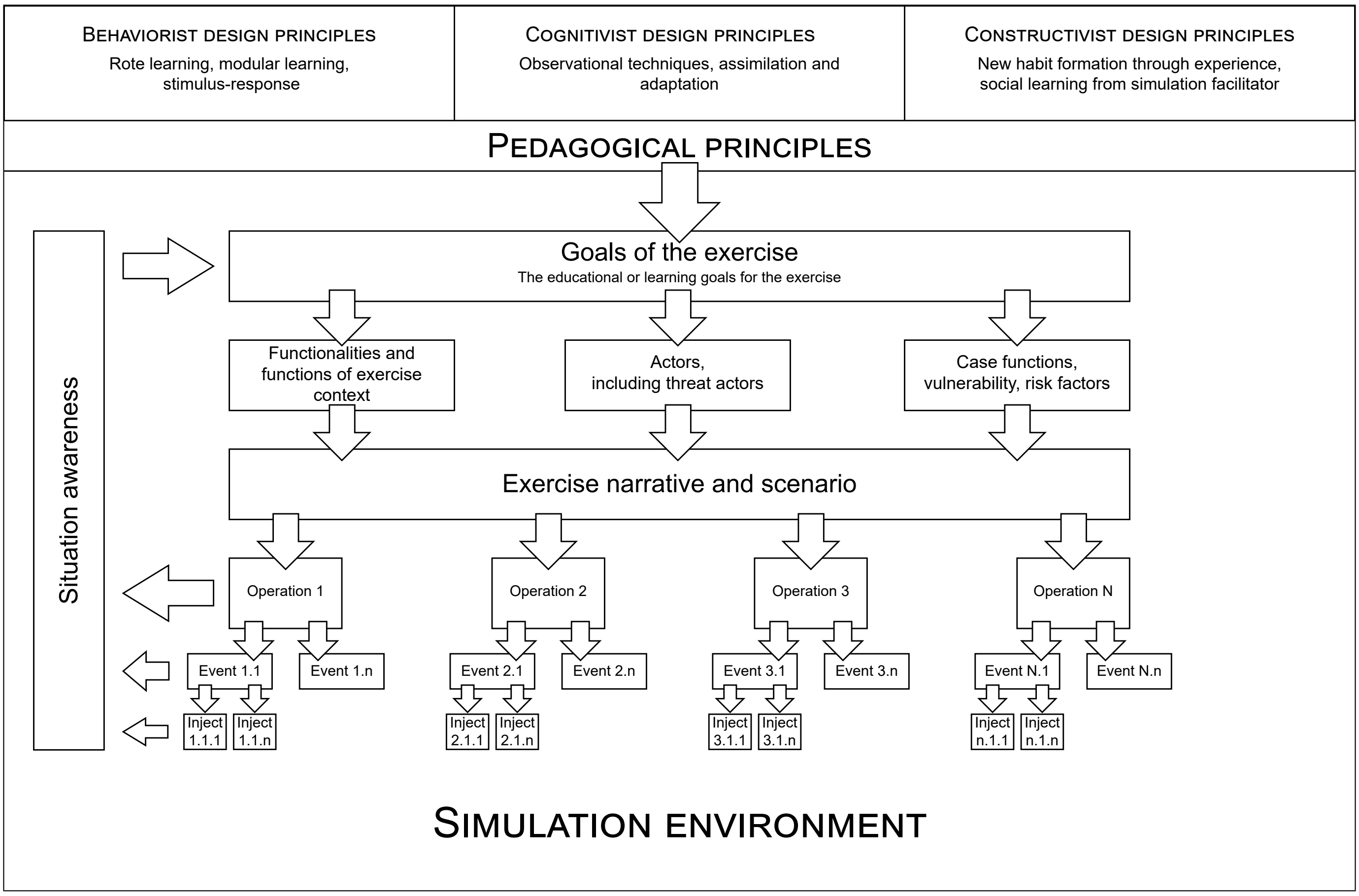
BEHAVIORIST DESIGN PRINCIPLES
Rote learning, modular learning, stimulus-response
COGNITIVIST DESIGN PRINCIPLES
Observational techniques, assimilation and adaptation
CONSTRUCTIVIST DESIGN PRINCIPLES
New habit formation through experience, social learning from simulation facilitator
PEDAGOGICAL PRINCIPLES
Situation awareness
Goals of the exercise
The educational or learning goals for the exercise
Functionalities and functions of exercise context
Actors, including threat actors
Case functions, vulnerability, risk factors
Exercise narrative and scenario
Operation 1
Operation 2
Operation 3
Operation N
Event 1.1
Event 1.n
Event 2.1
Event 2.n
Event 3.1
Event 3.n
Event N.1
Event N.n
Inject 1.1.1
Inject 1.1.n
Inject 2.1.1
Inject 2.1.n
Inject 3.1.1
Inject 3.1.n
Inject n.1.1
Inject n.1.n
SIMULATION ENVIRONMENT

Fig. 1. Cyber exercise simulation environment and the content of exercise life-cycle sections.

II. Pedagogy in Cyber Security Exercises

Live CSEs are mostly used to train or assess experts. This means that in order to create efficient learning environments we must understand how expertise works, and which training methods will provide increase in expert performance [11]. Ericsson, in their theory of deliberate practice (DP), argued that this specialized form of practice is necessary component if increase in expert performance is desired [12]. According to Ericsson, experts need well thought-out and specified goals that seek to improve a particular area of their domain. Ericsson argues that experts will not benefit or improve, if the tasks can be accomplished in an automated fashion; in other words, if conscious control is not required the expert can not spot what they should improve. Since DP is aimed at developing expert knowledge, it seems plausible that people who have not attained the highest level on Miller's pyramid [13] of competence lack the necessary experience to fully benefit from this approach.

Skills are often built with lecture-like teaching in the sense of behavioral learning, where the importance of the teacher's lecture material is central. When a student's knowledgeable capacity grows, their cognitive data processing increases, and the student ties in information he has learned earlier, selects the application of knowledge and builds meanings. This is cognitive learning approach that needs to be present when building the deeper knowledge of a subject [14]. In accordance with constructivist learning approach, commonly used learning and teaching methods are problem based learning (PBL) and exploratory learning [15], [16]. Problem based learning often starts directly with solving a real problem and exploring the related background information. Exploratory learning uses the same method. The idea is to react to learning as a researcher. The idea is to set meaningful and interesting questions from the topic to be learned and then solve them. Problem-based teaching practically resembles scientific research. Theoretical parsing of learning places the focus to be on the communities and networks, as well as in the learning and interaction therein, rather than the individual. At CSE, the pedagogical frame of the exercises is based on all these different pedagogical approaches and on combining the needed elements from the different stages of know-how building process (Figure 1). From the perspective of constructivist approach to learning this means that a participant in CSE needs to have a sufficiently high level of competence to be able to tie the educational objectives of the exercise to previously acquired knowledge. European Qualifications Framework (EQF) [17] describes eight different levels of learning outcomes. These learning outcomes consist of knowledge, skills, responsibility and autonomy. Competence is defined by EQF as the proven ability to use knowledge, skills and personal, social and/or methodological abilities in work or study situations.

III. Exercise Life-cycle

Cyber security exercise can be seen as a three phase process [18]: (i) planning phase that identifies the scope and objectives for the exercise, (ii) implementation, the exercise conduct phase where the plans are realized, and (iii) feedback, an evaluation phase where the whole process is analyzed and improved. The stages are also congruent with the stages described by MITRE [19] *Exercise Planning, Exercise Execution and Post Exercise*. Furthermore, the Homeland Security Exercise and Evaluation Program (HSEEP) which provides a set of guiding principles for exercise programs has similar phases, i.e. *Exercise Design, Exercise Conduct and Evaluation* [20]. In essence, each stage is affecting the other as exercises are held repeatedly. Moreover, we have observed that in practice the first two stages will overlap.

A. Planning Phase

The first stage, from a competence development standpoint, determines how effective and useful the later stages are. Almost in all cases, the exercise needs to be scoped to fit a certain subset of an organization.

Figure 1 illustrates how the exercise goals are derived from the pedagogical principles. Based on the desired learning outcomes and the organization in question, various exercise parameters are extracted from the goals and formulated into the exercise narrative. The goals will also define the operational environment (functionalities, threat actors, risks and vulnerabilities) that is to be included in the scenario. This scoping defines the simulation environment that has to be created for the exercise. The exercise scenario is further divided into discrete events and injects. They describe in detail what activity is going to be simulated during the run of a CSE. It is crucial that the role for each person participating in the exercise is well defined. There are several ways of constructing the game scenario, but it is often based on factors such as the threat model, available personnel, and specific skills or capabilities that have been selected after deliberation. The link between a game's scenario and the desired learning outcomes should be detailed at the level where each element and event in-game can be tied to a specific learning goal. Various frameworks have been created to categorize personnel and skills. For example, the NIST's NICE Framework [21] offers lists of specialty areas, work roles, tasks, skills, and abilities for constructing adequately detailed plans. This also allows creating a technical environment that serves the goals. If the plan is not accurate or detailed enough, the resulting technical environment is not tuned to support DP, and may fail to increase expert performance.

All of the above provide technical requirements that should be fulfilled when placing the attendee into a pedagogical situation such as a CSE. If the planning fails to produce detailed plans, the resulting technical environment might not develop the attendees' competences as expected.

Even though the technical environment might be on-par with the plans, the organization of the exercise into teams and responsibilities might fail. We have observed that the teams might (given the freedom) organize themselves less than optimally, and technical injects might not be detected. This can be remedied by the organizer; however, it sometimes lowers the motivation of the participant(s).

Planning a large-scale live CSE is a complex task where various constraints, such as money, planning time, availability of experts, and other practical factors limit the available resources. The process involves interviewing various persons, especially in cases where the exercise organizers are not domain experts on the field, e.g. military or aviation, and require additional support from the organization that contracted them. We have observed that these interviews have difficulties in maintaining their focus and scope, which degrades the quality of communication leading to suboptimal results. It seems likely that methods such as the semi-structured interview could improve the quality of communication, thus improving the results. In terms of future research, it would be beneficial to develop such a framework for CSE purposes.

B. Implementation Phase

The implementation phase differs from the other two stages in many crucial ways. Firstly, the time span for this stage is usually between one to five days. Secondly, the focus is on directing the exercise in a way that all planned objectives are achieved. This introduces the need for maintaining situation awareness (SA) on the exercise at all times. Moreover, since SA is an integral part of expertise, it is usually included in the list of skills that are under training [22], [23]. In other words, one of the challenges in conducting CSEs is in maintaining overall SA on the experts' SAs under training. SA allows the white team (WT) to observe the participants' decisions concerning all the operation lines. At this point, it is crucial also to verify the events and incidents handling from the participants' side. If it seems that participants are not responding to the incidents the way that the goals of learning are fulfilled, the WT will adjust the incidents in a way that the learning goals are reached. The most common way of doing this is to launch new planned incidents that will bring the needed information for the participants and practically guide them towards the set learning goals.

Classical model for decision making in tactical environment is Boyd's OODA loop (Observe-Orient-Decide-Act). Especially the modified version of OODA loop that regards the individuals' background and previous experiences in the Orient phase suits for decision making in cyber domains [24]. Authors of [25] have introduced the cognitive model of OODA loop that improves the level of granularity by considering Endsley's Situation Awareness theory [26] and Klein's Recognition-Primed Decision model [27]. These theories provide the basic for decision making and expertise including learning in stressful and complex CSEs.

In their paper, Lif et al. have studied information elements that should be used in the cyber-incident report during the exercises for a certain professional role known as log analyst [28]. That kind of element focusing can also be used for the competence development for certain roles in the exercises.

C. Feedback Phase

From the perspective of individuals' learning, the feedback phase is most important phase of the exercise. Thus, sufficient time should be reserved for feedback phase. In the feedback phase, all the main operation lines and events have to be gone through. This allows the participants to ask questions concerning the events that they have been phased during the exercise. In many cases it is essential to go into the details of certain incidents and explain how they had been executed, how the participants had responded and what else they could notice or do concerning the incidents. This allows the needed reflection for the participants and leads to understanding and hopefully to achievement of the set learning objectives. Based on our experiment, all the different actors of exercises need to participate in the feedback phase.

IV. Assessing Performance and Results

Evaluation is needed for assessing the effectiveness of a training program [29]. Kirkpatrick has divided program evaluation into four levels: (i) reaction, (ii) learning, (iii) behavior, and (iv) results [30]. The first level, reaction, is the reaction of the participants towards the training. Kirkpatrick characterizes this level as akin to "customer satisfaction". At this level Kirkpatric proposes that forms could be used for estimating how participants felt about the training event [30]. The second level, learning, is defined as the participants improving their knowledge, skills, or attitudes. Kirkpatrick et al. recommend using control groups and tests for assessing learning. They also note that measuring learning is more difficult and time-consuming than reaction measurement [29]. The third level, behavior, refers to the transfer of learned knowledge and skills to actual change in behavior at the actual job or task the participant does at their workplace. Kirkpatrick et al. note that this transfer is hard to measure, in part because the change is not instant; the individual has to have an opportunity for utilizing what they have learned. They recommend using surveys and interviews for assessing if behavioral changes have occurred, after adequate amount of time has passed from training event. The fourth level, results, refers to the final results that occurred because of the training program. These include increases in quality and productivity, and ultimately general return of investment from the training. Kirkpatrick et al. note that assessing these effects is difficult, and much of the same recommendations as for level three are applicable here. They also mention that absolute proof may not be cost-effective to obtain; instead the circumstantial evidence should suffice. [29], [30]

In CSEs the reaction measurements can be made using questionnaires. In addition to customer satisfaction forms, we have, on occasion, included other assessment tools such as the NASA Task Load Index (TLX) [31] for additional measurement. These provide a picture on customer opinion and whether the exercise was demanding enough for its purpose considering the desired learning outcomes. The tools have revealed that much care should be placed to task load planning. Although it may not be appropriate to equalize task loads between participants, there should be more than an occasional task for everyone.

Level two, learning, is considerably more challenging to measure in cyber training contexts. In expert training a simple written test, as Kirkpatrick et al. recommend as a practical instrument, is not applicable. It seems plausible that a more open questionnaire could provide more insight on what has been learned, and further aid in assessing if learning outcomes were met. This questionnaire could be drafted in exercise design phase to reflect the selected learning outcomes. The challenge is in creating a questionnaire that can reliably be used in assessing expert learning. An online evaluation for this level may be feasible, but the details remains a topic for further reseach.

Level three, behavior, is even more challenging to measure. We believe that in a frame of just one exercise there is no way to measure long term effects like changes in behavior, in part because the changes are not immediate; the individual needs time to utilize newly learned matters, and then be able to apply them in a real-world situation in order for them to turn into behavioral patterns. Nevertheless, measuring behavioral changes remains important aspect of any training program's result, as Kirkpatrick et al. point out. A feasible way of doing this assessment would be interviewing people when they return to participate next training program. One major obstacle here is that often there is a need to train persons who were not present in the first program. Questionnaires, both online and offline, may not be flexible enough for measuring training at this level. Semi-structured interviews with key personnel before the next training cycle could provide some insights on behavioral changes.

Level four, results, is the hardest level to assess also in cyber security training context. Agrafiotis et al. have created a taxonomy of "cyber-harms" [32]. They have identified five main harm types: (i) physical and digital harm, (ii) economic harm, (iii) psychological harm, (iv) reputational harm, and (v) social and societal harm. All of these types should be taken into account when assessing what positive effects and, ultimately, results one gets by participating a particular training program.

It is worth repeating that many of the assessments Kirkpatrick et al. recommend are only possible if training is repeated. In other words, a continuous training cycle allows organizations to truly assess how the training benefits them. This observation has been made also in the Cybersecurity Strategy of the European union, and the national cyber security strategy of Finland, among others [33], [34].

V. Conclusion

When dealing with cyber domain, the complexity of the operating environment and the predictability of causal and consequence relationships must always be taken into account. When it comes to teaching skills needed in this environment, the learning environment should be as realistic as possible. Thus, high demands are placed for the simulated environment in CSEs. The environment must therefore be of a sufficiently high standard and allow the needed complexity and realism. If the requirements for a simulated operating environment can be met, CSE is an excellent learning tool for cyber professionals.

As we introduced in exercise lifecycle section, the learning goals of exercises should be considered at all stages of the exercise life cycle. In the planning phase, the objectives of the exercise learning are determined in accordance with the objectives set the operational lines enabling the learning goals set for the participant to be implemented during the implementation phase, and the feedback stage ensures that all learning is possible through detailed level. It is also advisable to allow the material to be shared from the exercise so that the participants are able to return for the details after the exercise. Too often, CSEs focus on technical phenomena without considering what the primary goals set for the exercise are. In an exercise this way executed, the experience of the participants may be left behind to identify the specific technical phenomena instead of the learning that is being targeted. When the learning goals of the exercises are set, a commonly accepted frame such the NICE frame should be used. Using the frame enables a consistent structure implementation of the learning outcomes in the internal structure of exercise; namely, functionalities, processes, threat actors and determination of risk factors, different operation lines, event and inject that are being executed in exercise.Future research should focus on the levels of learning and behavior in Kirkpatrick taxonomy in the context of CSEs. Even though it is important to focus on the individual, the organizational focus should not be overlooked. Accordingly, it is vital to study how CSEs change the behavior of both the individual and and the organization, and ultimately, the cyber resilience capability of the whole society.

References

[1] JAMK University of Applied Sciences, Institute of Information Technology, JYVSECTEC, "Jyväskylä security technology," http://www.jyvsectec.fi/en/, Accessed: 7 February 2019.

[2] Ministry of Defence Finland, "The national Cyber Security Exercise is organised in Jyväskylä - Kansallinen kyberturvallisuusharjoitus KYHA18 järjestetään Jyväskylässä, Official Bulletin 11th of May 2018," https://www.defmin.fi/ajankohtaista/tiedotteet/2018?9610_m=9314, May 2018, Accessed: 7 February 2019.

[3] Ministry of Defence Finland, "Finland has the leader nation role in the EDA project - Suomelle johtovaltiorooli Euroopan puolustusviraston kyberhankkeessa, Official Bulletin 30th of June 2016," https://www.defmin.fi/ajankohtaista/tiedotteet/2016?8173_m=7894, June 2016, Accessed: 7 February 2019.

[4] The NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE, "Exercises," https://ccdcoe.org/exercises/, Accessed: 19 February 2019.

[5] B. Uckan Färnman, M. Koraeus, and S. Backman, "The 2015 report on national and international cyber security exercises : Survey, analysis and recommendations," Swedish Defence University, CRISMART (National Center for Crisis Management Research and Training), Tech. Rep., 2015. [Online]. Available: https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

[6] European Defence Agency, EDA, "Cyber ranges: Eda's first ever cyber defence pooling & sharing project launched by 11 member states," https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, Accessed: 4 February 2019.

[7] S. Nyström, J. Dahlberg, S. Edelbring, H. Hult, and M. Abrandt Dahlgren, "Debriefing practices in interprofessional simulation with students: A sociomaterial perspective," *BMC Med Educ*, vol. 16, no. 1, May 2016. [Online]. Available: http://dx.doi.org/10.1186/s12909-016-0666-5

[8] C. Kenaszchuk, K. MacMillan, M. van Soeren, and S. Reeves, "Interprofessional simulated learning: Short-term associations between simulation and interprofessional collaboration," *BMC Med*, vol. 9, no. 1, Mar. 2011. [Online]. Available: http://dx.doi.org/10.1186/1741-7015-9-29

[9] G. D. Erlam, L. Smythe, and V. Wright-St Clair, "Simulation is not a pedagogy," *OJN*, vol. 07, no. 07, pp. 779–787, 2017. [Online]. Available: http://dx.doi.org/10.4236/ojn.2017.77059

[10] M. Lehto, J. Limnéll, E. Innola, J. Pöyhönen, T. Rusi, and M. Salminen, "Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi," Prime Minister's Office, Tech. Rep., February 2017. [Online]. Available: https://tietokayttoon.fi/julkaisu?pubid=17805

[11] H. Collins and R. Evans, *A Sociological/Philosophical Perspective on Expertise: The Acquisition of Expertise through Socialization*, 2nd ed., ser. Cambridge Handbooks in Psychology. Cambridge University Press, 2018, p. 21–32.

[12] K. Anders Ericsson, "Deliberate practice and acquisition of expert performance: A general overview," *Academic Emergency Medicine*, vol. 15, no. 11, pp. 988–994, 2008. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1553-2712.2008.00227.x

[13] G. E. Miller, "The assessment of clinical skills/competence/performance," *Academic medicine*, vol. 65, no. 9, pp. S63–7, 1990.

[14] S. Lindblom-Ylänne and A. Nevgi, "The effect of pedagogical training and teaching experience on approach to teaching," in *11th EARLI conference, Padua*, 2003.

[15] J. R. Savery and T. M. Duffy, "Problem based learning: An instructional model and its constructivist framework," *Educational technology*, vol. 35, no. 5, pp. 31–38, 1995.

[16] M. Njoo and T. De Jong, "Exploratory learning with a computer simulation for control theory: Learning processes and instructional support," *Journal of Research in Science Teaching*, vol. 30, no. 8, pp. 821–844, 1993. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/tea.3660300803

[17] Official Journal of the European Union, "COUNCIL RECOMMENDATION of 22 May 2017 on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on the establishment of the European Qualifications Framework for lifelong learning," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H0615(01)&from=EN, Accessed: 14 February 2019.

[18] N. Wilhelmson and T. Svensson, *Handbook for planning, running and evaluating information technology and cyber security exercises*. The Swedish National Defence College, Center for Asymmetric Threats Studies (CATS), 2014.

[19] J. Kick, "Cyber exercise playbook," The MITRE Corporation https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf, 2014, Accessed: 19 February 2018.

[20] The Department of Homeland Security (DHS), "Homeland security exercise and evaluation program (hseep)," https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf, April 2013.

[21] W. Newhouse, S. Keith, B. Scribner, and G. Witte, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, Aug 2017. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-181

[22] M. R. Endsley, *Expertise and Situation Awareness*, 2nd ed., ser. Cambridge Handbooks in Psychology. Cambridge University Press, 2018, p. 714–742.

[23] P. Ward, A. M. Williams, and P. A. Hancock, *Simulation for Performance and Training*. New York, NY, US: Cambridge University Press, 2006, pp. 243–262, iD: 2006-10094-014.

[24] B. Brehmer, "The dynamic ooda loop: Amalgamating boyd's ooda loop and the cybernetic approach to command and control," in *10th International Command and Control Research and Technology Symposium, The Future of C2*, 2005.

[25] R. Breton and R. Rousseau, "The c-ooda: A cognitive version of the ooda loop to represent c2 activities," in *10th International Command and Control Research and Technology Symposium, The Future of C2*, 2005.

[26] M. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[27] G. Klein, *A Recognition Primed Decision (RPD) Model of Rapid Decision Making*, 01 1993.

[28] P. Lif, T. Sommestad, and D. Granasen, "Development and evaluation of information elements for simplified cyber-incident reports," in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, June 2018, pp. 1–10.

[29] D. L. Kirkpatrick and J. D. Kirkpatrick, *Evaluating Training Programs*. San Francisco: Berrett-Koehler Publishers, Inc., 2006.

[30] D. L. Kirkpatrick, "Evaluation of training," in *Training and Development Handbook*, L. R. Graig and L. R. Bittel, Eds. New York: McGraw Hill, 1967, pp. 87–112.

[31] S. G. Hart and L. E. Staveland, "Development of NASA-TLX (Task load index): Results of empirical and theoretical research," in *Advances in Psychology*. Elsevier, 1988, pp. 139–183. [Online]. Available: http://dx.doi.org/10.1016/s0166-4115(08)62386-9

[32] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, Jan. 2018. [Online]. Available: http://dx.doi.org/10.1093/cybsec/tyy006

[33] European Comission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," Feb. 2013.

[34] Secretariat of the Security Committee, "Finland's Cyber security Strategy, Government Resolution 24.1.2013," Jan. 2013.