

# Cyber Exercises in Computer Science Education

Melisa Gafic<sup>1</sup><sup>a</sup>, Simon Tjoa<sup>1</sup><sup>b</sup>, Peter Kieseberg<sup>1</sup><sup>c</sup>, Otto Hellwig<sup>2</sup><sup>d</sup> and Gerald Quirchmayr<sup>2</sup>

<sup>1</sup>*Institute of IT Security Research, St. Pölten University of Applied Sciences, 3100 St. Pölten, Austria*

<sup>2</sup>*University of Vienna, 1010 Vienna, Austria*

**Keywords:** Cyber Exercises, Cyber Security, Cyber Resilience, HEI.

**Abstract:** Due to the strong dependence of companies on their ICT and the high relevance of stable services to remain competitive in the global market, cyber security and resilience play an increasingly important role. However, information security is not only an important issue in the corporate context but also in the societal context. For this reason, nearly all computer science programs at higher education institutions (HEI) incorporate this topic. In this paper, we introduce a table-top cyber security exercise lecture format and the experiences gathered over the last years. The approach is currently used to teach computer science students as well as information security students at two higher education institutions in Austria. Additionally, we briefly highlight how the approach was adapted in order to satisfy the compelling need to teach the course remotely due to Corona restrictions.

## 1 INTRODUCTION

During COVID 19-crisis the security and resilience of critical information system have been more important than ever before. Breaches and cyber security incidents impressively highlighted the importance of cyber security and especially incident response (ENISA, 2020). In order to ensure resilience of systems, and to prepare for a such unpredictable cyber threats, it is necessary to continuously train people how to purposefully react on these threats and to communicate within the team under difficult circumstances (Wilhemson and Svensson, 2014). Therefore, exercises especially cyber exercises, play a central role in establishing a resilient society.

Cyber exercises have gained a lot of attention throughout recent years, especially in the cyber security sector, as an important tool for security training, awareness-building and testing incident response. The EU emphasises the importance of this field in its strategy for the digital decade (European Commission, 2020). Large exercises, that make it to the news, such as CyberStorm (Cybersecurity & Infrastructure Security Agency (CISA), ), Locked Shields (The NATO Cooperative Cyber Defence Centre of

Excellence, 2021) or Cyber Europe (ENISA, 2021), represent only a small fraction of the exercises carried out. Conducting cyber exercises also has an educational value. Through interactive activities, such as simulations and scenarios, exercise participants apply knowledge in practical situations using techniques and tools they are familiar with, thereby deepening their understanding of a particular type of incident (Dewar, 2018).

Although cyber security has gained a lot of attention and also found its way to most modern computer science curricula, the development of skills in the area of cyber exercises still did not get a lot of attention. A major discriminator to more traditional forms of training, especially lectures with test, is the simulation of real-life environments, realistic work environments and especially stress. To change the situation, we started to research how the topic can be taught to students in order to empower them to gain the necessary skill set to develop, run and evaluate cyber exercises in their future.

The major contribution of this paper is the presentation of a didactic concept highlighting how the increasingly important topic of cyber exercises can be taught in higher education institutions (HEI). It further shares our experiences of nearly ten years and outlines the challenges, pitfalls and benefits of cyber exercises in computer science curricula. Using cyber exercises as a learning method allows students at HEI to simulate cyber security incidents for hypothetical

<sup>a</sup> <https://orcid.org/0000-0002-0402-4283>

<sup>b</sup> <https://orcid.org/0000-0003-2280-9604>

<sup>c</sup> <https://orcid.org/0000-0002-2847-2152>

<sup>d</sup> <https://orcid.org/0000-0002-9172-0681>

situations and practice their required decision-making expertise and capabilities.

The remainder of this paper is structured as follows: In Section 2 we provide an overview about existing publications on cyber security exercises as well as on educational planning games. In Section 3 we outline our teaching concept, which was elaborated in the past decade. In Section 5, we highlight the feedback of the students of the corresponding courses. We conclude our work in Section 6.

## 2 RELATED WORK

In this section, we outline the relevant research in the context of cyber exercises in higher education. Besides providing an overview on selected approaches in teaching, we highlight essential literature, which has been influenced the design and conception of the herein presented approach.

The effectiveness and importance of planning/simulation games as a learning and teaching tool has been outlined in the meta-analysis by Vogel (Jennifer J. Vogel et al., 2006). It was found that interactive activities such as games and simulations increase motivation and learning outcomes compared to the traditional teaching methods.

Also Prensky discusses in his paper (Prensky, 2002) how challenging is to keep students motivated through the entire learning process. In contrast to the traditional environment in HEI, playing interactive games can be engaging and achieving some scores or prizes can be very relaxing and motivating.

Steinkuehler emphasizes in (Steinkuehler, 2010) that through games, students can acquire various skills and be more enthusiastic about learning. However, beside acquired knowledge, students, as a complete individuals, have to develop different skills and gain experiences that may help them to think or react rationally in new situations (Blazenska Divjak, 2011).

### 2.1 Cyber Exercise Guidelines

As defined in ISO 22398:2013 exercises are "a process to train for, assess, practice, and improve performance in an organization" (ISO, 2013). Derived from this definition, cyber exercises can be defined as an event, in which organizations simulate a cyber security incident in order to develop and test skills in the prevention, detection, mitigation and recovery of operations from cyber attack or security incident.

In order to facilitate a process of planning and organizing such events, many studies have been conducted, which identified key components of a cyber

exercise. In 2015, the Spanish National Cybersecurity Institute Incibe published a taxonomic classification scheme that provides a comprehensive survey on existing cyber exercises (Incibe, 2015). Based on collected information about existing cyber exercises, the authors defined a set of metrics and indicators for cyber exercise profiling and developed a taxonomy proposal to better plan and improve future cyber exercises.

In Cybersecurity and Cyberdefense Exercises Report (Dewar, 2018), the authors identified goals, types, actors and resources as a core elements of cyber defense exercise and also give insights into the experiences and lessons learned based on various After Action Reports (AAR).

The ENISA Good Practice Guide, which is widely used in the EU, describes the general organizational process from preparation to implementation of local and national cyber exercise (ENISA, 2009). The guide systematically explains the key steps in the lifecycle for exercises (identifying, planning, conducting, and evaluating). According to ENISA, it is essential to incorporate experiences from previous exercises into the planning and setting of framework conditions in order to achieve the best possible outcome. Therefore, in addition to this guideline, the Latest Report on National and International Cyber Security Exercises (ENISA, 2015) was published. The report analyses the consisting data set of over 200 exercises and discusses the outcomes of previous exercises.

Similar to ENISA Good Practice Guide, the Department of Homeland Security published The Homeland Security Exercise and Evaluation Program (HSEEP) (FEMA, 2020). HSEEP's life cycle (Program Management, Exercise Development and Design, Exercise Conduct, Exercise Evaluation, Improvement Planning) is very flexible and can be adapted to different types of exercises.

The Swedish Defence University (FHS) has published a Handbook for planning, running, and evaluating information technology and cyber security exercises (Wilhemson and Svensson, 2014). Besides the detailed description of exercise planning steps, this handbook contains practical experiences from previous exercises and a list of criteria for the technical exercise environment (e.g. Communication preparations, Exercise network, Equipment etc.).

In Cyber Exercise Playbook (Kick, 2015), MITRE describes practical guidance on cyber exercises process and gives an overview of essential activities of every phase. This playbook also provides tips and common pitfalls of previous exercises as well as sample documents and templates to assist planners of exercises.

## 2.2 Cyber Exercises

To get an overall overview of cyber exercise we analyzed after action reports (AAR) of previous cyber exercises and their results of the execution (goals, objectives, scenario, participants etc.). Based on the number of participants, three largest and popular cyber-exercises are Cyber Europe (ENISA, 2021), Cyber Storm (Cybersecurity & Infrastructure Security Agency (CISA), ) and Locked Shields (The NATO Cooperative Cyber Defence Centre of Excellence, 2021).

Cyber Europe is organised by the European Union Agency for Network and Information Security (ENISA) and takes place every two years. These exercises include both public and private institutions and participants from all 28 EU Member States and two European Free Trade Association (EFTA). The usual high-level strategic goals of this exercises are testing EU-level cooperation processes and training EU- and national-level capabilities (ENISA, 2018).

The largest national cyber exercise conducted in the US is organised by the US Department of Homeland Security (DHS). In Cyber Storm VI (US Department of Homeland Security, 2020) more than 1200 experts from both the private and the public sector from the US and abroad participated in order to evaluate and improve Nation's cyber security response capabilities and to strengthen relationships between the Federal Government and its partners (US Department of Homeland Security, 2020).

Unlike the two previous exercises, Locked Shields (The NATO Cooperative Cyber Defence Centre of Excellence, 2021) is an annual full-scale exercise, which is organised by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). A difference to other exercises is, that the exercise did not only focus on national IT systems and critical infrastructure, but also included military systems from nearly 30 nations. In Locked Shields exercises all aspects of cyber attacks are in real-time simulated (i.e. decision-making, legal, communication) (The NATO Cooperative Cyber Defence Centre of Excellence, 2021).

Panoptes (Dimitris Gritzalis, Spyros Papageorgiou, 2016) is a Greek National Cyber Defence Exercise organized annually since 2010 by the Cyber Defence Directorate of the HNDGS. This exercise is a mostly offline Cyber Defense Exercise (CDX) (Dimitris Gritzalis, Spyros Papageorgiou, 2016), so that cyber attacks are not simulated in a real-time. More than 200 participants from different sectors gain an opportunity to evaluate their own capabilities on various scenarios (i.e. Incident Handling, Digital Forensics,

Information Sharing, Following policies and procedures etc.).

Cyber Atlantic (ENISA, 2011) is the joint EU-US table top Cyber exercise organized by ENISA and DHS in 2011. An overall objective was to explore and identify potential improvements in communication and collaboration between EU Member states and US during cyber crisis management activities (ENISA, 2011).

## 3 PERFORMING CYBER EXERCISE IN HEI

In this section, we introduce our approach to teach students planning, conducting and evaluating tabletop cyber exercises in university courses. Related literature presented in Section 2, especially the guidelines (ENISA, 2009), (FEMA, 2020), (Kick, 2015) have influenced the design and conception of the herein presented approach.

In order to set the scope and define the learning objectives we made use of the Bloom's taxonomy (Bloom, 1956). In the following, the main learning objectives are outlines:

- The students understand current threats and are able to model threats.
- The students are able to derive exercise objectives from an exercise task and create suitable high-level scenario.
- The students decide on roles and responsibilities within the project according to the strengths and weaknesses of the planning team members.
- The students are able to refine the high-level scenario into a master scenario event list (MSEL) and the according injects.
- The students are able to manage and run a cyber exercise.
- The students can select evaluation criteria and apply them to come up with recommendations and improvements.

In order to achieve the main objectives, the lecture follows a five-step process (i.e. Knowledge transfer, Group formation, Planning, Conducting, Evaluation)(Hellwig, 2016) depicted in Figure 1.

### 3.1 Knowledge Transfer

The first part of the lecture is dedicated to the knowledge transfer of cyber exercise fundamentals. In this

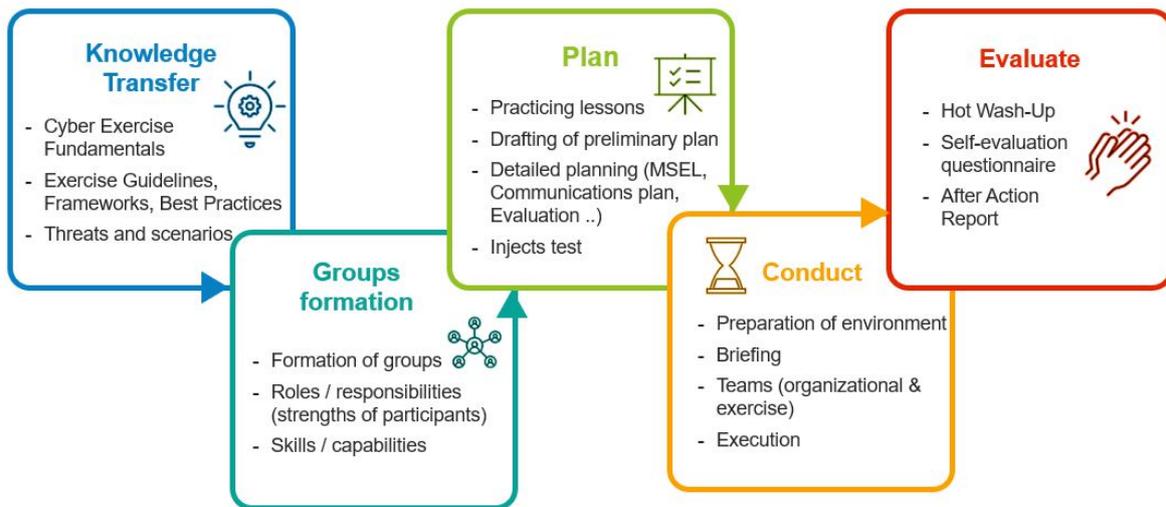


Figure 1: Cyber exercises procedure for courses in HEI.

part the theory of cyber exercises in general and table top exercises in particular are presented. The students learn about current exercise frameworks and best practices in the area, the anatomy of cyber attacks ATT&CK (MITRE, 2021), Cyber Kill Chain (LogSign, 2020), Diamond Model of intrusion (Caltagirone et al., 2013), current threat landscape (ENISA, 2020) and techniques for developing scenarios like Twitter account BadThingsDaily (Hafner, ), CWE (Mitre, 2021) and others.

As the level of knowledge in this area often varies amongst the students, inverted classroom settings showed good results. Providing the students with appropriated sources and guiding questions enables students to learn on their own pace and to dive into the topic.

### 3.2 Group Formation

Within the next section of the lecture student teams are formed. As planning and running a suitable exercise is a challenging task, it is important the team size is not too small (i.e. 8-12 members).

After the teams are established, they have to come up with a strategy how to assign roles and responsibilities. Past courses demonstrated that an effective way to allocate roles and responsibilities often starts by capturing the strengths of each team member, followed by reflecting which roles (i.e. team leader, facilitator, observer/evaluator, counter-player) require certain strengths in order to have a good exercise team structure.

### 3.3 Planning

The planning phase is the most critical part of the lecture. Planning errors can lead to severe problems while conducting the exercise. Therefore, students have to be closely coached during this phase. This planning phase consists of two parts.

In a first part students are asked to set the objectives for the exercises and to derive the skills they want to train and rehearse during the exercise. To define goals, objectives and capabilities, students often use the capability target method from HSEEP Framework (FEMA, 2020) and the SMART Methodology of goal setting (Specific, Measurable, Achievable, Relevant, Time-Bound). After definition of the objectives, the students get the assignment to identify a suitable and realistic high-level scenario to achieve the objectives.

A high-level scenario, as a combination of daily business and cyber attacks, provides stakeholders with an initial idea and intention of the exercise. At the end of the first part, students have developed rough plan that contains the general set-up of the cyber exercise, its goals and objectives, potential participants, roles and responsibilities of the planning team and the high-level scenario.

Succeeding in the second part of the planning phase, a high-level storyboard is developed to set the frame for the exercise. To come up with a suitable storyboard, it has to be defined what happens in each phase of the scenario. The transition from one phase to the next is characterized by time jump (e.g. phase 1: warming up events to learn the roles, phase 2: incident identification and containment, phase 3: eradication and recovery). The concept of phases plays

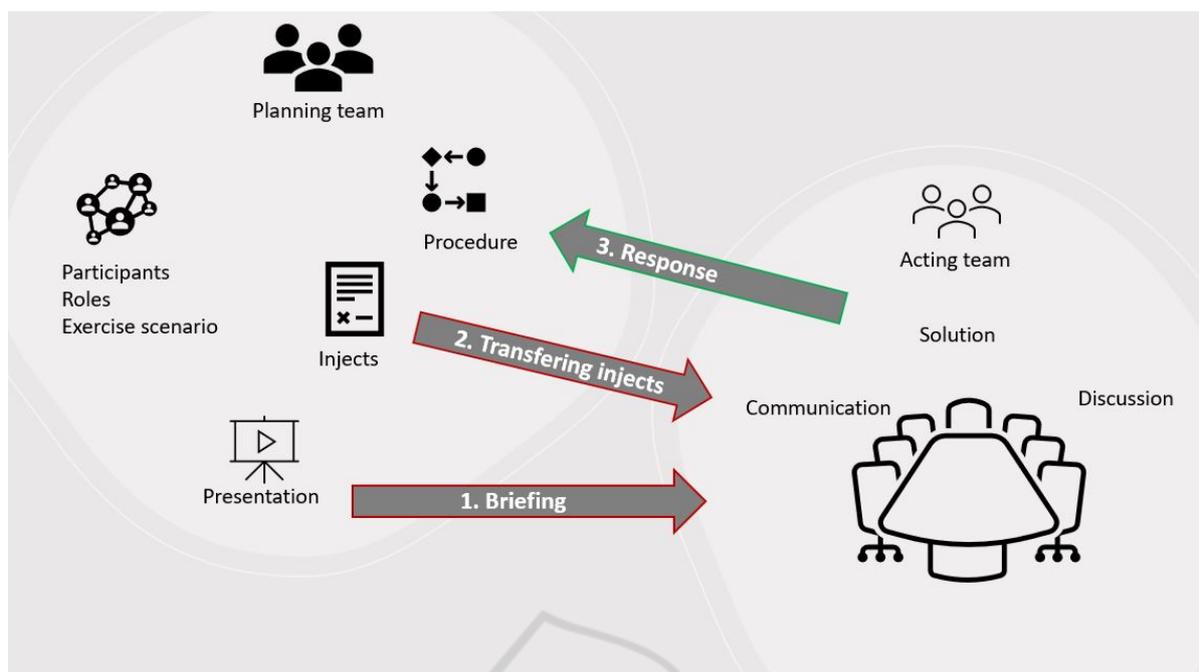


Figure 2: Setting of Cyber Exercise.

an important role in tabletop exercises as they help to synchronize the scenario even if participants are reacting in a different way than expected.

As soon as the high level scenario is outlined within the storyboard, the detailed planning can take place. The goal is to put the participants in a realistic situation in order to subsequently simulate a logical sequence of events. Participants act individually in a situation and can thus influence others with their behavior. For planning purposes, this means that there must be at least two different approaches to reacting to each situation in the exercise. However, it is necessary to make a balance between the path the planning group envisions and the flexibility the exercise requires.

The scenario must be managed throughout the implementation and adapted to the actions of the participants. For this purpose, injects are created to control the exercise and may be the decisive factor in whether an execution of exercise is successful. Typically, students create a template for injects and break them down into three categories: scenario relevant injects (i.e. attacks, cyber incidents), media (i.e. press statements), legal injects (i.e. law, regulations like GDPR). A key document in the planning stage is the Master Scenario Event List (MSEL), that provides an overview (Inject ID, delivery method, target, title, description, assumptions and expected actions) of all injects and ensures timely and organized execution of injects.

In the next step of the planning phase it is necessary to define communications rules with and between participants during the exercise (i.e. what communications channels are allowed, and how does the organisational (communication) structure look like). Moreover, game-rules are defined (e.g. allowed software and hardware, team resources, penalties for any violations during an exercise). Additionally, metrics are defined to make the success of a (cyber) exercise measurable. Usually, metrics correlate closely with the goals of the exercise, as the effectiveness of the exercise is critical for the achievement of the objectives.

The last step in the planning phase is the definition of the evaluation method. An evaluation method is to be designed by each of the group in order to ensure that all players of the exercise learn from the exercise. Moreover, before conducting the exercise, students perform some final preparations in order to test the injects and ensure readiness to start the exercise.

### 3.4 Conduct

After a successful design of cyber table top exercise, the preparation of the environment takes place. Typically this involves setting up the lecture rooms in an adequate manner. For clarification, such a set up could consist of the following steps:

- Assign rooms for the different teams (e.g. recovery team, crisis management team)

- Setup the rooms (e.g. table arrangement, flip charts)
- Test of technical equipment used during the exercise (e.g. email addresses, projectors, phones)

After the setup is complete, a final test is carried out by each group. This is also the last chance to coach the students managing the exercise without interfering the exercise. As soon as all final checks are finished and the exercise environment is ready, the students simulating the exercise participants are welcomed in a briefing by the students managing the exercise.

The aim of the briefing is to explain the exercise rules (e.g. allowed communication media), organizational issues (e.g. assignment of roles, course of the exercise, explanation on delivery and answering of injects, exercise time, exercise end) and the starting point of the scenario. In the course of the exercise, the injects are delivered by the exercise team. Dynamic injects support the exercise management team to adjust the difficulty depending on the performance of the player. In this phase, the lecturers take the role of an observer in order to capture the performance and provide feedback to both teams following the exercise. The main setting of conducting cyber exercise is shown in Figure 2.

The end of exercise must be clearly announced by the exercise leader and is usually achieved, if one of the following states is reached:

- exercise goals have been achieved: the ideal state is that all essential goals are reached by players.
- certain tasks have been completed: another option to determine the end is when all relevant activities have been performed by the exercise participants.
- if it is not certain how to proceed with the exercise: although it has turned out that this case is unlikely to occur, every exercise team leader must be prepared to end the exercise earlier than expected due to unforeseen events or reactions by the players.

### 3.5 Evaluation

After the exercise is declared finished by the exercise planning team, the evaluation begins. The evaluation consists of the two parts *hot wash up* and *after action report*.

Immediate captured feedback is collected within a so called *hot wash up*. The goal using this method is to get the impressions, experiences and opinions right after the exercise. Topics covered by the hot wash up are amongst others: strength and weaknesses of the exercise, performance of the players, achievement of

the exercise goals & objectives, lessons learned of all stakeholders.

The lecture ends for the students by handing in an after action report, which contains the goal and objectives of the performed exercise, information about the scenario and participants results and observation during the exercise as well as feedback of the participants.

## 4 VARIATION DURING CORONA

As the cyber exercise has been planned as physical table top exercise, the concept had to be strongly adapted to work in a remote setting during the Corona restrictions. All physical components, which have been normally used, had to be replaced by virtual means. Figure 3 provides an overview on the technologies used in the various phases of the exercise process.

As Microsoft Teams was already well known by the students, we decided to use this platform as foundation for the course (i.e. for communication and collaboration). Every student group was assigned to an individual team of up to 12 students (e.g. Team A, Team B). Furthermore, teams have been created for conducting the exercises (Exercise A-B). Instead of different rooms, which have been used in physical table top exercises during the exercise in the past, it was decided to use private channels.

Since the scenario definition and planning process mostly is creative process, we decided to use Mural to facilitate collaboration. Mural enables visual collaboration similar to the work on a whiteboard or flip chart and therefore was a good technological replacement for mind mapping, brainstorming or working with sticky notes in the classroom.

To provide a central master scenario event list and store details about the various injects, we created a Sharepoint list. This represented the Master Scenario Event List and supported the students to coordinate the delivery of injects as well as capturing the reaction at a central place. For the evaluation, we decided to perform a hot wash in Microsoft Teams and we prepared a form on a website to capture the experience of the students.

Instead of Microsoft Teams, at the University of Vienna students used an open source conferencing system BigBlueButton for planning and the Discord Server for conducting exercise. Based on our experiences, these tools are also a good alternative and have appeared to be suitable for performing virtual cyber exercises.

Although the COVID edition of the exercise was



Figure 3: Technologies used in the virtual edition.

challenging at the beginning, we could also identify advantages in the collaboration. Students have not been bound by time or place. A major challenge during the exercise in the virtual edition was the coordination of the exercise. For the improvement of the overall coordination, we are currently developing an application based on the captured requirements during the exercise.

## 5 EVALUATION OF THE PROPOSED APPROACH

In the last 9 years, cyber exercises have been used at St. Pölten University of Applied Sciences and University of Vienna for computer science and cyber security students in various settings (i.e. weekly teaching, block teaching). The results and experiences gained during this period are promising. In the following, we briefly provide the lessons learned and results of the evaluations.

The interactive way to elaborate a cyber security scenario and the development of a realistic cyber exercise motivates the students. The feedback of the students also indicated that this way of game based learning encourages students to further deepen their cyber security knowledge.

During the pandemics the well established concept had to be adapted to a remote teaching solution twice. While in the first year there had been minor

issues (e.g. challenges in the technical transformation of the exercises) when rapidly transforming the lecture, in the second year the remote lecture was a big success.

## 6 CONCLUSION AND FUTURE WORK

The COVID-19 crisis and the various cyber incidents in recent months have made us aware of the importance of functioning and secure IT systems. Cyber security and resilience gains importance as business processes and services increasingly depend on functioning ICT systems. Thus, it is no big surprise that security found its way into most modern computer science curricula. Cyber exercises are an effective way to create awareness of cyber security incidents and empowers students to experience various scenarios.

In this paper we introduced an approach for organising table-top cyber exercise in computer science education. The approach consists of five steps: Knowledge Transfer, Group Formation, Plan, Conduct, Evaluate. This approach can be used as template for institutions or companies that want to organize table-top exercises for educational purposes.

The virtual planning and performance of cyber exercises for teaching purposes is still in its infancy. First promising results have been achieved in the last

two years. However, the usage of a variety of tools and media is still a problem to solve. We therefore are working on a prototype, which combines the required capabilities in order to enhance the educational experience.

## REFERENCES

- Blazenka Divjak, D. T. (2011). The impact of game-based learning on the achievement of learning goals and motivation for learning mathematics - literature review.
- Bloom, B. (1956). Blooms taxonomy. <https://www.bloomstaxonomy.net/>. accessed Oktober 2021.
- Caltagirone, S., Pendergast, A. D., and Betz, C. (2013). The diamond model of intrusion analysis a summary by sergio caltagirone.
- Cybersecurity & Infrastructure Security Agency (CISA). Cyber storm: Securing cyber space. <https://www.cisa.gov/cyber-storm-securing-cyber-space>. accessed July 2021.
- Dewar, R. S. (2018). *Cybersecurity and Cyberdefense Exercises*. Center for Security Studies - ETH Zürich.
- Dimitris Gritzalis, Spyros Papageorgiou (2016). Panoptes: The greek national cyber defence exercise. <https://www.infosec.aueb.gr/Publications/CEER-ENISA-2016/%20Gritzalis%20Papageorgiou.pdf>. accessed July 2021.
- ENISA (2009). *Good Practice Guide on National Exercises*. European Union Agency for Cybersecurity.
- ENISA (2011). Cyber atlantic. <http://www.bic-trust.eu/files/2011/12/slides15.pdf>. accessed July 2021.
- ENISA (2015). The 2015 report on national and international cyber security exercises - survey, analysis and recommendations.
- ENISA (2018). Cyber europe 2018 - after action report. <https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report>. accessed July 2021.
- ENISA (2020). *The year in a review: ENISA Threat Landscape 2020*. ENISA.
- ENISA (2021). Cyber exercises - cyber europe programme.
- European Commission (2020). The eu's cybersecurity strategy for the digital decade. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&from=EN>.
- FEMA (2020). *Homeland Security Exercise and Evaluation Program*. Federal Emergency Management Agency.
- Hafner, R. Bad things daily - tabletop scenarios. <https://badthings.tedivm.com/>. accessed Oktober 2021.
- Hellwig, O. (2016). Die gestaltung von cyber-übungen als planspiel. *Planspiele-Vernetzung gestalten: Forschungsergebnisse und Praxisbeispiele für morgen*, 8:187.
- Incibe (2015). *Cyber exercises taxonomy*. Spanish National Cybersecurity Institute.
- ISO (2013). *ISO 22398:2013 Societal security – Guidelines for exercises*. International Organization for Standardization.
- Jennifer J. Vogel et al. (2006). Computer gaming and interactive simulations for learning: A meta-analysis. pages 229–243.
- Kick, J. (2015). *Cyber Exercise Playbook*. The MITRE Corporation.
- LogSign (2020). 7 steps of cyber kill chain. <https://www.logsign.com/blog/7-steps-of-cyber-kill-chain/>. accessed September 2021.
- Mitre (2021). Common weakness enumeration. <https://cwe.mitre.org/>. accessed Oktober 2021.
- MITRE (2021). MITRE ATT&CK adversary. <https://attack.mitre.org/>. accessed Oktober 2021.
- Prensky, M. (2002). The motivation of gameplay.
- Steinkuehler, C. (2010). Video games and digital literacies. The NATO Cooperative Cyber Defence Centre of Excellence (2021). Locked shields.
- US Department of Homeland Security (2020). Cyber storm vi: National cyber exercise. <https://www.cisa.gov/cyber-storm-vi>. accessed July 2021.
- Wilhemson, N. and Svensson, T. (2014). *Handbook for planning, running and evaluating information technology and cyber security exercises*. Swedish National Defence College.