Comprehensive Cyber Arena; The Next Generation Cyber Range

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

Abstract

The cyber domain and all the interdependencies between networked systems form an extremely complex ensemble. Incidents in the cyber domain may have an abundance effect on the physical domain. For example, a cyber attack or an intrusion against an electricity system may affect the performance of healthcare system as well. For organisation´s cyber resilience, know-how is the key resource. Cyber security training and exercises have an extremely important role for achieving the required level of know-how in the cyber domain. The old military based-proverb You Fight Like You Train is relevant in the cyber domain. Traditionally, the platform for cyber security training and exercises is called cyber range. Because of the accelerating digitalisation and more complex totality of the cyber domain, also the infrastructure for the cyber security training and exercises is required to be more and more complex. In this paper, the concept of cyber arena, next generation cyber range, is discussed.

Keywords

cyber security, cyber security exercise, cyber security training, cyber security exercise platform, cyber range, cyber arena

1. Introduction

Cyber security as a concept has become more widespread from the early 2010s because the fast growing digital world has brought in new classes of threats. The threats have grown more disruptive, which has led to the need to reassess and redefine the threat they pose to modern society. Naturally, the environmental change has reflected also on the requirements of education. The changes brought by digitalisation must be observed at all levels of education, and eventually digital skills should become part of our daily lives as new civic skills. One of the most important assets in cyber domain is know-how. It is achieved by training and exercises. Finland's new cyber security strategy [1] states that *the high level of education required by nationally critical cyber competence areas will be ensured. This is supported by both national and international training and exercises*. In addition, the cyber security strategy of the European Union [2] recognises the importance of cyber security training and exercises.

Cyber range performs as a technical platform for research & development and training & exercise in the cyber domain. Cyber range simulates the required networks and systems for supporting the research & development or training & exercises. Cyber range is a closed and the controlled environment with the required systems, tools and networks including a realistic Internet simulation with background traffic generation and user simulation. Because cyber range a closed environment, it is risk-free to use realistic cyber security threat environments with real attacks and intrusions [3]–[5].

In the field of training and exercise, cyber range can be equated as classical shooting range with capability to train and develop skills with weapons, operations or tactics [6]. One of the first cyber ranges was developed by the Defense Advanced Research Projects Agency (DARPA). DARPA realised the scientific advances of cyber security and requirements for research and development based on testing and experimentation. They developed the first version of national test bed that was later established as National Cyber Range (NCR) [5]. For example, paper [7] uses NCR as a blueprint of cyber range.

There are numerous different cyber ranges in the world, developed by industry, universities, research centres or national security organisations. The capabilities of those cyber ranges vary from laboratory based one server test bed infrastructures to massive virtualised Internet-kind of infrastructures. Yamin et.al [8] have conducted a literature review of cyber ranges and security testbeds including scenarios, functions, tools and architectures. As stated in [9], cyber ranges are often built for a specific purpose for fulfilling the narrow scale requirements of specific test scenarios. There also exist industry specific cyber ranges or test systems. He et al. [10] introduce a design of a cyber range test system for power industry, while Chen et al. [11] introduce a construction of cyber range in a power information system. Cybertropolis is a United States Department of Defense resource that can be seen as cyber-electromagnetic range including both kinetic and non-kinetic activities [12].

The perspective and requirements for developing the cyber ranges are often narrow and limited to a specific area of interest. Frank et al. [13] state that national cyber ranges are testbeds with command and control functionality, while the authors of [14] state that training environments are often not realistic enough. Paper [15] proposes a tool for creating an emulated network environment for cyber defence exercises while paper [16] introduces an architecture for cyber defence training and education. Cyber range is also effective for research and development activities, for example the authors of paper [17] utilised cyber range for deep learning based

DOI 10.1109/EuroS&PW51379.2020.00010

network security assessment and indication.

The complexity of networked systems has increased the effect of unexpected behaviours and dependences [18]. In that complex totality it is extremely important to understand what is happening in the cyber domain, what the statuses of the valuable assets are and how different dependencies affect to the valuable assets. In that sense, the Situational Awareness (SA) has an important role in the cyber domain. Debatty & Mees introduce cyber range for training the SA [19]. Because of the different capabilities of different cyber ranges and the growing requirement for simulating the complexity of the cyber domain, the Cyber Defence Pooling & Sharing Project of European Defence Agency (EDA) has recognised requirement for co-operation between national cyber ranges at the European level [20]–[22].

1.1. Motivation and Structure

As can be seen, the spectrum of cyber ranges is extremely heterogeneous and because of the evolution of cyber domain, there is a requirement for simulation of total complex cyber-physical environment with unexpected dependencies and consequences. Because of that, the new concept Cyber Arena (CA) is introduced and discussed.

The paper is organised as follows. In section 2, the pedagogical aspects for a complex system are discussed. According to that, the Cyber Arena (CA) is introduced in section 3. Lastly, in section 4, the study is concluded with emerging future research topics.

2. Pedagogical aspects for complex system

For decades, technical education has utilised learning environments that simulate real environments or functions as a learning tool. Information technology laboratories and project based learning have been widely used in the ICT field, particularly in applied software engineering studies. Cyber security has brought new challenges to ICT education. It has previously been adequate to teach spot-points from the individual areas of expertise using traditional teaching environments. However, by doing so the significance of cause-and-effect relationships will be missed. Furthermore, the learning goals for larger entities, such as an organisation's cyber security entity, may not be achieved. Often the effectiveness between the existing systems or their multiplier effects is difficult to predict and these elements also have to be included into training. From the viewpoint of pedagogical frameworks, research on simulation environments has been conducted, especially regarding the application of simulation teaching in healthcare [23]–[25]. In part, these studies are also applicable to cyber security teaching; however, the need for applied research, especially regarding the training and exercise environments (cyber range) built for cyber security teaching, is obvious.

In order to accommodate the changes driven by digitalisation in education and teaching, we need specific educational environments that model those complexities our societies increasingly rely on. In the digital business environment, it is typical that the in functionalities that are executed, the cause and effect relationships are difficult to understand. On the other hand, it can be said that it is crucial for the success of society and organisations that the skills of experts can be brought to a level where they can operate, develop and solve problems in the modern operating environments. New technologies require new skills from the experts, while the existing legacy systems still require administrator skills. Complex systems that are constantly evolving require risk-free, realistic learning environments where practical training and exercises can be provided for both beginners and advanced experts. It is not enough for knowledge to accumulate, but learning must aim at the level where specialists have the capability to react to real-life situations quickly with the right actions and in the face of ever more complex information entities. It is impossible to learn these skills without addressing these situations during training or exercise. Thus, according to Herrington and Oliver's theory of designing frameworks of authentic learning environments, continuous training is required in authentic learning environments, which refers to the accumulation of knowledge and skills in contexts that reflect the ways and environments where knowledge and skills will be used in real life [26]. The following list describes Herrington and Oliver's designing framework.

1) Provide authentic context that reflect the way the knowledge will be used in real-life
2) Provide authentic activities
3) Provide access to expert performances and the modelling of processes
4) Provide multiple roles and perspectives
5) Support collaborative construction of knowledge
6) Promote reflection to enable abstractions to be formed
7) Promote articulation to enable tacit knowledge to be made explicit
8) Provide coaching by the teacher at critical times, and scaffolding and fading of teacher support
9) Provide for integrated assessment of learning with in the tasks

In addition to the listed design criteria of authentic learning environment, it should be noted that also the pedagogical tasks that are executed in the environment should be designed by Authentic learning theory [27]. Collins [28] defines, that based on the theory of situated learning, when the new skills are learned and practised in an environment that reflects the real-life the new knowledge will also be useful in real life.

3. Comprehensive Cyber Arena

In order to fully achieve the educational goals so that the knowledge is applicable in the real environment, the cyber-training environment should be able to express cyber security phenomena and technology on a large scale. When considering cyber security, the complexity, difficulty to predict causal relationships, accountability, and other ecosystem-related phenomena need to be considered.

In the cyber ecosystem it must be taken into account that the influences and relationships of the actors are very sensitive and complex. For example, a company's cyber resilience consists not only of the security status of its own corporate network, but also of the security level of its partners, subcontractors, customers, service providers, and the critical infrastructure connected to it. In order to these ecosystemic influences to be reflected in teaching, the learning environment requires the ability to model the real environment and its phenomena at a sufficiently realistic level.

When describing cyber security training environments, there is an established term cyber range which is widely used. In their literary review Yamin [8] extensively mapped the existing cyber ranges. Based on Yamin's literature review, it can be said that the term cyber range can include many different uses, technical solutions and functionalities. Thus, the use of the term cyber range should be clarified in order to better identify the purpose, technical implementation or educational objectives of the environment. Many of the cyber ranges mentioned in Yamin's literature review focus on some aspect or functionality of cyber security. In order to be able to teach the ecosystemic influences of the real-world cyber operating environment in a sufficiently realistic operating environment, the training environment must be able to implement most of these functionalities.

An overall figure of Cyber Arena is shown in Figure 1. In Figure 1, Range 1 illustrates a cyber security training environment modelled on a single organisation's ICT architecture and business capabilities, including enterprise IT and OT operations. Range 2 illustrates a cyber security training environment modelling the ICT architectures of two or more organisations, enterprises' business as well as enterprise interdependences of ICT architecture and business. Range 3 illustrates a cyber security training environment modelling internet architecture and the different tier levels internet, enterprise business and ICT architecture, and the cloud architecture that is supporting the business. Range 4 illustrates a cyber security training environment which has the internet architecture, as well as the services used over the Internet and the cloud service architecture. National Initiative for Cyber security Education (NICE), led by the National Institute of Standards and Technology (NIST), has created a framework for managing the industry-based know how in the domain of cyber security [4]. The NICE framework boxes exemplify the positioning of certain NICE knowhows in different areas of Cyber Arena. The goal of the NICE boxes is to embody the manifestation of cybersecurity expertise across the cybersecurity ecosystem. It should be noted that the various range types exemplified in the figure can also be modeled by combining the functions differently than what is presented in the figure. The main argument is that when teaching the functionality of the cyber ecosystem, one should be able to model the ecosystem extensively. Once the ecosystem has been comprehensively modeled, the educational requirements of different knowledge areas of expertise can also be met.Once the ecosystem has been comprehensively modeled, the educational requirements of different knowledge areas of expertise can also be met.

3.1. Requirements of Comprehensive Cyber Arena

To achieve the capability for complex training environment in cyber security domain, following high-level requirements shall be fulfilled. Detailed technical requirements of specific technical implementation can be derived according to these requirements.

3.1.1. Realism. *Cyber Arena shall reflect the complexity and interdependences of real cyber domain*. Theory of authentic learning sets the central principle that the teaching environment is adapted to the environment where the learned knowhows will be practically used. One of the key challenges in cyber security education is to be able to express the difficult predictability of the causal relationships in the complex operating environment, so the Cyber Arena should be able to reflect the trainee's activities elsewhere in the ecosystem.

3.1.2. Isolated and controlled environment. *Cyber Arena shall be an isolated and controlled environment*. For allowing risk free usage of different attack vectors with real attacks and malware without jeopardising production environments, the Cyber Arena shall be isolated and centrally controlled. The national criminal laws of many countries prohibits the dissemination or processing of real malwares. Therefore, a closed environment must be in place to ensure the security and legality of training and exersices.

3.1.3. Internet simulation. *Cyber Arena shall simulate global Internet with its structures and services*. Global Internet is one of the main assets in the cyber domain. By simulating the main services and structures of the Internet, Cyber Arena has much more realism than just simulating some specific network infrastructures. Internet simulation offers the global environment for training and exercises with for example social media applications and usage of Internet based attack vectors. That Internet simulation shall also have the capability to simulate TOR network with Dark-Web capabilities. As said in [29] *"Simulation on Internet services adds the realism of scenarios being implemented by the cyber range. Modern attacks utilise global infrastructure and services considerably in order to avoid detection. Therefore, it is very important for cyber ranges nowadays to be able to simulate the Internet and its services realistically. However, in many cases, Internet services are not simulated due to the added complexity required in order to guarantee the right level of realism."*

3.1.4. User and network traffic generation. *Cyber Arena shall have the capability of network traffic simulation*. As part of the centralised control of Cyber Arena, there shall be the capability to generate network traffic from users and applications. With this capability the Cyber Arena will have ongoing network traffic as in the real networks. Simulated network traffic shall contain for example web-browsing, video

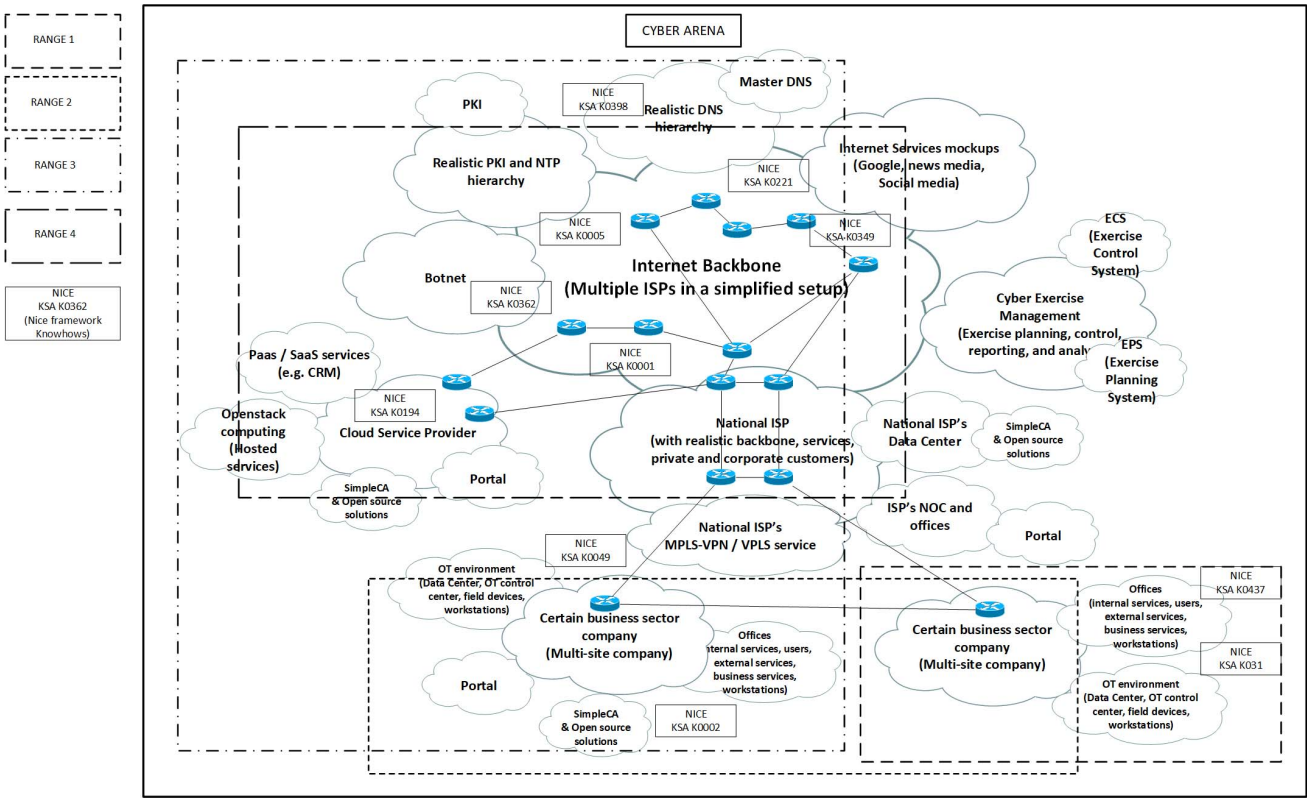

Fig. 1. Comprehensive Cyber Arena

streaming, remote-disk traffic, traffic from office software and e-mails. During the trainings and exercises that simulated network traffic allows usage of different attack vectors as in the real cyber domain, for example usage of hidden command and control channel, or some of the simulated network users can be part of distributed denial of service campaign.

3.1.5. Attack execution and simulation. *Cyber Arena shall have the capability of attack execution and simulation*. As part of the cyber security trainings and exercises it is important to execute and simulate attacks. As described earlier, an isolated environment enables the usage of real attacks and malware, in addition to real man made attacks some of those can also be simulated. Attack simulation can also be a part of the user and network traffic simulation. Cascade effects of some attacks can also be simulated without a real attack if relevant for the current education. Attacks and effects of attacks shall be planned beforehand as part of the exercise scenario (explained later).

3.1.6. Organisations' infrastructures. *Cyber Arena shall include varied organisation environments*. As in the real cyber domain, in addition to the Internet there is also an organisation environment connected to global network infrastructure. Those simulated organisation environments shall include both Information Technology (IT) and Operational Technology (OT) systems as well as interconnections of IT and OT systems and operations. In many cases it will be beneficial to execute two or more organisations in the same training or exercise in order to express interdependences between the organisations at the process and information system level . Good examples of that are an electricity company or an Internet Service Provider (ISP); if there is a cyber attack against those, it will most probably also affect the infrastructure of other organisations. The above-mentioned also illustrates real life interdependencies in organisations, networks and / or ecosystems.

3.1.7. Collaboration. *Cyber Arena shall have the capability for collaboration and co-operation with other training platforms*. According to collaborative learning theory [30], enabling collaboration between the students creates a better opportunity for learning. Students' collaboration enables collegial learning and problem solving. The cyber environment as a working context is very broad. Thus, areas of expertise are bound, which forcesbetween the organisations real-life experts into collegial problem-solving. This is why teamwork is one of the key elements of the cyber security exercise. Additionally, if there is lack of some technical capability of Cyber Arena, it can be achieved by interconnection and co-operation with other technical training platforms.

3.1.8. Planning, executing, monitoring and analysing. *Cyber Arena shall be able to provide authentic activities with*

real-life scenarios. The pedagogical goals of the exercise must be taken into account at all stages of the exercise [31]. In order to accomplish this, the Cyber Arena shall have exercise planning, execution, monitoring and analysing capabilities and tools. Via this capability the exercise and the scenarios can be planned and executed but also instructors can evaluate training audience/students' performance assessment and allow training audience/students to evaluate their performance after the exercise. This enables reflection, which is one of the key elements of learning.

4. Conclusion

In this paper the concept Cyber Arena (CA) is introduced and discussed. First, the classical cyber range concept is introduced with the examples of extremely heterogeneous definitions with the term cyber range. Because of the unexpected dependencies of the systems in the digitalised cyber domain and kinetic domain, more complex training infrastructures are required to support training, exercising and learning in complex environments. Especially when it comes to educational activities where a degree program is provided, the program should have a Cyber Arena type of facility in use. If the training and exercises are carried out in a traditional laboratory environments or in limited range environments, the core know how elements of the cyber domain cannot be realised and combined. Thus the key element of technical complexity and the interdependences between the elements will not be involved in the education program.

The pedagogical aspects are introduced for proving the need for the Cyber Arena concept and the Cyber Arena concept is introduced with its high-level requirements. As the result of the paper, it is recommended to use the term Cyber Arena when discussing state-of-the-art modern and complex cyber security exercise platforms. Term cyber range shall be used when discussing classical limited platforms.

As for future research, more specified technical requirements can be developed and state-of-the-art trainings and exercises implemented.

Acknowledgment

This research is funded by *Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)* -project of the Horizon 2020 SU-ICT-03-2018 program.

References

[1] Secretariat of the Security Committee, "Finland's Cyber security Strategy, Government Resolution 3.10.2019," Oct. 2019. [Online]. Available: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

[2] European Comission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," Feb. 2013. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

[3] P. Nevavuori and T. Kokkonen, "Requirements for training and evaluation dataset of network and host intrusion detection system," in *New Knowledge in Information Systems and Technologies*, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham: Springer International Publishing, 2019, pp. 534–546.

[4] National Institute of Standards and Technology NIST, "Cyber Ranges," https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf, Accessed: 13 January 2020.

[5] B. Ferguson, A. Tall, and D. Olsen, "National cyber range overview," in *2014 IEEE Military Communications Conference*, Oct 2014, pp. 123–128.

[6] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, and X. Cui, "A real-time correlation of host-level events in cyber range service for smart campus," *IEEE Access*, vol. 6, pp. 35 355–35 364, 2018.

[7] V. E. Urias, W. M. S. Stout, B. Van Leeuwen, and H. Lin, "Cyber range infrastructure limitations and needs of tomorrow: A position paper," in *2018 International Carnahan Conference on Security Technology (ICCST)*, Oct 2018, pp. 1–5.

[8] M. Yamin, B. Katt, and V. Gkioulos, "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture," *Computers & Security*, vol. 88, p. 101636, 10 2019.

[9] H. Winter, "System security assessment using a cyber range," in *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, Oct 2012, pp. 1–5.

[10] Y. He, L. Yan, J. Liu, D. Bai, Z. Chen, X. Yu, D. Gao, and J. Zhu, "Design of information system cyber security range test system for power industry," in *2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*, May 2019, pp. 1024–1028.

[11] Z. Chen, L. Yan, Y. He, D. Bai, X. Liu, and L. Li, "Reflections on the construction of cyber security range in power information system," in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Oct 2018, pp. 2093–2097.

[12] G. M. Deckard, "Cybertropolis: breaking the paradigm of cyber-ranges and testbeds," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, Oct 2018, pp. 1–4.

[13] M. Frank, M. Leitner, and T. Pahi, "Design considerations for cyber security testbeds: A case study on a cyber security testbed for education," in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Nov 2017, pp. 38–46.

[14] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, May 2012, pp. 256–262.

[15] S. Chapman, R. Smith, L. Maglaras, and H. Janicke, "Can a network attack be simulated in an emulated environment for network security training?" *Journal of Sensor and Actuator Networks*, vol. 6, p. 16, 08 2017.

[16] G. Subaşu, L. Roşu, and I. Bădoi, "Modeling and simulation architecture for training in cyber defence education," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, June 2017, pp. 1–4.

[17] H. Liu, W. Han, and Y. jia, "Construction of cyber range network security indication system based on deep learning," in *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, June 2019, pp. 495–502.

[18] L. Pridmore, P. Lardieri, and R. Hollister, "National cyber range (ncr) automated test tools: Implications and application to network-centric support tools," in *2010 IEEE AUTOTESTCON*, Sep. 2010, pp. 1–4.

[19] T. Debatty and W. Mees, "Building a cyber range for training cyberdefense situation awareness," in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2019, pp. 1–6.

[20] 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, May 2017, Accessed: 13 January 2020.

[21] European Defence Agency, EDA, "Cyber ranges federation project reaches new milestone," https://www.eda.europa.eu/info-hub/press-

centre/latest-news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone, Sept 2018, Accessed: 13 January 2020.

[22] European Defence Agency, EDA, "Eda cyber ranges federation project showcased at demo exercise in finland," https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland, Nov 2019, Accessed: 13 January 2020.

[23] S. Nyström, J. Dahlberg, S. Edelbring, H. Hult, and M. Dahlgren, "Debriefing practices in interprofessional simulation with students: A sociomaterial perspective," *BMC Medical Education*, vol. 16, 12 2016.

[24] S. Bariran, K. Sahari, and B. Yunus, "A novel interactive obe approach in scm pedagogy using beer game simulation theory," 04 2014.

[25] V. Emin-Martinez and M. Ney, "Supporting Teachers in the Process of Adoption of Game Based Learning Pedagogy," in *ECGBL 2013 - European Conference on Games Based Learning*, P. Escudeiro and C. V. de Carvalho, Eds. Porto, Portugal: ACPI, Oct. 2013, pp. 156–162. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00872282

[26] J. Herrington and R. Oliver, "An instructional design framework for authentic learning environments," *Educational Technology Research and Development*, vol. 48, no. 3, pp. 23–48, Sep 2000. [Online]. Available: https://doi.org/10.1007/BF02319856

[27] J. Herrington, "Authentic e-learning in higher education: Design principles for authentic learning environments and tasks," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. Association for the Advancement of Computing in Education (AACE), 2006, pp. 3164–3173.

[28] A. Collins, "Cognitive apprenticeship and instructional technology. technical report." 1988. [Online]. Available: https://files.eric.ed.gov/fulltext/ED331465.pdf

[29] European Cyber Security Organisation, ECSO, "Understanding Cyber Ranges," https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf, March 2020, Accessed: 6 April 2020.

[30] T. Panitz, "Collaborative versus cooperative learning: A comparison of the two concepts which will help us understand the underlying nature of interactive learning." 1999. [Online]. Available: https://files.eric.ed.gov/fulltext/ED448443.pdf

[31] M. Karjalainen, T. Kokkonen, and S. Puuska, "Pedagogical aspects of cyber security exercises," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 103–108.