Pedagogical and Self-Reflecting Approach to Improving the Learning Within a Cyber Exercise

Anni Karinsalo[1], Karo Saharinen[2], Jani Päijänen[2] and Jarno Salonen[3]
[1]VTT Technical Research Centre of Finland, Oulu, Finland
[2]JAMK University of Applied Sciences, Jyväskylä, Finland
[3]VTT Technical Research Centre of Finland, Tampere, Finland
anni.karinsalo@vtt.fi
jani.paijanen@jamk.fi
karo.saharinen@jamk.fi
jarno.salonen@vtt.fi

Abstract: In the digitalized world, there is a growing need not only to improve one's cybersecurity skills and knowledge, but also to find ways to optimize the learning process, for example by motivating the learners or optimising the learning facilities, material and the learners for the process. Cyber exercises ran within cyber ranges/arenas (CR) are an efficient way for the exercise participants to improve their cybersecurity skills and knowledge level. The pedagogical way of orienteering the participant to a learning situation is to have a preliminary survey, which prepares the participant for the upcoming event, adds self-reflection, and may even provide feedback and background information for the educator about the upcoming event. The objective of the survey is to improve the quality of the exercise by knowing the interest areas, preferences and other useful information about the participants that is then be used optimise the exercise accordingly. This study analyses the structure of one preliminary survey targeted for the cyber exercise event to be held in January 2022. The questions are justified according to existing frameworks. We have collected a set of structured questions presenting different topics related to the participants' professional background and expectations towards the exercise. In addition to the short-term goal of analysing the survey for one cyber exercise, this work benefits the long-term goal for improving the skills of cybersecurity professionals. Our further work will validate the results of our preliminary analysis and analyse its correspondence with the survey results, and the final analysis constructed after the cyber exercise.

Keywords: cyber range, cyber exercise, cybersecurity skills, cybersecurity, survey

1. Introduction

In the current research, there is an acknowledged need to improve the level of cybersecurity knowledge on European level. This includes both means of personal skill development for the cybersecurity professionals (European Commission. Joint Communication to the European Parliament and the Council, 2020), but also larger-scale, administrative policies such as developing a common European framework for monitoring and developing the skills of cybersecurity professionals (ENISA, 2019) (Nurse et al., 2021).

We perceive the motivating factors for this study from three dimensions. First, we want to extend the pedagogical knowledge of the learning process. The pedagogical aspect of cybersecurity learning has been studied for example in (Karjalainen, 2021) and (Le Compte, 2015). However, to the best of our knowledge, the concept of using a preliminary survey before the cyber exercise has not been employed in a very broad manner. Second, as we will be facilitating a cyber exercise ourselves, we study the ways to improve the cyber exercise practical arrangement with the pre-study from the organiser's perspective. Third, the knowledge we gain regarding learning within the cybersecurity exercise can affect other similar exercises. Thus, we hope our experience will add to the lessons-learned of such events, especially on European level, and where possible, also on the education framework development for security professionals.

The aim of this article is to describe the structure and benefits of, and theory behind the survey that is sent to the participants before the cyber exercise in January 2022. In this article, we argue, that by using a pre-survey to collect information about the participants' professional skills and areas of interest, and fine-tuning the exercise according to the responses, we can impact the development of the participants' professional skills as well as enhance the learning experience during the cyber exercise or other cyber event. The benefits of this study relate to resolving the following research questions:

- How can we better understand the needs and interests of cyber exercise participants (that can also be considered as "customers" in some sense) by using a pre-survey?
- What kind of questions should the pre-survey consist of?

- What kind of existing frameworks can we use to create our pre-survey?

The survey questions proposed in this article are tailored to the targeted exercise, namely Flagship #2, but we will generalise them in future research as well as provide the results from our pre-survey. We consider that this study lays groundwork for the benefits of increased learning about motivation of the participants, acquiring the necessary information for the cyber exercise, and increased general knowledge for the organisation of cyber exercises.

The article is structured as follows. In section two we provide the background to our research, namely describing the European and worldwide guidelines, taxonomies and other frameworks that we have used to create our pre-survey. In section three we introduce the pre-survey and justify the questions that we have decided to use in it. Finally, in section four we discuss the general justifications and lessons-learned for the construction of the study, before concluding the article in the last section.

2. Theory and framework background

2.1 Regulation and theory

The European Higher Education Area (EHEA) was adopted in May 2005 and it specified three cycles of qualification to which national frameworks were encourage to be made compatible with (European Higher Education Area, 2005). The cycles of qualification were updated by 2008 in a recommendation of the European parliament and of the council in establishment of the European Qualifications Framework (EQF) for lifelong learning. This update gave way for an eight level of qualifications; each of which were described by Knowledge and Skills to create Competence. Within the recommendation was also the requirement of mapping National Qualifications Frameworks (NQF) to the EQF from the Member States of the European Union (European Commission. Directorate-General for Education and Culture, 2008). Just before the 10th year anniversary of the EQF, the Council of the European Union refreshed their recommendation. These recommendations were divided into 18 different topics, e.g. to have member states ensure their consistency of national frameworks with the EQF periodically. (Council of the European Union, 2017) Within the European Union this background of guiding frameworks and recommendations give a good background in individual competence building and have established a common terminology within the EU (Brockmann, Clarke and Winch, 2009).

Bloom *et al.* (1956) introduced in their book a taxonomy to *"help (curriculum builders) to specify objectives so that it becomes easier to plan learning experiences and prepare evaluation devices"*. This taxonomy declared six major classes: Knowledge, Comprehension, Application, Analysis, Synthesis and Evaluation. Even though the learner could perform the major classes in different order than introduced in the book; it is still used as a tool of evaluation. Bloom's taxonomy has been revised by Anderson *et al.* (2001) to have a more dynamic conception of the classifications made earlier. Thus, the revised categories / cognitive processes are as follows; Remember, Understand, Apply, Analyze, Evaluate and Create. Curriculum developers use the taxonomy extensively in different universities.

2.2 Cybersecurity frameworks

Cybersecurity, as a paradigm of computing, has been a continuous topic of framework definition in multiple countries and international organisations. Several guiding frameworks have been introduced at the end of the last decade, with continuous work being done at the start of this decade. This chapter introduces the main cybersecurity frameworks related to this research paper.

Background of the *NICE Framework* came from the Comprehensive National Cybersecurity Initiative where one of the objectives was to expand cybersecurity education (Rollins and Henning, 2009). This Initiative was further emphasized into the formation of a National Initiative for Cybersecurity Education or NICE (The White House, 2010). The first available version of the NICE framework was published in 2017 (Newhouse et al., 2017). The framework described the cybersecurity work through tasks assigned to different work roles. These tasks required *Knowledge*, *Skills* and *Abilities* (KSA's) and the work roles themselves were defined into specialty areas and categories.

Association for Computing Machinery publishes their Curricula Recommendations on their web pages (Association for Computing Machinery, 2022). The overview report from 2005 on Curricula guidelines (CC2005

Task Force, 2005) had no section on cybersecurity. This was later published as "*Cybersecurity Curricula 2017"* guideline book in 2018 (Joint Task Force on Cybersecurity Education, 2018) next to the Computing Curricula recommendations of 2005. Finally in 2020 the updated work of ACM published the Computing Curricula 2020 (CC2020 Task Force, 2020) which declared cybersecurity as its own field of education.

In the European Union, several research and development projects had the goal of producing a cybersecurity framework to be used within the European Union. ECSO has published a European Cybersecurity Education and Training - Minimum Reference Curriculum (ECSO 2021) aimed at providing *"the guidelines relative to the competence & skills development framework along with pedagogical methodologies for the higher education programme requirements".* SPARTA -project published its deliverable on cybersecurity skills framework (Piesarskas *et al.*, 2020) with stating *"This document serves as a basis for setting in motion a process of development of a comprehensive European cybersecurity skills framework"*. The framework analysed that European Cybersecurity Taxonomy (European Commission. Joint Research Centre, 2019) to be coupled with the NICE Framework would be a good starting point for a more comprehensive framework for the EU. CyberSec4Europe -project published its own Design of Education and Professional Framework (Karinsalo and Halunen, 2021) which combined a small part of the NICE framework with the ACM Cybersecurity Curricula 2017 Knowledge Areas. Other notable framework is The Cyber Security Body of Knowledge (Rashid *et al.*, 2021) in the United Kingdom, however it is not used in this research paper.

2.2.1 Flagship #1 cyber exercise

Flagship #1 was an online-only cyber exercise, organised in January 2021. The exercise platform used was a cyber-arena, a large-scale cyber range, as a technical platform. Participants used the prepared environment to perform their tasks. Flagship #1 was a reactive cyber exercise, showcasing real-world skills needed in every organisation that uses ICT-services. The task was to detect and investigate a successful cyber-attack that the exercise organisation had previously faced. Once the attack was detected and deemed successful, the participants started following the prepared (cyber) incident management documents and procedures, alerting organisations' staff and stakeholders, and various authorities. Flagship #1 showcased that the organisation benefits from using the existing documentation and procedures in a cyber exercise. When a cyber incident happens, there is some knowledge on the expected behaviour to mitigate and respond to the incident.

During registration to the exercise, the participants completed a short self-assessment questionnaire on their skills and knowledge in cybersecurity and previous experience related to cyber-exercises. This self-assessment was the basis for the preliminary survey covered in this paper. After the exercise, a comprehensive self-assessment questionnaire in skills improvement was filled-out. The post-exercise questionnaire was based on NICE framework KSA's. (CyberSec4Europe, 2021)

2.2.2 Flagship #2 cyber exercise

The forthcoming two-day Flagship #2 exercise showcases a simulated successful cyber-attack targeting a critical infrastructure operator, a train operator using a (simulated) next-generation Rail Traffic Management System. In the scenario, trains have smart devices installed that include Trusted Platform Modules (TPMs). The (simulated) technology is dependent on various ICT-infrastructure services and functionalities located in the train and alongside the railway. Attacking against such technology stack requires besides malicious objectives, also technological skills to avoid or bypass the security controls in a train or infrastructure.

The objective of Flagship #2 is to showcase that analyzing and investigating a sophisticated attack against complex technology requires broad and deep understanding of the technology, and that a (simulated) company, whilst having competent cybersecurity employees may still lack the skills needed. Given the scenario is successful from this point of view, the exercise participants receive support from a (simulated) cybersecurity analyst company that they have hired. The analyst company has a vast amount of workforce that focuses on analysing and investigating complex cyber-attacks. Due to the aforementioned needs, we aim to impact the development of the participants' professional skills as well as enhance the learning experience during the cyber exercise or other cyber event with our pre-survey.

2.3 Target groups

Flagship #2 exercise is targeted to the following target groups:

- Project group members
- Other personnel from project member organisations
- External stakeholders of the project (external cybersecurity analyst role)

In general, the exercise is targeted to any members of the aforementioned groups with interest towards attending the cyber exercise. In other words, one does not need to be a cybersecurity professional to participate even though professionals might benefit from the exercise more than non-professionals. The main difference to the previous Flagship #1 exercise is the inclusion of external cybersecurity analysts who participate in a separate capture-the-flag (CTF) exercise during Flagship #2 and analyse a simulated cyber-attack using real tools and applicable methodology in a dedicated environment. The cybersecurity analyst role has a prerequisite of having previous experience in using Linux command line tools and naturally the exercise benefits cybersecurity professionals more than non-professionals.

3. Survey design

In this section, we analyse each of the survey questions and their theoretical background in order to justify their use. By "survey", we mean the preliminary survey (or pre-survey) which is targeted to the forthcoming Flagship #2 exercise participants.

3.1 Survey design and process

The survey in question is an online survey sent to the registered participants of the forthcoming cyber exercise and it collects information about their competence levels and preferences prior to the exercise. The survey consists of eleven questions with eight single-choice, two multiple-choice and one open question. All but the last question (#11) are mandatory in order to get responses to all survey questions. However, we have included a specific "I prefer not to disclose this information" response to questions #1-#5 that collect information concerning the educational background, knowledge/skill levels, participant job roles and the organisation sector in case the respondent is concerned about the responses. All the other questions are collecting information about areas of interest, preferred exercise roles and opinions about suitable exercise group sizes and session times and therefore they do not have the aforementioned response option. Since these extra response options do not provide additional value to this article, they are not included in the figures nor covered in the next sub-sections. In addition to the survey questions covered in the following sub-sections, the survey also consists of an introductory/invitation text and a field to ask/verify the respondent email address. The email is used for connecting the right pre-survey with the post-survey that will be sent to the exercise participants after the event and used to match the expectations to the learning experience. Since these aforementioned survey parts do not have additional value to this article, we just mention them here.

3.2 Survey questions

The first survey question is shown in the figure below. The question is a single-choice one with four response options categorised according to the European Qualifications Framework (Council of the European Union, 2017). It also includes an "Other, please specify" option in case the respondent doesn't belong to any of the following groups or even has multiple degrees from different areas and would like to clarify.

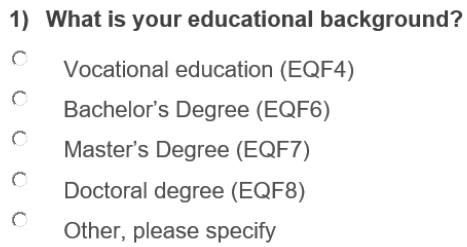
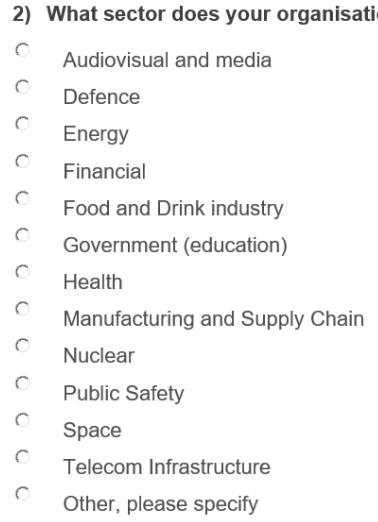


Figure 1: Survey question #1

The first survey question helps the exercise organisation to be more aware of the educational background and competence levels of the participants. With this gained awareness, the cybersecurity exercise could be adjusted or participant roles designed with more precision to match the capabilities of the participants.

The second survey question is shown below. The question is a single-choice one with 12 response options categorised according to the sectors specified in the European Cybersecurity Taxonomy (European Commission. Joint Research Centre, 2019). It also includes an "Other, please specify" option e.g. in case the respondent organisation doesn't belong or doesn't recognize him/herself to be in any of the groups.

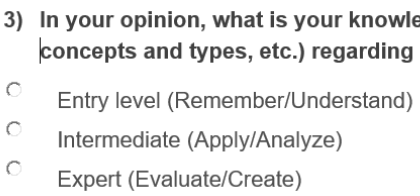

2) What sector does your organisation primarily belong to?

- Audiovisual and media
- Defence
- Energy
- Financial
- Food and Drink industry
- Government (education)
- Health
- Manufacturing and Supply Chain
- Nuclear
- Public Safety
- Space
- Telecom Infrastructure
- Other, please specify

Figure 2: Survey question #2

Given the multipurpose cybersecurity exercises in development to day (Fischer-Hübner *et al.*, 2020) it would be of interest of the exercise conducting organization to get more familiar with the participants organization background. This gives way to customize the exercise towards a certain security of supply area.

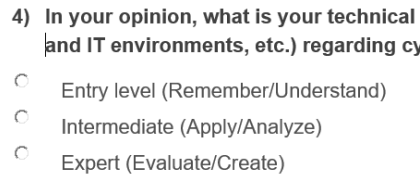
The third survey question is shown below. The question is a single-choice one with three response options categorised according to Bloom's taxonomy (Bloom *et al.* (1956)). This gives a self-estimation of the participants' competence level in this particular area of expertise; of cybersecurity exercises in general.


3) In your opinion, what is your knowledge level (e.g. understanding of exercise concepts and types, etc.) regarding cybersecurity exercises/hackathons?

- Entry level (Remember/Understand)
- Intermediate (Apply/Analyze)
- Expert (Evaluate/Create)

Figure 3*:* Survey question #3

The objective of this question is to categorise participants according to their knowledge level and then, based on the exercise type and objectives, organise exercise groups accordingly. Generally, the groups are formed evenly, i.e. each group has members from each skill level, which makes it possible for the expert level members to assist the entry and intermediate level members during the exercise. However, in some exercise types it is also possible to assign members of the same level into one group, which among others helps the facilitation of the group. In practice this could mean e.g. that the entry level groups receive more comprehensive explanation than others do. The fourth survey question is shown. The question is a single-choice one with three response options categorised according to Bloom's taxonomy (Bloom *et al.,* 1956). As cybersecurity exercises usually are quite technical events, the participants are asked to self-evaluate their competence levels in technical skills.


4) In your opinion, what is your technical skill level (e.g. usage of operating systems and IT environments, etc.) regarding cybersecurity exercises/hackathons?

- Entry level (Remember/Understand)
- Intermediate (Apply/Analyze)
- Expert (Evaluate/Create)

Figure 4*:* Survey question #4

This question is very similar to the previous one, but focuses on the technical skill level of the exercise participants instead of the overall knowhow of the exercise types and processes. The objective of this question is to categorise participants according to their technical skill level and then, based on the exercise type and objectives, organise the exercise groups accordingly. For example, if the exercise supports multiple simultaneous tasks at different levels, then groups could be formed according to the participants' knowledge level and they would complete different tasks or "missions" during the exercise. In case the exercise consists of tasks or "missions" that every group must complete in the same order, then the groups would most likely be formed in such a way that each group has members from each knowledge level. In general, the advantage of having members of different technical skill level in one group may support the learning of those in the lower, i.e. entry and intermediate skill levels. However, there is a rather high probability that the members at expert level perform most of the exercise tasks, which may hinder the learning of the less advanced members. In most cases, it is the role of the group facilitator to monitor the progress and ensure that all members of the group understand the things done during the exercise despite their technical or other skill level.

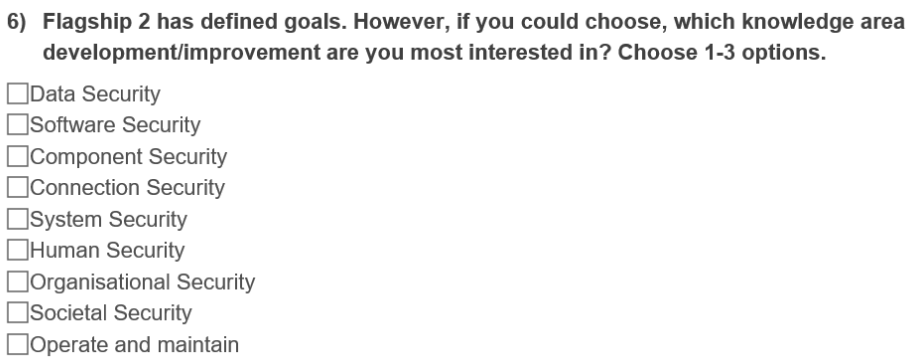
The fifth survey question is shown below. The question is a single-choice one with seven response options categorised according to the sectors specified in the NIST - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse *et al.*, 2017). It also includes an "Other, please specify" option e.g. in case the respondent job role doesn't belong to any of the aforementioned groups.


5) In which category does your job role primarily belong to?

- Securely Provision (SP)
- Operate and Maintain (OM)
- Oversee and Govern (OV)
- Protect and Defend (PR)
- Analyse (AN)
- Collect and Operate (CO)
- Investigate (IN)
- Other, please specify

Figure 5*:* Survey question #5

The sixth survey question is shown below. The question is a multiple choice one with nine options that have been applied from the CyberSec4Europe deliverable "Design of Education and Professional Framework" (Karinsalo and Halunen, 2021). The respondents are instructed to choose from one to three options from the list.


6) Flagship 2 has defined goals. However, if you could choose, which knowledge area development/improvement are you most interested in? Choose 1-3 options.

- ☐ Data Security
- ☐ Software Security
- ☐ Component Security
- ☐ Connection Security
- ☐ System Security
- ☐ Human Security
- ☐ Organisational Security
- ☐ Societal Security
- ☐ Operate and maintain

Figure 6*:* Survey question #6

This question is very important one since it enables fine-grained exercise customisation according to the participants' areas of interest. In case the survey is conducted before or during the planning of the cyber exercise, it may enable quite radical customisation. However, as the question text in the previous figure specifies, the exercise may already have defined goals in which case the customisation could apply e.g. to spending more time in a desired type of session or include additional pieces of information to them in order to enhance the learning process. In case the exercise consists of different simultaneous tasks, then customisation

could be done by grouping the members according to their desired interest areas and choosing suitable tasks for them.

The seventh survey question is shown below. The question is a single-choice one with seven response options categorised according to the sectors specified in the NIST - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017). It also includes an "Other, please specify" option e.g. in case the respondent job role doesn't belong to any of the aforementioned groups.

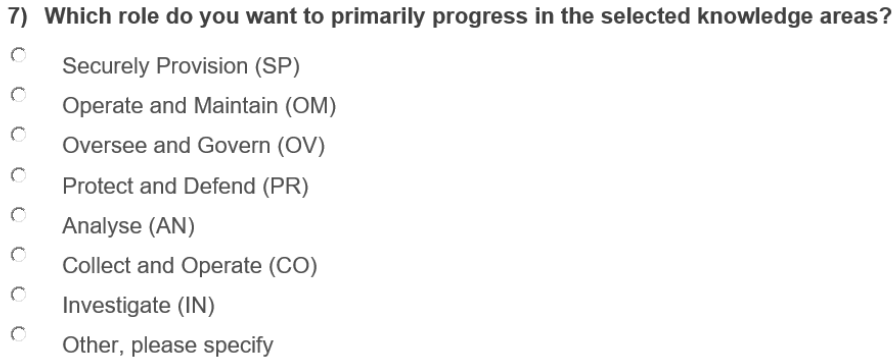


Figure 7: Survey question #7

The objective of this question is to assign suitable roles for each cyber exercise participant and where possible, target some tasks in order to support specifically the learning of specific roles. As an example, the Flagship #2 exercise consists of a parallel capture-the-flag (CTF) type of cybersecurity analyst exercise that is directed specifically to people interested in that role.

The eighth survey question is shown below. The question is a single-choice one with four response options with the objective of collecting the respondent's opinion about their preference regarding the ideal number of participants for the exercise teams.

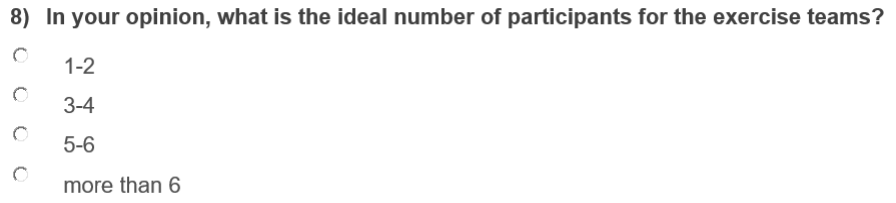


Figure 8*:* Survey question #8

The objective of this question is to assign the participants in groups that are pleasing in terms of the number of members and therefore enhance participation, learning and elements like peer teaching. According to the research by e.g. Koolos et al. (2011), the group-size effect is observed in favour or working in smaller groups (subgroups), i.e. students prefer smaller assignments and smaller groups that enable peer teaching.

The ninth survey question is shown below. The question is a single-choice one with six response options ranging from zero to more than 90 minutes.

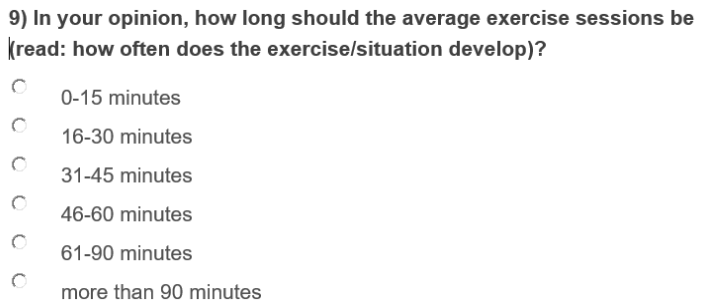


Figure 9*:* Survey question #9

The question relates to the intensity of learning events in the cybersecurity exercise. The effective training length is a topic researched in education e.g. by Ericsson (2006) and Bunce et al. (2010). Since Flagship #2 lasts for two days, the individual sessions are bound to be quite lengthy. However, we are searching for possibilities to adjust the exercise intensity at least to some extent based on the responses to this question.

The tenth survey question is shown below. The question is a multiple choice one with nine options that have been applied from the Cybersecurity Curricula 2017 (Newhouse *et al.*, 2017). The respondent is instructed to choose from one to three options from the list.

Figure 10*:* Survey question #10

Similarly to question six, this question enables customising the exercise contents in detail according to the responses. However since Flagship #2 exercise has already defined goals, customisation applies mainly e.g. to spending less time in the less desired knowledge areas or the related information can be provided as an extra.

The eleventh survey question is shown below. The question is an open one with the instructions to the respondent for giving any thoughts about the exercise or comments/greetings to the organisers.

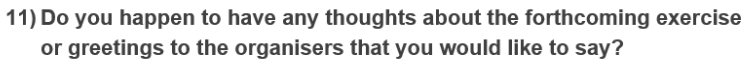


Figure 11*:* Survey question #11

The objective of this question is to allow participants express feelings and raise concerns about the forthcoming exercise, if any. The question is partially linked to the research by, e.g. Arbaugh and Benbunan-Fich (2007) that highlight the importance of participant interaction in online learning environments such as Flagship #2. In other words, the question also intends to motivate them by increasing their engagement to the exercise.

4. Discussion

In this study, we analysed how to use a pre-survey for understanding the needs and interests of the cyber exercise participants. We also analysed how to format the questions, and what frameworks to use when creating the survey. In this context, we constructed eleven questions using existing cybersecurity frameworks. We also provided related justifications based on the Flagship2 event requirements. One option could have been, that we would have used ranking scale for the question selections. However, if we rank the questions, we need to analyse the results with data analysis and come up with a weighted average, which does not serve our purpose with the survey end goal.

Regarding the general structuring of the survey, we concluded that since the audience consists of professionals and the event is voluntary for them (i.e. not a part of a student curriculum), the survey should not be too demanding or time-consuming. If the pre-survey has too complex or too many questions, there is a risk that the respondents do not care to answer. Instead, we will deepen our knowledge by sending another survey after the Flagship2 event. Thus, we optimized the questions to attain as much information as possible while trying to keep the number of the questions as low as possible. Regarding the question setting, we wanted to use the questions to improve the commitment of participants by increasing their motivation. Fishbach et al (2022) describe intrinsic (i.e. internally driven or rewarding) motivation to be “critical predictor of engagement”. According to them, one approach for increasing intrinsic motivation is to factor “the positive experience while pursuing the

activity, with choice." Questions formulated such as question 6, enabling participants feel they can affect or make choices of interest regarding the course content, potentially increase the intrinsic motivation of the participant towards the exercise. Further work will include analysing the pre-survey answers and reflecting them in the summary of the cyber exercise outcomes, lessons-learned and post-survey results.

5. Conclusions

This article presents the construction process and structure of a pre-survey targeted to the participants of a cyber exercise. We have constructed a survey consisting of eleven questions that are based on existing frameworks such as EQF, NICE, European and Cybersecurity Curricula. Based on our current analysis, the questions help us better understand the needs and interests of the Flagship #2 cyber exercise participants. The article also provides related justifications that are linked to the upcoming cyber exercise details.

References

Anderson, L. et al. (2001) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.

Arbaugh, J.B., Benbunan-Fich, R. (2007). The importance of participant interaction in online environments. Journal of Decision Support Systems, 43 (3), pp. 853-865. https://doi.org/10.1016/j.dss.2006.12.013.

Association for Computing Machinery (2022) Curricula Recommendations. Available at: https://www.acm.org/education/curricula-recommendations (Accessed: 10 January 2022).

Bloom, B.S. et al. (1956) Taxonomy of Educational Objectives - The Classification of Educational Goals. London: Longmans, Green and Co Ltd.

Brockmann, M., Clarke, L. and Winch, C. (2009) 'Competence and competency in the EQF and in European VET systems', Journal of European Industrial Training, 33, pp. 787–799. doi:10.1108/03090590910993634.

Bunce, D., Flens, E. and Neiles, K. (2010) How Long Can Students Pay Attention in Class? A Study of Student Attention Decline Using Clickers. Journal of Chemical Education 2010 87 (12), 1438-1443. doi: 10.1021/ed100409p.

CC2005 Task Force (2005) Computing Curricula 2005: The Overview Report. New York, NY, USA: Association for Computing Machinery. Available at: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf (Accessed: 10 January 2022).

Council of the European Union (2017) Council Recommendation on European Qualifications Framework for lifelong learning. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=EN (Accessed: 5 January 2022).

CyberSec4Europe. (2021) "CyberSec4Europe Hosting Flagship 1: An Online Cybersecurity Exercise", [online], Cyber Security for Europe (CyberSec4Europe), https://cybersec4europe.eu/cybersec4europe-hosting-flagship-1-an-online-cybersecurity-exercise/ (Accessed: 15 January 2022).

ECSO (2021) European Cybersecurity Education and Professional Training: Minimum Reference Curriculum SWG 5.2 I Education & Professional Training. https://ecs-org.eu/documents/publications/61967913d3f81.pdf (Accessed: 5 January 2022).

ENISA (2019) Cybersecurity skills development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union (Accessed: 15 January 2022).

European Commission. Joint Communication to the European Parliament and the Council (2020) The EU's Cybersecurity Strategy for the Digital Decade

European Commission. Joint Research Centre (2019) A proposal for a European cybersecurity taxonomy. LU: Publications Office. Available at: https://data.europa.eu/doi/10.2760/106002 (Accessed: 5 January 2022).

European Higher Education Area (2005) The Framework of Qualifications for the European Higher Education Area. Available at: http://www.ehea.info/media.ehea.info/file/WG_Frameworks_qualification/85/2/Framework_qualificationsforEHEA-May2005_587852.pdf (Accessed: 5 January 2022).

Ericsson, K.A. (2006) 'The Influence of Experience and Deliberate Practice on the Development of Superior Expert Performance', the Cambridge handbook of expertise and expert performance, p. 22.

Fischer-Hübner, S. et al. (2020) 'Quality Criteria for Cyber Security MOOCs', in Drevin, L., Von Solms, S., and Theocharidou, M. (eds) Information Security Education. Information Security in Action. Cham: Springer

International Publishing (IFIP Advances in Information and Communication Technology), pp. 46–60. doi:10.1007/978-3-030-59291-2_4.

Fishbach, A. and Woolley, K. (2022). The Structure of Intrinsic Motivation. To be published in: Annual Review of Organizational Psychology and Organizational Behavior, Volume 9, number 1, doi:10.1146/annurev-orgpsych-012420-091122 (Accessed 17. January 2022)

Joint Task Force on Cybersecurity Education (2018) Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. New York, NY, USA: Association for Computing Machinery.

Newhouse, W. et al. (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST SP 800-181. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-181. doi:10.6028/NIST.SP.800-181.

Karinsalo, A. and Halunen, K. (2021) 'Design of Education and Professional Framework'. CyberSec4Europe. Available at: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Framework_Final.pdf. (Accessed: 14 January 2022).

Karjalainen, M. (2021). Pedagogical Basis of Live Cybersecurity Exercises. https://jyx.jyu.fi/handle/123456789/76371 (Accessed: 12 January 2022).

Kooloos, J.G.M. *et al.* (2011) 'Collaborative group work: Effects of group size and assignment structure on learning gain, student satisfaction and perceived participation', *Medical Teacher*, 33(12), pp. 983–988. doi:10.3109/0142159X.2011.588733.

Le Compte, A., Elizondo, D. and Watson, T. "A renewed approach to serious games for cyber security," 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015, pp. 203-216, doi: 10.1109/CYCON.2015.7158478.

Nurse, J. R. C. and Adamos, K. and Grammatopoulos, A. and Di Franco, F. (2021) Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA). Available at: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport (Accessed: 5 January 2022).

Piesarskas, E. et al. (2020) 'Cybersecurity skills framework'. Available at: https://sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf (Accessed: 10 January 2022).

Rashid, A. et al. (2021) 'The Cyber Security Body of Knowledge'. Available at: https://www.cybok.org/ (Accessed: 15 January 2022).

Rollins, J. and Henning, A.C. (2009) Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, UNT Digital Library. Library of Congress. Congressional Research Service. Available at: https://digital.library.unt.edu/ark:/67531/metadc743582/ (Accessed: 10 January 2022).

The White House (2010) Advancing Our Interests: Actions in Support of the President's National Security Strategy, whitehouse.gov. Available at: https://obamawhitehouse.archives.gov/the-press-office/advancing-our-interests-actions-support-presidents-national-security-strategy (Accessed: 10 January 2022).