Measuring Learning in a Cyber Security Exercise

Mika Karjalainen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 40 574 8012
mika.karjalainen@jamk.fi

Samir Puuska
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 40 652 6767
samir.puuska@jamk.fi

Tero Kokkonen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 438 5317
tero.kokkonen@jamk.fi

ABSTRACT
In recent years, cyber security exercises have established themselves as an integral part of cyber security education. Cyber security professionals usually work as a part of a team that monitors and responds to incidents in the environment. A sufficiently realistic complex learning environment is necessary for collaborative learning at the expert level. Evaluating the learning outcomes of complex exercises is an important task for both assessing how individuals met the learning objectives, and how to improve the exercise to better serve those goals. This requires the assessment of multiple skill and knowledge categories independently. We leveraged the NIST NICE Cybersecurity Workforce Framework as a base for building knowledge categories for questionnaire use. However, the NICE framework is comprehensive and detailed requiring that the areas of competence assessment needed to be simplified for questionnaire use. We summarized the NICE framework into 44 questions addressed to the individuals who participated in the exercise. A web-based questionnaire was used to query 21 participants' skill level before and after the exercise, as well as their familiarity and experience with the topic before and during the exercise. The results indicate that cyber security exercises will increase the knowledge of the participant in the knowledge areas that were present in the exercise. This increase was more prominent in cases where the participant was more likely to recognize, and experience events related to that category during the exercise. Furthermore, we concluded that the NICE framework can be used to assess individual know-how and as a basis for knowledge-related questionnaires.

CCS Concepts
• **Social and professional topics → Professional topics → Computing education →Adult education**

Keywords
Cyber security; Education; Competence; Skill; Knowledge; Cyber Arena

1. INTRODUCTION
Cyber security exercises (CSE) are an efficient resource for personnel training. There is a long tradition of using laboratory environments in engineering education. Typically, the laboratory environment has been constructed to reflect the phenomenon or operating environment of the subject being taught. Previously the laboratory environment often expressed spotted targets from the bigger entirety. Traditional ICT environments have been used in ICT teaching, for example data network laboratories to teach routing and network protocol design. In pedagogical thinking, the above-mentioned teaching method fits into self-regulated learning (SRL) or self-directed learning (SDL) as well as under the experimental learning theories (ELT) [1]. Over the past decade, cyber security has become one of the key topics in the ICT industry. Programs in graduate education are slow to respond to the changes in the surrounding society, so there has been a delay in responding to the pedagogical demands of cyber security. When considering the phenomenon of cyber security, the multidimensionality of the phenomena must be taken into consideration. A cyber security professional should be able to master the in-depth details; however, at the same time, professionals should have an understanding of the impact of details on other technologies, processes or functionalities.

This sets specific requirements for the laboratory environment where cyber security education and training will take place. On one hand, it can be said that traditional laboratory environments still have value when teaching the basics or the spotted details of larger environment. On the other hand, a full-scale simulation environment is required, thus in the domain of cyber security cyber ranges have been built to execute cyber security exercises (CSE).

2. BACKGROUND AND RATIONALE

2.1 Andragogy
The theory of andragogy makes a difference in the learning between adults and children [2]. For adult learners, the learning process is described as a self-directed learning process. An adult learner is perceived to be self-directed, able to apply what one has learned in the past and to apply what one has learned to practice [3]. For adult learners, education should induce a distorted cognitive dissonance that breaks the habit of old thinking and generates the desired critical-analytical stage of engaging the learner with new knowledge, opinion or action. Cognitive dissonance theory (CDT) suggests that when learners have two or more cognitions that are conflicting, they will feel a displeasing state – dissonance – until they are able to resolve this state by modifying their cognitions [4]. It can be said that in andragogy theory learning is focused on a hands-on perspective implemented in the context of real-life simulation environment [5].

2.2 Experiential Learning
The theory of experiential learning cogitates that the experiencing alone does not guarantee good learning outcomes; it also requires thinking and conceptualization, such as speech and reflection [6]. Through conceptualization an individual can transform unimaginative and unconscious information into conceptualized and conscious information building. This means that by contemplating an action verbally, the vague blur of experience and emotion becomes a word-made activity that can be understood and transformed to new knowledge. Thus, there must be a lot of reciprocity and discussion between the teacher and the student. A student reveals what he or she is trying to learn by deeds and words, and the teacher responds with a variety of feedback methods, such as advice, criticism, explanation or examples [6], [7], [8], [9]. In his theory of deliberate

practice (DP), Ericsson argued that a specialized form of practice is a necessary component if the aim is to increase the expert performance is desired [10]. Accordingly, Ericsson´s DP model experts need well-defined learning objectives to develop a specific area of their expertise. Thus, experts should attain the highest level on Miller´s pyramid [11] to fully benefit from CSE as a learning method.

2.3 Collaborative Learning

Collaborative learning (CL) is a pedagogical theory where collaboration and built consensus between the student group members generates learning [12]. Group members take responsibility for their own learning, share their insights and work towards a common goal by solving problems, completing tasks, and thus learning [13]. In order to execute successful group work towards the CL five basic elements should be fulfilled: (i) clearly perceived positive interdependence, (ii) considerable interaction, (iii) individual accountability and personal responsibility, (iv) social skills, and (v) group self-evaluation [14], [15]. CSE can be seen as an application of collaborative learning methodology. The above elements are realized at different stages of the CSE life cycle [16].

2.4 Complex Environments

In the real cyber domain, the interdependencies between different systems, network and data form an extremely complex totality. Cyber incident as one component of that complex domain may affect erratic consequences on other systems or even in a physical domain. When discussing learning environments in cyber security, it must be realized that the realistic training environments shall be complex enough for in order to reflect the sophisticated interdependent relationship of networks, systems and data of the real world. Traditionally, these training environments are called as *"Cyber Range"*. The problem with that familiar term is that the spectrum of cyber ranges is extremely heterogenous varying from simple laboratory-based test beds to complex mimics global Internet. Paper [17] introduces the concept of cyber arena; the next generation cyber range, with its pedagogical viewpoints and technical requirements. As stated in [17], "*it is recommended to use the term Cyber Arena when discussing state-of-the-art modern and complex cyber security exercise platform*".

2.5 NICE Framework

To manage know how in the domain of cyber security, National Institute of Standards and Technology (NIST) has created National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [18]. This NICE framework can be used to describe the competencies required for various cyber security jobs [19]. Its purpose is to unify the concepts and taxonomies of business, industry and education providers for the cyber content-specific needs in different areas of expertise. The framework can also be applied to define the necessary contents of the core competency of cyber skills and thereby to develop curricula and course content [20].

3. RESEARCH METHOD

The research was carried out in JAMK University of Applied Sciences master's degree program in cyber security [21]. The course uses the comprehensive cyber arena as a training platform that is able to embody key Internet functionalities, as well as the modeled companies' ICT infrastructure and the interdependence between them [17]. The training platform also enables the modeling of the needed complexity, which is a key phenomenon in cyber security education. In the degree program one element of the course is a cyber exercise which is carried out so that students participate in the planning and implementation of the exercise. At the beginning of the course, there is a planning phase where students plan the information security controls of the fictional company's ICT environment.

The basics and practices of security control design have been taught and practiced in the previous courses of the degree program. The course proceeds to the active phase of the exercise, which is implemented as so-called blue team cyber security exercise method, where students act as an ICT team of the company´s infrastructure they have built in the design phase. The exercise proceeds according to the planned scenario and lasts approximately two working days. After the active phase of the exercise, the events of the exercise are reviewed, and students write an after-action report of the exercise where they reflect the learning they have reached during the course. We sent the questionnaire via e-mail to 86 persons that participated in the cyber exercise as blue team members. The questionnaire was sent to the students after they had completed the after-action report.

We used the NIST NICE framework as a starting point for creating a questionnaire that captured the key learning elements of a cyber security exercise. In order to leverage the NICE framework, the authors and two other cyber security experts familiar with CSEs ranked the frameworks 630 "Knowledge" related areas of expertise. The ones marked by every author were included as basis for further refinement. They were further distilled by combining overlapping areas into broader categories, resulting in 44 topics overall (Table 2). For assessing knowledge increase we selected a total of five questions addressing the knowledge level before and after the exercise, a question regarding subjective feeling of increased knowledge, and two questions about the topic if it was seen as present and personally encountered during the exercise. The exact questions are listed in Table 1.

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 topics covered in questionnaire.

1. Cyber threats and vulnerabilities	25. Specific operational impacts of cybersecurity lapses
2. Organization's enterprise information security and architecture	26. Authentication, authorization, and access control methods
3. Resiliency and redundancy	27. Application vulnerabilities
4. Host / network access control mechanisms	28. Communication methods, principles, and concepts that support the network infrastructure
5. Cybersecurity and privacy principles	
6. Vulnerability information dissemination sources	29. Business continuity and disaster recovery continuity
7. Incident categories, incident responses, and timelines for responses	30. Local and Wide Area Network connections
8. Incident response and handling methodologies	31. Intrusion detection methodologies and techniques for detecting host or network -based intrusions
9. Insider Threat investigations, reporting, investigative tools and laws/regulations	32. Information technology security principles and methods (e.g. firewalls, demilitarized zones, encryption)
10. Hacking methodologies	
11. Common attack vectors on the network layer	33. Knowledge of system and application security threats and vulnerabilities
12. Different classes of attacks	
13. Cyber attackers	34. Network traffic analysis methods
14. Confidentiality, integrity, and availability requirements and principles	35. Server and client operating systems
	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.)	
18. Common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.)	39. Risk/threat assessment
	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	
20. Security implications of software configurations	
21. Computer networking concepts and protocols, and network security methodologies	41. Packet-level analysis using appropriate tools (e.g. Wireshark, tcpdump)
22. Laws, regulations, policies and ethics as they relate to cybersecurity and privacy	
	42. Hacking methodologies
23. Risk management processes (e.g. methods for assessing and mitigating risk)	43. Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
24. Cybersecurity and privacy principles	44. Methods and techniques used to detect various exploitation activities

4. RESULTS

Overall, 21 people submitted answers to all questions. Improvements were seen in almost each category. Figure 1 presents the box plot statistics containing the interquartile ranges (IQR) of answers. The left box plot (red) describes the knowledge before the exercise and the right box plot (blue) the knowledge after the exercise. Inside of the box plot, the median line of the answers can be seen. Small balls or stars outside of the box plots are outlier answers which were out of the corresponding IQR's whisker's max/min 1.5 times IQR. Based on the answers from the questionnaire, it can be stated that the competence level of the respondents generally increased. Notably, the exceptions in the questions where knowhow of the respondents did not increase significantly (questions 21, 25, 26, 28, 29, 30, 36, 41) were likely due to the fact that the areas of those questions were not prominently present in the exercise where this data was collected. The above observation supports the correlation of responses with the type of exercise that was executed. In overall 36 questions the responses indicated that they had experienced significant learning. The top five areas (questions 1, 2, 7, 8, 33) where according to the questionnaire answers the learning took place the most are the general principles of cyber security, the threats and vulnerabilities on a large scale, and the areas dealing with the security architecture of the organization.

The result shows that cyber security training implemented in a comprehensive cyber range is an excellent teaching method and platform. The exercise can summarize the previous course sections and bring students an understanding of the large complex operating environment which is needed knowledge for cyber security professionals in cyber security domain. The data of the answers shows that participants with a lower level of knowledge achieved greater competence growth. However, the respondents' knowledge level was on average 6-7, which means that the respondents were not beginners for their level of knowhow. It should be noted that the assessment of the person's own knowledge before and after the exercise is a subjective assessment of the person for question; the respondents were not given any baseline test to identify any difference between their own rating and the level of proficiency found in the questionnaire.

Building an objective metric to assess a person's competence remains elusive. This is because the exercise is a very complex environment, where it is challenging to evaluate people who have e.g. different roles. It is also difficult to predict what kind of tasks and difficulty level of the tasks each participant will encounter during the exercise. In this exercise the participant's performance was not scored. This is because we believe that by scoring a participant's activity will begin to guide the participant's activities towards activities that he or she finds to receive more points. The focus of the exercise has been on the development of the

individual's skills and knowledge, through when it is possible, to develop also the competence of the organization participating in the exercise.

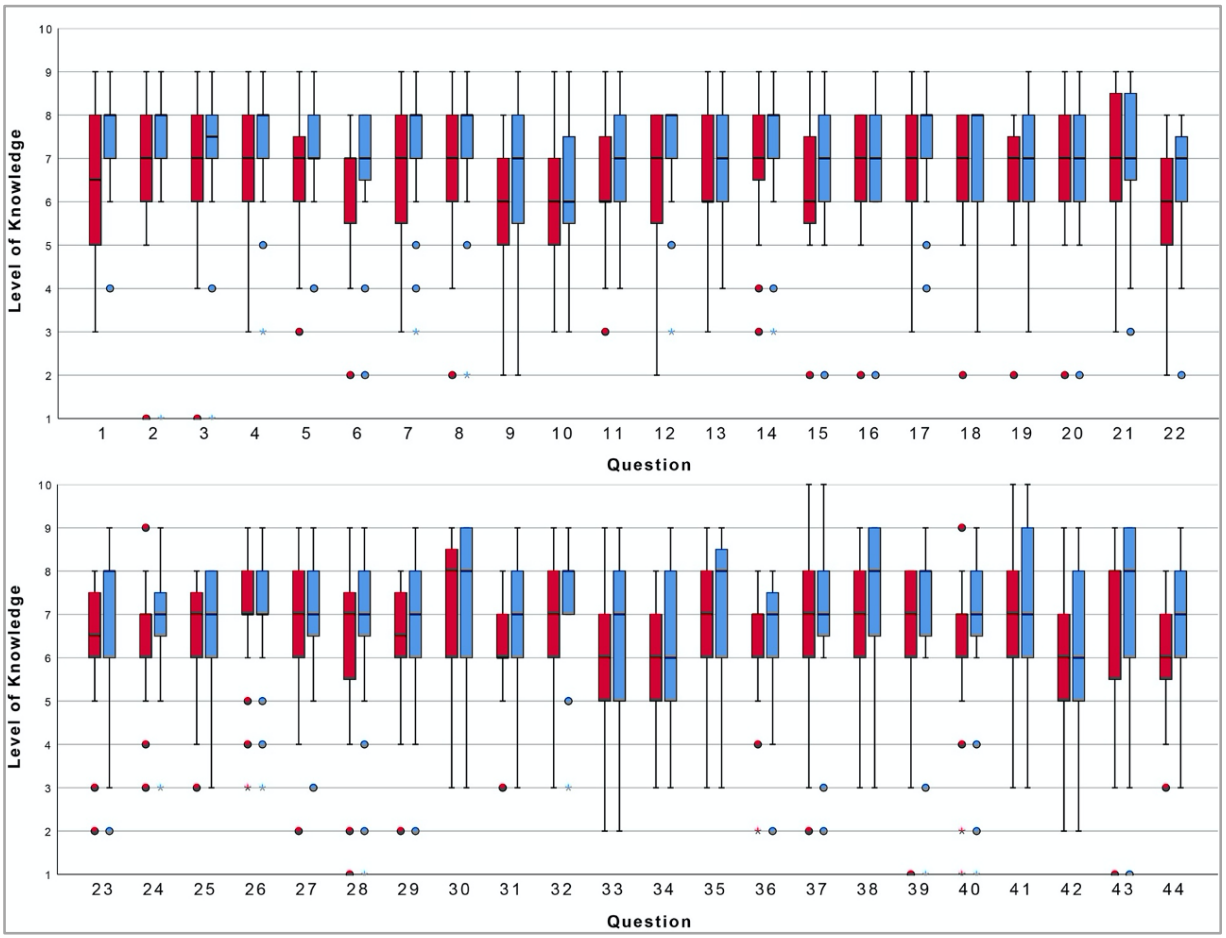

Figure 1. Level of knowledge before and after the exercise.

5. CONCLUSIONS

Based on the conducted research, it can be said that the NICE framework can be used as a baseline for creating questionnaires that measure levels of knowledge improvement. The NICE framework can also be used in a targeted way to measure the competence in a certain substance area. In this paper, a common set of indicators on various aspects of cybersecurity was desired. The used pedagogical theory is not complete. The cyber security exercise is a large pedagogical learning event where various elements are manifested. Some pedagogical phenomena's do not always materialize in practice, so it is almost impossible to build a comprehensive theoretical framework for exercise. However, key theories of experiential learning combined with collaborative learning provide a sufficient basis for the theory. There are also recognizable elements of problem-based learning and exploratory learning frameworks in the exercise, as during the exercise the student acts as a researcher observing the environment and reacting to the findings of the operating environment.

The qualifying was done by a mapping list of questions by experienced teachers and experts, so that only the most relevant questions remained in the final questionnaire. The difficulty with the NICE framework is the level of details in the framework. With a total of 630 knowledge areas alone, the resulting questionnaire would be prohibitively long if they all were included. However, it should also be noted that the framework's knowhow descriptions are at very different levels of details. Some of the knowhow descriptions are very general and some very detailed. This should be taken into account when constructing the questionnaire.

A development proposal for future work would also be the categorization of a list of questions, which would provide a much-needed summary through possible overlaps between different issues. Answering the questionnaire was scheduled at the end of the course so that all the elements influencing learning would been reviewed before answering. Especially the hot wash up event after the exercise is an essential opportunity to review the implemented scenarios and technical elements in different cyber events and / or threat campaigns that have been executed during the exercise. From the learning perspective, the hot wash up event is an important part of the course. It seems that at this stage the students were no longer motivated to answer the question set, which was quite time consuming.

The observation is also corroborated by the phenomenon observed from the data, which addressed that 53 respondents started answering the question set; however, only 21 answered it fully.

This indicates that answering the 44 detailed questions is challenging for the respondents. In the future research, we will place answering the question set as part of the course performance, which will hopefully result in a significantly better sampling. Although the number of respondents to the questionnaire set remained relatively low, it can be said that the cybersecurity exercise serves as an excellent wide-ranging learning environment. The learning outcomes were significant in the area of 36 questions from 44. It also seems that possible differences in students' entry levels knowledge do not interfere the learning during the exercise and students will be able to adapt their actions according to their own level of knowledge to perform tasks that enable contributing to the team and thus, they will be able to learn at their own level.

Other studies measuring the development of the knowledge of the students who participated in the cybersecurity exercise have not been conducted with this method.

As future research, we will collect a larger sample, so the sample will be more representative. We will also continue to analyze qualitative interview data that was collected as part of the research. This allows for a more detailed analysis of the phenomena that have now emerged but which cannot be explained by the quantitative data. Such an observation was, for example, that few of the respondents estimate that their knowhow level would have increased; however, the numerical estimate shows that the respondent had maintained the same knowhow level. In the future, research will be extended to the area of organizational learning. This will be possible utilizing exercises for commercial operators where organizations train their staff on an annual basis.

6. ACKNOWLEDGEMENT

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

7. REFERENCES

[1] Gemmell, R. M., Boland, R. J., and Kolb, D.A. 2012. The Socio-Cognitive Dynamics of Entrepreneurial Ideation. *Entrepreneurship Theory and Practice* 36, 5 (2012), 1053–1073.

[2] Knowles, M. S. 1995. *Designs for adult learning: Practical resources, exercises and course outlines from the father of adult learning.* Alexandria, Va: American Society for Training & Development.

[3] Merriam, S. B. and Bierema L. L. 2013. *Adult learning: Linking theory and practice*. John Wiley & Sons.

[4] Festinger, L. 1962. *A theory of cognitive dissonance*. Vol. 2. Stanford university press.

[5] Knowles, M. S. et al. 1984. *Andragogy in action.* Jossey-Bass San Francisco.

[6] Kolb, D. A., Boyatzis, R. E., Mainemelis, C., et al. 2001. Experiential learning theory: Previous research and new directions. *Perspectives on thinking, learning, and cognitive styles* 1, 8 (2001), 227–247.

[7] Engeström, Y. 2001. Expansive learning at work: Toward an activity theoretical reconceptualization. *Journal of education and work* 14, 1 (2001), 133–156.

[8] Schön, D.A. 1987. *Educating the reflective practitioner.* Jossey-Bass San Francisco.

[9] Malinen, A. 2000. *Towards the Essence of Adult Experiential Learning: A Reading of the Theories of Knowles, Kolb, Mezirow, Revans and Schon*. International Specialized Book Services.

[10] Ericsson, K. A. 2008. Deliberate practice and acquisition of expert performance: A general overview. *Academic Emergency Medicine* 15, 11 (2008), 988–994. 2008

[11] Miller, G. E. 1990. The assessment of clinical skills/competence/performance. *Academic medicine* 65, 9 (1990), S63–7.

[12] Panitz, T. 1999. *Collaborative versus Cooperative Learning: A Comparison of the Two Concepts Which Will Help Us Understand the Underlying Nature of Interactive Learning.*

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

[14] Johnson, D. W., Johnson, R. T., Stanne, M. B., and Garibaldi, A. 1990. Impact of group processing on achievement in cooperative groups. *The Journal of Social Psychology* 130, 4 (1990), 507–516.

[15] Johnson, R. T., and Johnson, D. W. 2008. Active learning: Cooperation in the classroom. *The annual report of educational psychology in Japan* 47 (2008), 29–30.

[16] Karjalainen, M., Kokkonen, T., and Puuska, S. 2019. Pedagogical Aspects of Cyber Security Exercises. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).* IEEE, 103–108.

[17] Karjalainen, M. and Kokkonen, T. 2020. Comprehensive Cyber Arena; The Next Generation Cyber Range. Accepted *for 2020 IEEE European Symposium on Security and Privacy Workshops* (EuroS&PW).

[18] Paulsen, C., McDuffie, E., Newhouse, W., and Toth, P. 2012. NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy* 10, 3 (2012), 76–79.

[19] Newhouse, W., Keith, S., Scribner, B., and Witte, G. 2017. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication 800* (2017), 181.

[20] Saharinen, K., Karjalainen, M., and Kokkonen, T. 2019. A Design Model for a Degree Programme in Cyber Security. In *Proceedings of the 2019 11th International Conference on Education Technology and Computers* (ICETC 2019). Association for Computing Machinery, New York, NY, USA, 3–7. DOI:https://doi.org/10.1145/3369255.3369266.

[21] Master's Degree Programme in Information Technology, Cyber Security. 2019. *JAMK University of Applied Sciences*. Retrieved April 18, 2020 from https://asio.jamk.fi/pls/asio/asio_rakenne_julkaisu.rakenne_komp_osaamisalue?ckohj=YTC&csuunt=99999&cvuosi=9S&caste=J&cark=2019-2020&lan=e