Author(s): Karjalainen, Mika; Kokkonen, Tero; Taari, Niko

Title: Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise

Year: 2022

Version: Accepted Manuscript

Please cite the original version:

Karjalainen, M., Kokkonen, T., Taari, N. (2022). Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. Computational Methods in Applied Sciences, vol 56. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_2

Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise

Mika Karjalainen and Tero Kokkonen and Niko Taari

Abstract Cyber security exercises have experienced broad evolution in their relatively short lifetime. Cyber security exercises have been changing from individual technical skill based trainings or even competitions to the team based organisational learning experiences where different work-roles are trained and exercised during the cyber security incidents. Nowadays the modern requirements for cyber security exercises are collaboration between different training platforms and on-line remote participation of the learning audience. In the domain of cyber security, the most valuable assets are skills and know-how, so the basic ambition for conducting the cyber security exercises for individuals and for organisations is the learning. In this research, the learning experience during the state-of-the-art on-line remote cyber security exercise is studied. NIST NICE cyber security framework is used as a base for knowledge categories of used questionnaire. The results from the on-line cyber security exercise are analysed with and concluded with future research topics.

Key words: Cyber Arena, Cyber Security, Cyber Security Exercise, Learning, On-Line Training

Mika Karjalainen
Institute of Information Technology, JAMK University of Applied Sciences, Jyväskylä, Finland,
e-mail: mika.karjalainen@jamk.fi

Tero Kokkonen
Institute of Information Technology, JAMK University of Applied Sciences, Jyväskylä, Finland,
e-mail: tero.kokkonen@jamk.fi

Niko Taari
Institute of Information Technology, JAMK University of Applied Sciences, Jyväskylä, Finland,
e-mail: niko.taari@jamk.fi

1 Introduction

Modern digitalisation have brought novel threats in the cyber domain. That transformation of cyber domain has reflected to the learning requirements of the cyber security exercises. Not only technical evolution is changing the behaviour in the digital ecosystem. Current Corona-virus (Covid-19) pandemic [25] has induced transitions globally. People are working remotely on-line from their homes which brings new considerations from the viewpoint of cyber security. According to the European Union Agency for Cybersecurity (ENISA): *"The outbreak of Covid-19 has brought an immense change in the way we conduct our lives"*. ENISA have released several articles including guidance for cyber security during the pandemic.

That new norm of remote working raises major requirement for conducting the cyber security exercises: *There shall be remote on-line capability in the cyber security exercise* where learning audience shall be capable of joining exercise remotely from their homes. supposedly, that raises new technical requirements for the exercise platforms and also for the processes of controlling the exercise. Generally technical platforms for cyber security exercises are described with the term Cyber Range. However, the existing spectrum of cyber ranges is heterogeneous and that term is inconsistent. In the modern cyber security exercises the global complex cyber domain shall be simulated and such holistic platform with modern on-line capabilities shall be described with the term Cyber Arena [8].

Various teams with separate missions and functions are utilized for organising the cyber security exercises. Establishment and assignment of the team is formed according to training objectives, exercise category, personnel and other obtainable resources. Blue Team (BT) is the group of exercise learning audience that are responding to the cyber incidents and defending the valuable assets against cyber threats according to the incident response procedures of the particular organization. Traditionally, BT is modelled according to the real organisation structure and there can be one to several BTs operating in the exercise. Red Team (RT) is the threat actor of the exercise. RT is executing real (or simulated) cyber attacks and intrusions against information technology assets of the BT according to the exercise scenario and guidance of the exercise control team titled White Team (WT). WT is responsible for controlling the exercise and maintain situational awareness of the exercise by observations and collected data. WT is also assessing the learning audience of BTs. [1, 16, 21, 24, 12]

The life-cycle of cyber security exercise can be considered as a process with three phases: (i) planning, (ii) implementation/exercise execution and (iii) feedback/post exercise [24, 12]. JAMK University of Applied Sciences Institute of Information Technology have organised cyber security exercises since 2011 for the national security authorities, for the private companies of critical infrastructure and for the university students. Overall, during those years, there have been nearly 2 000 individuals as exercise target audiences. This research is conducted for the cyber security students of the bachelor's and master's programs during the academic course of cyber security exercise.

In our earlier publication [9], we studied learning outcome in the cyber security exercise by the questionnaire based on National Initiative for Cyber security Education (NICE) Cyber security Workforce Framework (NICE Framework) [19]. That study was based on on-site exercise and because of the new requirements of on-line exercise capability, the same questionnaire is utilized for the learning audience of the on-line cyber security exercise. That enables analysis for learning outcomes of the on-site exercise similarly as done earlier for the on-line exercise.

Structure of the research is as follows. In the section 2, the Learning during the cyber security exercises is discussed with the relevant theories and frameworks. After that, in the sections 3 and 4, the questionnaire based survey is presented with the analysed results. Finally, conclusions are derived with the found future research topics in the section 5.

2 Pedagogical framework for Learning in on-line Cyber Security Exercises

From the theoretical framework perspective, the cyber security exercises consist a multidimensional theory frame. It is a learning element for the adult learner, so the rationale for learning must be understood within an andragogy framework of theory [13]. According to the theory of andragogy, the adult learner is most often self-directed, and is able to apply prior knowledge in to learning new things [17]. In cyber security exercises, the learner's operating environment is a learning environment that conforms to the most authentic operating environment as possible, in which the learner monitors and acts independently, as part of a team. According to authentic learning theory [4], a sufficiently authentic learning environment stimulates learning and enables transfer of the learning to work environment. In order for the learning environment to support the competence requirements of modern digital operating domain, the learning environment should be a comprehensive Cyber Arena as described in paper of Karjalainen and Kokkonen [8], thus being able to express sufficient real-life complexity. When the learning environment is as realistic as possible, it can be stated that authentic learning environment theory also includes the thought of experiential learning theory [14], where in addition to experience, communication between the actors is needed. The importance of communication and interaction cannot be ignored, as learning through collegial reflection deepens the learning and makes it possible to bond with the existing competence. In the study [16], Maennel proposed a learning analytics reference model to be used in the life-cycle of cyber security exercise.

A key element in cyber security exercise is the learner's role as part of a team, so collaborative learning theory must also be applied as a learning theory [20]. Students act as in their given roles, as a member of an imaginary organization's IT infrastructure maintenance team. Thus, the ability of the students to work as a part of a team, and to be able to communicate their own observations and build a collective situational picture of the events in the operating environment, and this way to enable learning, is crucial [15]. The cyber security exercise as a teaching method is best suited for a learner who already has the basic cyber security skills. Based on these existing skills and knowledge's learner can construct the new lessons offered by a realistic simulation environment during the exercise. In a cyber security exercise, the student's entry level should be at the highest level of Miller's pyramid [18].

In present study, we examine learning in an on-line form of cyber security exercise. According to Kersley, on-line implementation can be as much a social event for students as on-site implementation [10]. Critical elements of an on-line exercise course implementation can be considered the planning of the course content the methods how the interaction between the participants in the course is built [23], especially when designing a cyber security exercise course where the interaction between students, lecturers and formed exercise teams is a key, to achieve the learning objectives of the course. A critical factor is the ability of the teaching staff to build the necessary interaction between the teaching environment (Cyber Arena) and the required interaction framework [11]. When building an on-line cyber security exercise, special attention must be paid to the engagement of co-operation between students within and between the teams, which is the core of the exercise and has been found to contribute to the quality of the course [2]. However, in addition to these qualitative elements, special attention must also be paid to the secured implementation of the course. When dealing with genuine cyber threat vectors during the course, special attention should be paid to the isolation of the environments and instructions for handling the data.

3 Methods and Data

In our previous research, we have studied the requirements of the cyber security learning environment from the perspective of the functional requirements of the training platform [8]. In this research, we also used the questionnaire from our previous study [9] about learning during cyber security exercises in on-site exercise by using the NIST NICE framework basic question battery [19]. The original research plan was to supplement the 2019 survey sample by collecting new set of answers and by conducting qualitative interviews to deepen the interpretation of the data. In March 2020, just when the course began, the Corona-virus pandemic forced us teaching transferring to an on-line mode. Therefore, the cyber security exercise course [7, 6] was implemented in on-line mode. The students accessed the university's Cyber Arena though VPN tunnel, and thus the entire exercise was planned and implemented in on-line mode.

According to the curriculum, students participate in the planning of the exercise event and contribute to build the IT infrastructure and its cyber security architecture to be used. In previous courses, students have been taught various cyber security controls, their construction, configuration, and management. Environmental vulnerability analysis and auditing methods are also part of the course prerequisites and has been taught to them. When students from both Bachelor and Master degree levels participate in the exercise, the roles of the participants are divided so that Masters level students have more responsibility for organizational entities, architectural level functionalities, and in the event management process for tier 2 and 3 level analysis and investigation. Correspondingly, Bachelor level students are mostly responsible for monitoring security controls, and troubleshooting in the event management process for tier 1 and possibly tier 2 level tasks.

Virtual collaboration groups and rooms were also formed for the students by using various collaboration tools, same collaboration tools were used already during the planning process of the course. The collaboration infrastructure of the on-line cyber security exercise is illustrated in Figure 1. By using the built-in training environment and collaboration tools, the training was conducted in full on-line mode in June 2020. The training was carried out using the planned scenario. The active phase of the exercise consisted of a two-day exercise. The planned original research set-up changed, but the changed research set-up allowed to study the on-line exercise arrangements, as well as the analysis of learning during the on-line exercise.

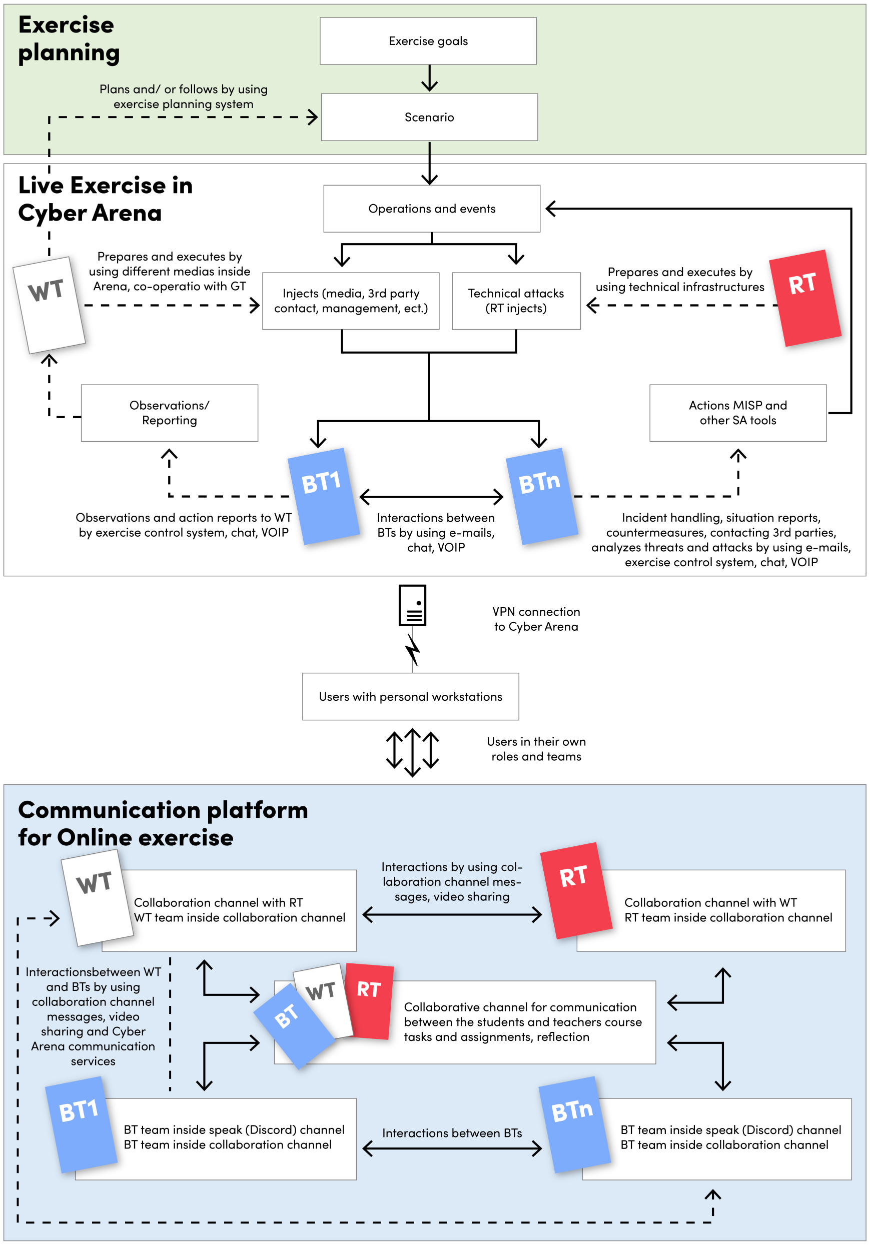
Exercise planning
Exercise goals
Plans and/ or follows by using exercise planning system
Scenario
Live Exercise in Cyber Arena
Operations and events
WT
Prepares and executes by using different medias inside Arena, co-operatio with GT
Injects (media, 3rd party contact, management, ect.)
Technical attacks (RT injects)
Prepares and executes by using technical infrastructures
RT
Observations/ Reporting
Actions MISP and other SA tools
BT1
BTn
Observations and action reports to WT by exercise control system, chat, VOIP
Interactions between BTs by using e-mails, chat, VOIP
Incident handling, situation reports, countermeasures, contacting 3rd parties, analyzes threats and attacks by using e-mails, exercise control system, chat, VOIP
VPN connection to Cyber Arena
Users with personal workstations
Users in their own roles and teams
Communication platform for Online exercise
WT
Collaboration channel with RT
WT team inside collaboration channel
Interactions by using collaboration channel messages, video sharing
RT
Collaboration channel with WT
RT team inside collaboration channel
Interactionsbetween WT and BTs by using collaboration channel messages, video sharing and Cyber Arena communication services
BT
WT
RT
Collaborative channel for communication between the students and teachers course tasks and assignments, reflection
BT1
BT team inside speak (Discord) channel
BT team inside collaboration channel
Interactions between BTs
BTn
BT team inside speak (Discord) channel
BT team inside collaboration channel

Fig. 1 Communication infrastructure of the on-line cyber security exercise

In a research sample that was conducted in 2019, answering to the questionnaire was voluntary for the students. However, we found that among the respondents the disappearance of the respondents was significant. We changed the requirements of the curriculum so that answering of the questionnaire was a mandatory for students to complete the course. Thus, the 2020 sample includes all 33 students who participated in the course.

Similarly as in our earlier study, for evaluating the learning of the topic, five questions were selected to addressing the knowledge level before and after the exercise (Table 1). Similarly, from NICE framework 44 relevant knowledge topics were chosen to the questionnaire as can see from the Table 2.

Table 1 List of questions for each topic

(Topic) was/were present in the exercise [Yes/No]
(Topic) was/were something I personally encountered during the exercise [Yes/No]
My knowledge of (topic) increased during the exercise [Yes/No]
Level of knowledge before the exercise [1–10]
Level of knowledge after the exercise [1–10]

Table 2 List of the knowledge topics covered in the questionnaire of the survey

1. Cyber threats and vulnerabilities	23. Risk management processes (e.g. methods for assessing and mitigating risk)
2. Organization’s enterprise information security and architecture	24. Cybersecurity and privacy principles
3. Resiliency and redundancy	25. Specific operational impacts of cybersecurity lapses
4. Host / network access control mechanisms	26. Authentication, authorization, and access control methods
5. Cybersecurity and privacy principles	27. Application vulnerabilities
6. Vulnerability information dissemination sources	28. Communication methods, principles, and concepts that support the network infrastucture
7. Incident categories, incident responses, and timelines for responses	29. Business continuity and disaster recovery continuity
8. Incident response and handling methodologies	30. Local and Wide Area Network connections
9. Insider Threat investigations, reporting, investigative tools and laws/regulations	31. Intrusion detection methodologies and techniques for detecting host or network -based intrusions
10. Hacking methodologies	32. Information technology security principles and methods (e.g. firewalls, demilitarized zones, encryption)
11. Common attack vectors on the network layer	33. Knowledge of system and application security threats and vulnerabilities
12. Different classes of attacks	34. Network traffic analysis methods
13. Cyber attackers	35. Server and client operating systems
14. Confidentiality, integrity, and availability requirements and principles	36. Enterprise information technology architecture
15. Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications	37. Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)
16. Network traffic analysis (tools, methodologies, processes)	38. System administration, network, and operating system hardening techniques
17. Attack methods and techniques (DDoS, brute force, spoofing, etc.)	39. Risk/threat assesment
18. Common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.)	40. Knowledge of countermeasures for identified security risks. Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
19. Malware	41. Packet-level analysis using appropriate tools (e.g. Wireshark, tcpdump)
20. Security implications of software configurations	42. Hacking methodologies
21. Computer networking concepts and protocols, and network security methodologies	43. Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
22. Laws, regulations, policies and ethics as they relate to cybersecurity and privacy	44. Methods and techniques used to detect various exploitation activities

In addition to the learning survey presented above, we conducted an interview to the course lecturers to find out about the key elements of planning and construction of the on-line exercise environments, as well as possible suggestions for improvement that would have arisen from the lecturers. We also wanted to ask for the lecturers experiences and views in relation to the learning outcomes measured from students during the on-line exercise. The interviews were conducted in the fall of 2020 as face-to-face on-line interviews by video conference system due to Covid-19 situation. The data consists of three semi-structured interviews. The third author of this paper, a member of the course teaching staff, was excluded from the interviews in order to be able to rule out his preconceived notions about the material. The interviews were started with background questions about the role and tasks of the lecturer during the course. Lecturers were then asked to describe the communication environment built for the on-line exercise, what learning environments were used in the course, and how they were used. Informants were also asked to describe in particular how and on what platforms the students and lecturers communicated and what kind of visibility the teaching staff had to the mentioned forums. Lecturers were also asked to qualitatively evaluate how successful the exercise arrangements were in terms of the technical arrangements of the learning environment, and the success of the students' learning. The duration of the interviews ranged from 22 minutes to 42 minutes. The interviews were recorded and transcribed. The interviews were conducted by the first author.

The data analysis started by differentiating from the data the sections for descriptions of the training arrangements as well as the sections dealing with the students' learning and suggestions for improvement of on-line arrangements. In the analysis, we used conventional method of qualitative analysis, where data is structured, categorized, and merged in higher-level themes [5]. In the analysis, we combined the approach of inductive and abductive analysis [3] in an effort to understand the specific requirements of cyber security exercise in relation to the more general theories of on-line pedagogy presented above.

4 Results

The survey data was comprehensively examined. The calculations of average, median and standard deviation was analysed for each knowledge before and after the on-line exercise. In addition to analysing the statistical significance, p-values for each knowledge were calculated and analysed with the null hypothesis of *"no learning during cyber security exercises"*. Calculated p-values for individual knowledges can be found from Table 3. Commonly referred p-values are $p < 0,05$ as statistically significant and $p < 0,001$ as statistically highly significant [22]. If we use those commonly used p-values as the basis of the analysis, we can see that the learning in almost all of the knowledge areas was statistically highly significant and in all except one knowledge it was statistically significant. That specific knowledge where the learning was not statistically significant is the *"Packet-level analysis using ap-*

propriate tools", which can be explained that only limited amount of students (one blue team) used packet-level capture and analysis software tools. For the rest of the students there were no appropriate deep packet-level analysis executed during the hectic exercise event.

Table 3 P-values calculated for each knowledge of the survey.

$knowledge$	$p-value$	$knowledge$	$p-value$
1	0,000000015	23	0,001277018
2	0,000079831	24	0,001534458
3	0,001048385	25	0,000421841
4	0,001472250	26	0,002135130
5	0,001254890	27	0,000067056
6	0,000016276	28	0,001534458
7	0,000008653	29	0,011447886
8	0,000176480	30	0,006124649
9	0,000803151	31	0,008672679
10	0,000377142	32	0,000107062
11	0,000004378	33	0,000435434
12	0,000003624	34	0,000501850
13	0,002590328	35	0,000226935
14	0,036821182	36	0,006124649
15	0,004182652	37	0,001762796
16	0,000057269	38	0,004789459
17	0,000012334	39	0,000939544
18	0,000028078	40	0,001534458
19	0,005926692	41	0,152397681
20	0,000698501	42	0,000004218
21	0,001230732	43	0,000008632
22	0,031610717	44	0,001393172

For visualising the trends of learning during the on-line and on-site exercises, the box plot figures were produced. Figure 2 illustrates the box plot statistics containing the interquartile ranges (IQR) of answers in different years. The red (left) box plot shows the level of the knowledge before the exercise while the blue (right) box plot shows level of the knowledge after the exercise. The median line of the answers is drawn inside of the box plot. Outlier answers are presented as bullets outside of the box plots.

It can be easily seen from the numerical data that there is increasing of the knowledge during the exercise covering all the selected knowledge areas. In advance, there was significant amount of learning during the on-line exercise even if on-line exercise is more complex for the learning audience and it suffers lack of face-to-face communication. That is the most prominent observation based on the numerical estimations.

Because number of samples was limited (number of students participating the course), there was also qualitative analysis done. As qualitative analysis, the lecturers of the course were interviewed. The aim of the interview was to map the essential

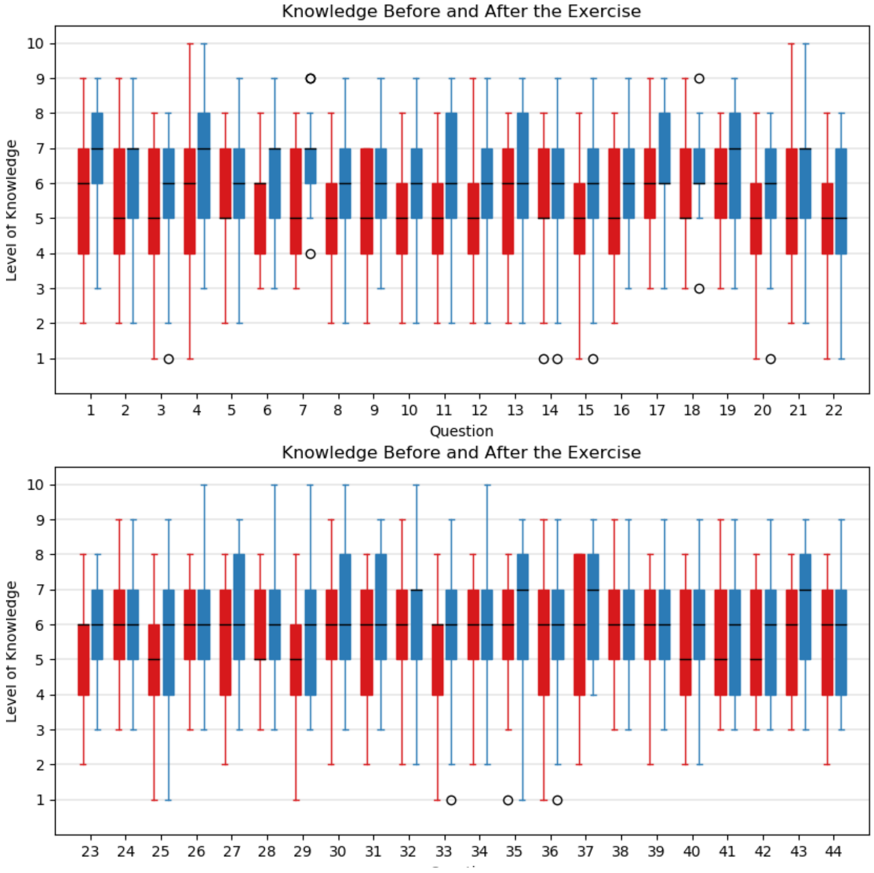

Fig. 2 Level of knowledge before and after the 2020 on-line exercise

structures and functionalities of the on-line exercise. The interview also sought to find out the lecturers views and experiences of students learning during the on-line exercise. All of the lecturers have several years of experience from this particular exercise course. The informants saw their own role more as an adviser role who ensures that the set learning goals will be achieved and supports the students by answering the questions from them. Lecturers had no previous experience of cyber security exercises as an on-line exercise, so the implementation design was experimental in nature and the introduction of best practices arising from other on-line activities.

> *” The role is to guide, how such an exercise is built from the BT / WT / RT team perspectives. That is, what needs to be considered, how threat activity should be built so that other participants can learn. Role is more of a mentor role, less of a lecturer, for the student there is a big need for self-study and we support the issues that arise for students.”*

The first contact of the course had been implemented by using traditional classroom teaching, after that first contact lessons the situation quickly changed, so the lecturers need to start planning the on-line execution of the course. Due to the urgency of the schedule, the decision was made to implement the necessary communication platforms and channels by using a communication system familiar to students and lecturers. So they made a decision to use the Microsoft Teams [1] collaboration platform, as the schedule did not allow the construction of a custom made platform inside the Cyber Arena. The GitLab [2] environment was used as the platform for the distribution and saving of the general material of the course. Students logged in to the Cyber Arena from their own workstations using the VPN tunnel to the VMware Cloud Director [3]. An additional chat service was built inside the Cyber Arena, which thus also made it possible to communicate also within the training environment. In addition to this, BT used the Discord [4] system for intra-team communication, which was mainly used as a voice channel. WT / RT used the Rocket.Chat [5] service for their own mutual and internal communication. The implemented platform for communication and information sharing is shown in Figure 1.

> *" A significant issue was to make the decisions on which (communication) system to install all the information and whether to build systems related to, for example, study or exercise guidance within the Cyber Arena environment, or whether to use out of the Cyber Arena systems / communication channels, such as Teams. At this point, students and lecturers came to the conclusion that Microsoft Teams would be strongly used for its various channels and screen-sharing technology for communicating and sharing information. Students' internal meetings and information sharing was held at Teams and a lot of documentation was shared also at Teams. In the Cyber Arena environment, the actual technical systems, defended targets and attack computers were then used. The planning and conducting of the exercise was carried out with such out-of-game solutions, another option would have been to build everything inside the training system. Here, the students felt that this was (using Teams) a more natural way for them, to use a tool that they also normally use in other studies and communication in everyday life."*

Lecturers had access to all communication channels created and they were able to monitor events and discussions in existing forums without interfering with the content of the discussions. There was also a mode of operation how students or the team were able to invite the lecturer to the channel when they experienced problems or ambiguities during the exercise. Lecturers found the procedure even more effective than in a traditional on-site exercise where they visit classrooms used by students. The transition between the facilities was quick and when problems arose, it was easy for the lecturer to join the conversation when the students invited them to the channel. All lecturers stated that the technical arrangements for the on-line exercise went smoothly. The implemented environment was able to be seamlessly integrated into the exercise, even though it was differentiated from the Cyber Arena. Lecturers

[1] https://www.microsoft.com/teams/

[2] https://about.gitlab.com/

[3] https://www.vmware.com/products/cloud-director.html

[4] https://discord.com/

[5] https://rocket.chat/

felt that the on-line exercise was an encouraging, good experience and gave insight and reassurance that the on-line cyber security exercise also enabled students to learn.

> *"This was an interesting experience and it is especially interesting to see that students learned so well in this on-line exercise. It shows that, at least for myself, I had doubts about how well an individual is able to learn when there are no elements of live / on-site exercise around them. At least this survey shows that learning during an exercise has been even better than an on-site exercise, whether it's because of a lower starting level or a careful assessment of one's own skills and then it feels like this went well, so I can't explain that. This was an encouraging, good experience and gave me the reassurance that this exercise should continue to be facilitated in this way. Through further development, this will certainly be a good way to organize an on-line exercise."*

As further development needs, the lecturers identified the need to build the entire communication platform inside the Cyber Arena. This was pointed because there is a risk that the training content becoming entangled with other content in the Teams platform. When the Teams platform is also used for other study or work, other possible communication on the Teams platform interferes with the focus on the exercise. Lecturers also found it difficult to monitor an individual student's performance during the exercise. As a result, the evaluation of the exercise was simplified and the numerical evaluation was abandoned. The development of evaluation and the analysis tool used for it, was also seen as a future development task. The situation awareness of students activities during the exercise should also be improved by bringing new situational awareness tools to the exercise. In the future, the communication channels used by the students will also be defined more precisely by the lecturers. Some lecturers also expressed the need to simplify the cyber environment modelled in the Cyber Arena, as in on-line mode students are more passive to ask and thus some threat activities may be left without any actions.

As an overall result, combined from quantitative and qualitative result, it can be said that significant learning takes place during the on-line cyber security exercise. Cyber security exercises are extremely effective for gaining the understanding of the complex cyber incidents and the unexpected behaviour and dependences of the cyber incidents. Infirmity of the on-line exercise versus on-site exercise is the lack of face-to-face communication which reduces analysis of scenarios. However it can be solved with the accomplished technical implementation of the communication infrastructure supporting the requirements of the on-line exercise event.

5 Conclusion

The present study examined learning in on-line exercise with a questionnaire built from the NIST NICE framework. The result of the study confirms the analysis of the data collected in the previous study [9], whereby the cyber security exercise serves as an excellent teaching platform and as an tool for teaching cyber security contents with a versatile focus. The on-line exercise also showed that the on-line exercise achieves the set learning objectives well. The self-assessment carried out by the students, where they assess their own level of competence before and after the cyber security exercise, shows statistically significant learning in 43 from 44 content areas of the questionnaire. The result also correlates well with the previous sample, which helps to eliminate the result uncertainties raised by the loss of the respondents in the previous sample.

The qualitative part of the study retrieved information on the aspects of organizing an on-line cyber security exercise, which allows the exercise to be organized in such a way that the exercise can reflect the needed collaborative learning elements, between the individuals and the teams co-operations, problem solving and learning. As a core result, the requirement to build an adequate collaboration platform was emerged. In the exercise under review, the collaboration platform was built on a so-called out of the game style, i.e. outside the actual Cyber Arena. The arrangement was successful in a technical sense, but the lecturers of the course also highlighted areas for development. As things to be developed, the lecturers saw the construction of an collaboration platform inside the Cyber Arena. This avoids security risks and reduces the disadvantages of concentration that may arise from a more general collaboration forum in relation to other activities. Lecturers were positively surprised by the measured learning outcomes, which contributed to strengthening their perception of the future transition of the course to a permanent on-line format. The lecturers found the individual assessment of students difficult, as the rapidly constructed collaboration platform did not allow for sufficiently detailed monitoring of the actions taken by the individual student. For the assessment of the individual, it was felt that better visibility into the student's performance was needed.

The results indicates the difference between students level of knowledge between those who have been in on-line course and those who have been in on-site course. However, the data collected do not provide enough information to analyse the reasons for the difference between the levels of learning outcomes. Future research should seek to analyse the reasons that explain the differences in levels of knowledge between on-line and on-site teaching methods.

Acknowledgements

- This research is funded by the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund as part of the Health Care Cyber Range (HCCR) project of JAMK University of Applied Sciences Institute of Information Technology.
- The authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript.
- The authors would like to thank Ms. Heli Sutinen for finalizing the Figure 1.

References

[1] Almroth J, Gustafsson T (2020) Crate exercise control – a cyber defense exercise management and support tool. In: 2020 IEEE European Sympo-

sium on Security and Privacy Workshops (EuroS PW), pp 37–45, DOI 10.1109/EuroSPW51379.2020.00014

[2] Chen PSD, Gonyea R, Kuh G (2008) Learning at a distance: Engaged or not? Innovate: Journal of Online Education 4(3)

[3] Graneheim UH, Lindgren BM, Lundman B (2017) Methodological challenges in qualitative content analysis: A discussion paper. Nurse education today 56:29–34

[4] Herrington J, Oliver R (2000) An instructional design framework for authentic learning environments. Educational Technology Research and Development 48(3):23–48, DOI 10.1007/BF02319856, URL https://doi.org/10.1007/BF02319856

[5] Hsieh HF, Shannon SE (2005) Three approaches to qualitative content analysis. Qualitative health research 15(9):1277–1288

[6] JAMK University of Applied Sciences (2020) Cyber Security Exercise, 5 cr - YTCP0400. https://opetussuunnitelmat.peppi.jamk.fi/fi/YTC2020SS/course_unit/YTCP0400, accessed: November 30 2020

[7] JAMK University of Applied Sciences (2020) Kyberturvallisuusharjoitus, 5 op - TTC7530. https://opetussuunnitelmat.peppi.jamk.fi/fi/TTV2020SS/course_unit/TTC7530, accessed: November 30 2020

[8] Karjalainen M, Kokkonen T (2020) Comprehensive Cyber Arena; The Next Generation Cyber Range. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, pp 11–16

[9] Karjalainen M, Samir P, Kokkonen T (2020) Measuring Learning in a Cyber Security Exercise. In: Accepted for 12th International Conference on Education Technology and Computers, ICTC 2020 and will be published in the conference proceedings

[10] Kearsley G (2000) Online education: Learning and teaching in cyberspace. Wadsworth Publishing Company

[11] Kearsley G (2008) Tips for training online instructors. Unpublished article

[12] Kick J (2014) Cyber exercise playbook. The MITRE Corporation https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf, accessed: 2 December 2020

[13] Knowles MS (1995) Designs for adult learning: Practical resources, exercises, and course outlines from the father of adult learning. Amer Society for Training &

[14] Kolb DA, Boyatzis RE, Mainemelis C, et al (2001) Experiential learning theory: Previous research and new directions. Perspectives on thinking, learning, and cognitive styles 1(8):227–247

[15] Laal M (2013) Collaborative learning; elements. Procedia-Social and Behavioral Sciences 83:814–818

[16] Maennel K (2020) Learning analytics perspective: Evidencing learning from digital datasets in cybersecurity exercises. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp 27–36, DOI 10.1109/EuroSPW51379.2020.00013

[17] Merriam SB, Bierema LL (2013) Adult learning: Linking theory and practice. John Wiley & Sons

[18] Miller GE (1990) The assessment of clinical skills/competence/performance. Academic medicine 65(9):S63–7

[19] Newhouse W, Keith S, Scribner B, Witte G (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. DOI 10.6028/nist.sp.800-181, URL http://dx.doi.org/10.6028/NIST.SP.800-181

[20] Panitz T (1999) Collaborative versus Cooperative Learning: A Comparison of the Two Concepts Which Will Help Us Understand the Underlying Nature of Interactive Learning. https://files.eric.ed.gov/fulltext/ED448443.pdf

[21] Seker E, Ozbenli HH (2018) The concept of cyber defence exercises (cdx): Planning, execution, evaluation. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp 1–9, DOI 10.1109/CyberSecPODS.2018.8560673

[22] StatsDirect Ltd (2020) P values. https://www.statsdirect.com/help/basics/p_values.htm, accessed: November 30 2020

[23] Swan K (2001) Virtual interaction: Design factors affecting student satisfaction and perceived learning in asynchronous online courses. Distance education 22(2):306–331

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

[25] World Healt Organization (WHO) (2020) Coronavirus disease (covid-19) pandemic. https://www.who.int/emergencies/diseases/novel-coronavirus-2019, accessed: November 5 2020