



Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education

Willi Lazarov¹ · Tiina Schafeitel-Tähtinen² · Joseph Squillace³ ·
Zdenek Martinasek¹ · Aneta Coufalikova⁴ · Marko Helenius² · Petr Gallus⁴ ·
Radek Fajdiak¹

Accepted: 10 March 2025
© The Author(s) 2025

Abstract

In today's modern society, it is difficult, nearly impossible, to work and study effectively without using the internet. With services moving into cyberspace and the ever-increasing number of users, new cyber threats are emerging with the potential to cause devastation to both organizations and individuals. For this reason, it is necessary to educate users regardless of their age, gender, and qualification. This paper addresses the challenges associated with the need for cybersecurity education and presents lessons learned from applying an interactive and gamified approach within a cyber range (CR), a controlled environment that enables the deployment of virtual machines and networks for research, training, and testing purposes. In our work, we utilized the CR platform to teach cybersecurity at the primary, secondary, and high school levels of education. Through a series of tests, different approaches, surveys, and feedback collected from students and teachers, we identified their perceptions and critical aspects of CR-based cybersecurity education. We found that gamification positively influences learning, with students emphasizing the fun aspect and teachers highlighting engagement and motivation. Both groups value interactivity for developing practical skills and reinforcing theoretical concepts. Although scoring encourages competition, some students find it stressful. Similarly, penalizing hints can motivate problem solving, but may also deter those needing assistance. These and other findings presented in this paper may be useful for building and further developing cyber ranges to improve the effectiveness of teaching, learning and training cybersecurity.

Keywords Cybersecurity education · Learning environment · Cyber range · Hands-on training · Awareness

1 Introduction

As digital services have been increasingly integrated into many facets of society around the world, risks and threats to cybersecurity also rise. The pervasive presence of cybersecurity threats across various industries (Shulha et al., 2022; Wasserman & Wasserman, 2022), including critical infrastructure, manufacturing, transport, healthcare, or banking,

Extended author information available on the last page of the article

has added pronounced pressure on educators and students to adapt to rapidly changing threats. As criminals also operate in cyberspace, security skills and awareness are even more important. People must be aware of the dangers of the digital world and have the knowledge and skills to protect sensitive data and their digital self (De Bruijn & Janssen, 2017).

Cybersecurity is a global phenomenon that possesses a complex and dynamically changing threat landscape that cannot be easily learned in traditional educational structures. Such a technology-driven world demands success in developing methods and techniques for effective cybersecurity education, which is considered one of the best measures to fight against cyber adversaries and threats. Moreover, security education, along with training and awareness, have been identified as key components to assist in the development of a robust security culture within organizations (Hadlington & Murphy, 2018; Alshaikh, 2020). Education and knowledge form a basis for security awareness (Kruger & Kearney, 2006; Kruger et al., 2010) and it has been demonstrated that as individual awareness increases, they can better defend themselves against cyberattacks and other threats (Zwilling et al., 2022).

To build a more secure digital world, it is imperative to address cybersecurity education at all levels, from primary schools to universities, as well as training of public and private organization employees. Everybody, even young children, use networks and digital services in schools, at work, and in leisure time. Therefore, cybersecurity education should be offered from the very beginning, through all levels of education, and should not be left only to adults in universities (Saglam et al., 2023). Moreover, it is essential to consider prior knowledge and professional experience to better determine the complexity and form of educational training offered, which can be further segmented into learning new techniques and fortifying pre-existing knowledge (Mouheb et al., 2019). Further, the hands-on practice of cybersecurity skills is important for knowledge retention and in establishing skills in such a way that students can seamlessly use them in real-world situations (Wolfenden, 2019).

Ideally, students should develop their security mindset from the beginning of their education in such a way that it grows into a natural way of behaving and acting in the networks and digital services. Appropriate, interesting, and engaging cybersecurity education can help to achieve this goal. Previous research shows that, for example, gamified and game-based cybersecurity education can have positive impacts on students' interest, engagement, and motivation (Pirta-Dreimane et al., 2024; Cole, 2022; Katsantonis & Mavridis, 2021), and can also help in skill building by offering the possibility of hands-on practice and learning by doing (Wolfenden, 2019).

When considering a wide range of students from elementary schools to universities, it is clear that education also needs to be tailored to fit students with very different knowledge and skills. Due to the significant differences between the different user groups, it is evident that a more customized approach should be recognized. Therefore, it is important to take into account the difficulty, duration and form of learning and training (Mountrouidou et al., 2019). As an example, different types of cybersecurity games, competitions, and practical exercises offer educational opportunities that can be adjusted to the difficulty and level of the tasks according to the age and skills of the students (Ros et al., 2020; Matovu et al., 2022; Berisford et al., 2022).

For cybersecurity education, various approaches can be used, ranging from virtualization in computer labs to the comprehensive utilization of the cyber range (CR), a cloud or on-premise platform that enables the deployment of controlled and isolated virtual environments, including fully connected clients, servers, networks, and other types of devices. This approach is particularly useful in education, where it can simulate different scenarios

to teach cybersecurity in a practical and safe way (Blazic, 2021). These aspects were further explored in our research, where we present the lessons learned from applying an interactive and gamified approach to cybersecurity education, which was implemented in the CR platform to teach cybersecurity from primary to higher level of education. Furthermore, we present and discuss testing results, different approaches, and feedback collected from students and teachers to identify their perceptions and critical aspects of CR-based cybersecurity education.

1.1 Key Contributions

We highlight the key contributions of our work, providing a wide perspective on the application of cyber range in different environments. The key contributions of this paper are as follows:

- Application of cyber range platform for education, training, and awareness in cybersecurity at primary, secondary, and higher education levels.
- Presentation of lessons learned from extensive testing of cybersecurity scenarios with students in different environments.
- Identifying teacher, university student, and secondary school student perspectives in a cyber range environment.
- Assess the importance, need, and usefulness of cyber range features through a survey conducted among teachers, as well as university and secondary school students, followed by recommendations based on the survey findings.

This paper highlights different approaches and perspectives on the use of cyber range. The utilization of these platforms can be highly individualized, as demonstrated by the testing sessions we conducted in primary, secondary, and higher education, as well as in different environments of Czech, Finnish, and American universities.

1.2 Paper Structure

The paper is divided into 5 sections. The background and related work on cybersecurity education and cyber range platforms are summarized in Sect. 2. This is followed by Sect. 3 on our application of cyber range and different approaches to teaching cybersecurity in higher, secondary, and primary education. Section 4 presents the different perspectives of our approach from both teacher and student points of view, whose perceptions we investigated through a survey. Furthermore, we discuss the survey results and present the recommendations for the use of cyber range at the end of this section. Section 5 concludes the paper and introduces future work.

2 Background and Related Work

Before introducing our approach and application in more detail, this section provides background information and discusses existing work related to cybersecurity education and the concept of using a cyber range as the main focus of our paper.

2.1 Cybersecurity Education

Security education in general is considered an effective measure against various cyberattacks and threats. To be able to choose secure actions, users must be aware of threats and have sufficient knowledge on how to defend themselves against these threats or mitigate the security risks they pose. Such knowledge and skills are important for every day life, but even more important in workplace and organizational environments, where cyberattacks and data breaches can have serious and widely affecting consequences. Security education, training and awareness (SETA), as well as awareness education, have all been researched, especially in organizational and workplace contexts. For example, early research found that aware employees have better engagement regarding security practices and policies (Bulurcu et al., 2010; Hadlington & Murphy, 2018; Li et al., 2019; Alshaikh, 2020). In addition, aware employees can better identify risks and vulnerabilities and avoid risky workflows (Kirlappos et al., 2015; Alshaikh, 2020). These findings highlight the importance of security education as a key strategy for increasing awareness and enhancing overall security.

The previous research also found out that in organizations, information security training and education can reduce the number of incidents. Kweon et al. (2021) analyzed the relationship between the duration of training, participants, and education outsourcing in relation to the number of cybersecurity incidents. They found a direct correlation between increased time spent on training provided by professional educators and a reduction in the overall number of security incidents. As education can have an impact on different types of incidents, its importance is emphasized. However, security education should not be left solely to organizations and workplaces, nor should it be reserved only for professionals. In today's society, basic cybersecurity awareness and skills can be considered civic skills that everyone should possess. Therefore, the foundation for cybersecurity awareness should be built throughout a person's educational path and across all education levels, regardless of whether the individual is pursuing a cybersecurity or IT-related career.

2.1.1 Cybersecurity in Curricula at Different Education Levels

At the higher education level, universities educate cybersecurity professionals and students using a cybersecurity curricula comprised of highly specialized training and research-based education. In university-level curricula, cybersecurity can be offered as major, minor, or individual courses. At the course level, cybersecurity-specific courses can teach various topics, such as cryptography, network security, and digital forensics. Additionally, cybersecurity-related content may be integrated into other courses, such as software development or networking. The objectives of university-level curricula may vary. For example, educating cybersecurity professionals for various security tasks in industry, encouraging students toward a career in cybersecurity research, or teaching other ICT professionals (e.g., software engineers) the principles of security and the mindset of secure development (Catota

et al., 2019). Universities may also offer general cybersecurity awareness training and courses meant also for students with non-technical backgrounds.

To further enhance their cybersecurity skills, university and secondary school students can participate in various training programs and challenges outside curricula organized by public or private organizations at the national and international level. For example, the National Cybersecurity Lab in Italy organizes (CyberChallenge.IT, n.d.) which is a training program for university and secondary school students. In addition, the European Cybersecurity Challenge (n.d.), supported by the European Union Agency for Cybersecurity (ENISA), is organized annually and aimed at young people under 25 years of age. In the United States, there are various contests organized every year, such as a social engineering themed competition for university and secondary school students organized by the Temple University and the National Science Foundation (Cybersecurity in Application, Research, and Education (CARE) Lab, n.d.). The goal of many of these types of activities is to increase interest in cybersecurity and encourage young people to pursue cybersecurity careers.

At the secondary level education, the teaching of cybersecurity varies according to the field of study. In non-ICT fields, students may only encounter the fundamentals of cybersecurity, especially awareness courses. On the other hand, in the ICT-related fields of study, cybersecurity can be incorporated as a separate course or as a whole study program. In this case, similar to universities, students learn about the practical aspects of cybersecurity alongside its foundations and theory. However, these introductory-level courses are less technically demanding and are designed to provide a deeper background and general education in this domain (Mountrouidou et al., 2019). However, cybersecurity education cannot be overgeneralized at this level of education, because the curricula of schools and universities may vary from country to country or school specific approach.

Some studies have been conducted comparing secondary school and university or college students related to cybersecurity education. One of the related works was done by Peker et al. (2018), which developed an online cybersecurity awareness module and evaluated its effectiveness in raising awareness using pre- and post-surveys. The study involved 122 sary school students and 250 college students. The main finding was that college students' awareness was more affected after studying the module than secondary school students. However, awareness also increased among secondary school students. The study concluded that the experiences of the participants and the level of cybersecurity knowledge should be considered when the goal is to influence their awareness. In addition, they mention that it is essential that young people are educated early about cybersecurity awareness.

At the primary level of education, cybersecurity education is the least encountered. This is due to an overly general education with only basic or missing technical courses. However, multiple approaches have been presented in pedagogy literature to increase children's awareness of cybersecurity (Quayyum et al., 2021), for example, videos, interactive storytelling, and digital comics have been utilized for this purpose with positive outcomes. In addition, game-based and gamified approaches, such as in Kumar et al. (2018), Bioglio et al. (2019) and Vanderhoven et al. (2015), have been investigated among children, but they are focus more on privacy-related awareness. In these studies some have shown an increase in privacy awareness among children (Bioglio et al., 2019; Vanderhoven et al., 2015). As nowadays even young children are internet users and are exposed to a large number of cyber threats (Valcke et al., 2010), there is a need for cybersecurity education in primary schools to some extent. However, this opens up further challenges, as the age difference between user groups in educational level is significant, requiring various approaches to ensure effective learning.

2.1.2 Educational Strategies and Approaches

In curricula, cybersecurity teaching has many approaches. The combination of lectures and hands-on laboratory exercises is often referred to as traditional teaching, and although the exercises give students the opportunity to try learned concepts in practice, they often lack problem-solving perspectives similar to real-world situations and thus fail to build these skills (Shivapurkar et al., 2020). Further, lecture-based teaching can be passive from the students' perspective if the teacher is not using active learning methods, such as demonstrations, discussions, or quizzes, to activate and engage the students.

To address the problems of traditional teaching, problem-based and case-based learning, originating in the field of medicine, has been introduced to cybersecurity teaching (Shivapurkar et al., 2020; Deng et al., 2022; Ahmad et al., 2021; Yuan et al., 2010; He et al., 2014). In these approaches, students are presented with a real-life problem that is solved in a small group. The key difference is the role of the teacher. In problem-based learning, students are more independent, but in case-based learning, teachers can guide students, for example, by asking helpful questions (Srinivasan et al., 2007). In cybersecurity teaching, students have considered case-based approaches engaging and relevantly improving cybersecurity knowledge (Ahmad et al., 2021). They have also improved interest and motivation, increased knowledge and skills, and deepened understanding of the concepts (Yuan et al., 2010; He et al., 2014).

To further increase the students' active participation in learning, gamified or game-based teaching can be utilized. In game-based learning, active learning is included, as games require active decision making and interaction with the content, thus increasing the engagement (Plass et al., n.d.). The gamified teaching approach is considered well-suited for cybersecurity teaching and learning, as games also offer the opportunity to practice and acquire skills in real-world like situations (Wolfenden, 2019). In addition, cybersecurity teaching with a gamified approach shows promising results at all levels of education, including adults in employment. For example, the cybersecurity awareness program in an organization was gamified and the result was more engaging and effective than traditional awareness programs (Abu-Amara et al., 2024). In another example, a serious game for raising awareness among software developers about secure coding guidelines was presented, showing that the game was useful for awareness (Zhao et al., 2024). In higher education, various game-based or gamified interventions have gained high scores from players regarding effectiveness in learning and engagement (Katsantonis & Mavridis, 2021; Malone et al., 2021). At the secondary education level, educational games have, for example, improved knowledge of strong passwords (Qusa & Tarazi, 2021), and affected students' self-awareness of cybersecurity (Salazar et al., 2013). Furthermore, game-based and gamified teaching has increased security awareness among children at the primary education level (Bioglio et al., 2019; Vanderhoven et al., 2015).

Another way to enhance the suitability of game-based or gamified teaching in cybersecurity education is by combining it with problem-based learning. This approach has been studied in the field of mathematics, where it has increased students' grades, creativity and engagement (Boom-Carcamo et al., 2024). In cybersecurity teaching, gamified simulations and scenarios, for example, in the form of Capture The Flag (CTF) sessions, can improve the problem-solving skills, support traditional lecture-based teaching and enhance students' confidence in their own abilities (Leune & Petrilli, 2017).

2.2 CTF-based Learning

In cybersecurity context, CTFs are gamified exercises, where students look for “flags” that contain hidden text strings (e.g., in the vulnerable websites), or which are revealed after successfully completing a cybersecurity task (e.g., password cracking). There are several types of CTFs and each type can be organized for teams or individual users (McDaniel et al., 2016; Cole, 2022). For example, in team-based CTFs, participants form teams that compete against each other in hunting flags, or alternatively, try to steal flags from another team. In individual-based CTFs, participants look for flags from vulnerable systems and environments by themselves, but there can still be competitive elements (e.g., the scores of all participants can be listed in the scoreboard during the CTF).

To further explore learning based on CTFs among secondary school and university students, we reviewed some recent research papers. McDaniel et al. (2016) analyzed results of GenCyber camps, which were CTF competitions for secondary school students. The goal was to introduce students to cybersecurity concepts and also encourage them to study further. They found that this type of competition was an effective way of increasing the student’s understanding of cybersecurity. However, they also found that participants may have deficiencies in basic ICT skills, and this should be taken into account when designing tasks, as these students may not be able to effectively explore the concepts or may have difficulties in using the tools. The study concludes that proper introductory tasks designed to introduce the tools may help.

Ibrahim et al. (2020) had a similar CTF event for secondary school students in Malaysia. Their goal was to introduce students to cybersecurity and raise interest in the subject. Students participated in the pre- and post-test during the event, and their cybersecurity interest and intentions to pursue cybersecurity education opportunities were measured. The result was that the number of interested participants increased, but the intention of learning more decreased. The authors explain this by mentioning that some challenges were quite technical and hard, especially if the participant did not have a cybersecurity background. In addition, they measured the impact by asking students to assess their gained cybersecurity knowledge. The participants agreed that they had learned a lot during the CTF event.

Previous research has also explored the impact and effectiveness of CTFs among university students. For example, Cole (2022) compared the concept of CTF exercises to traditional exercises and found that both had similar learning results, but CTFs increased student motivation. Similarly, Beltran et al. (2018) reported an experience in changing virtual exercises to CTF. The study found that the students perceived the CTF approach as more useful, interactive, collaborative, and motivating. Furthermore, in their research, Karagiannis and Magkos (2021) found that CTFs increased students’ confidence, had positive outcomes in terms of technical skills and knowledge, and the learning process was considered engaging. In addition, Chothia et al. (2019) studied the narrative aspects of the CTF exercises and found that story engagement was associated with better course performance. Students appreciated the entertainment aspect of the narrative, which in turn improved their engagement.

In summary, CTF-based learning has positive impacts on the learning process, participation, and motivation of students. In addition, the task-based nature of the CTFs allows designing the games in such a way that the task difficulty gradually increases, encouraging students to use their capabilities and building self-confidence along the

successfully performed tasks (McDaniel et al., 2016). Furthermore, tasks can be built in such a way that they reflect real-world problems, and their solution teaches students to use real-world tools (Karagiannis & Magkos, 2021; Wolfenden, 2019). In other words, students gain practical experience in situations that they might encounter in their possible careers as cybersecurity professionals. Therefore, the suitability of the CTF-based teaching approach seems very promising in a cybersecurity context.

2.3 Cyber Range

Due to the versatility of the gamified teaching approach and the ability to support active learning and problem-solving skills, we have focused on CTF-based learning in this research. With the implementation of CTF-based learning, we forecast good results in building cybersecurity skills, improving confidence in newly learned cybersecurity skills, and demonstrating positive results across all student education and background levels. Based on the projected results from this learning approach, we recognize the potential for our CTF-based learning approach as a suitable and sustainable framework for cybersecurity education and long-term teaching using a dedicated cyber range. CR platforms offer one way to teach cybersecurity practically. These platforms provide a comprehensive environment for teaching, training, or research in the field of cybersecurity. The number of cyber range platforms has grown significantly since the inception of the industry and with that comes a wide range of features, such as interactive graphical user interface (GUI), customizable training scenarios, sandboxes (isolated virtual machines and networks), automation and orchestration, or logging and monitoring system (Lazarov et al., 2023). These platforms can be deployed as on-premise (self-hosted) solutions or in public and private cloud environments.

The learning and training environment in the cyber range is built on the concept of CTF scenarios described in Sect. 2.2. According to the taxonomy proposed by Yamin et al. (2020), CR platforms can be further assessed by scenarios, monitoring tools, scoring types and methods, management roles, teaming types, etc. Based on Yamin et al. (2020), Ukwandu et al. (2020), Lates and Boja (2023) and our experience with building cyber range, we present the basic taxonomy in Fig. 1.

The application domain of cyber range can vary from education to testing advanced technologies. A comprehensive review of CR platforms and related testbeds conducted by Ukwandu et al. (2020) states that cyber ranges are predominantly used for education and research in academia (31%), followed by applications in the commercial sector by private organizations or the military to provide training (24%). The authors then list the remaining 15% of cyber range application domains for government purposes and 2% of free use as open source.

In relation to this research area, there are papers that directly deal with the CR domain. From recent work, Katsantonis et al. (2023) summarizes existing approaches to building cyber ranges and presents its own Cyber Range Design Framework (CRDF) for the development of cybersecurity education, training, and assessment approaches. Similarly, but with a focus on the military, Park et al. (2022) presents a model for combining multiple CRs for the purpose of hands-on training and testing cybersecurity. Other authors are more focused on building their own cyber ranges. The scope of these CR platforms is wide, which we have already summarized and discussed along with CTF-based solutions in our previous work (anonymized self-citation).

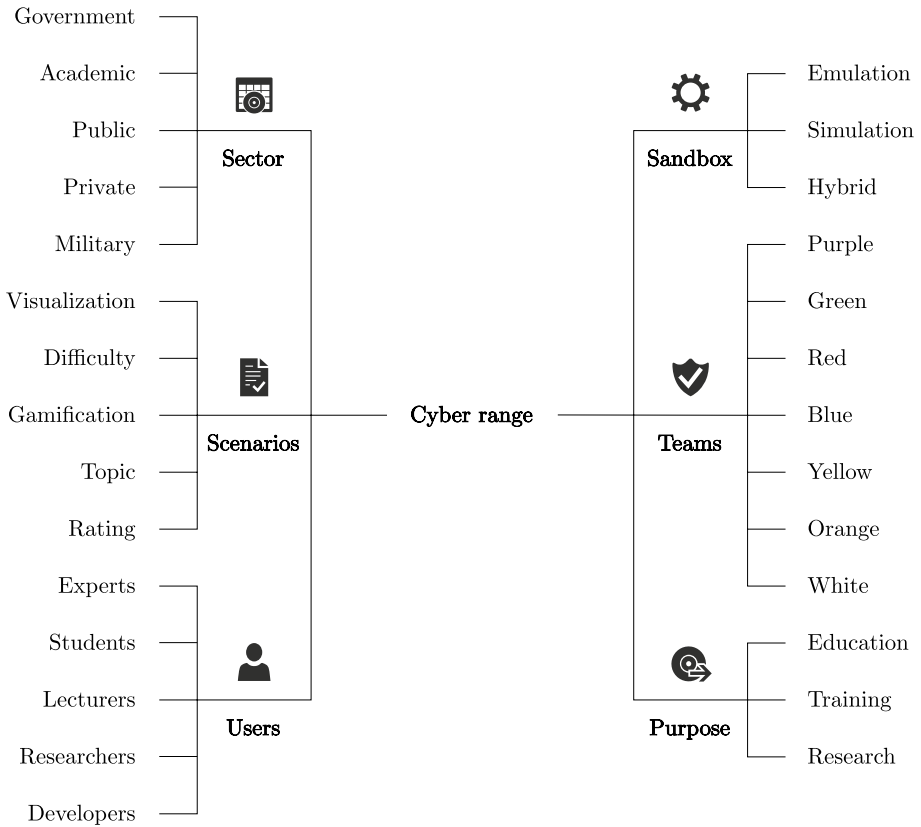


Fig. 1 Taxonomy of cyber range

The main advantage of CR platforms is the ability to deploy controlled and isolated environments that can represent home or enterprise networks including fully connected clients, servers, networks, and other devices (Chouliaras et al., 2021). This environment is called a sandbox and can be used to efficiently perform teaching, training, research, testing, and other activities for which the sandbox was deployed. However, CR platforms come with several drawbacks, such as the complexity and cost associated with their deployment, operation, and maintenance. This also entails the need to have an infrastructure with sufficient computing power and technical staff or the need to use public cloud services (Katsantonis et al., 2023).

3 Cybersecurity at Different Levels of Education

We utilized the BUTCA (Brno University of Technology Cyber Arena) cyber range platform for teaching and training cybersecurity (Brno University of Technology, n.d.). BUTCA is an integrated hybrid platform that serves as a controlled environment for cybersecurity education. The platform has its cyber-physical environment (see Fig. 2) with various scenarios in ICT and industry and offers a wide range of customizable scenarios

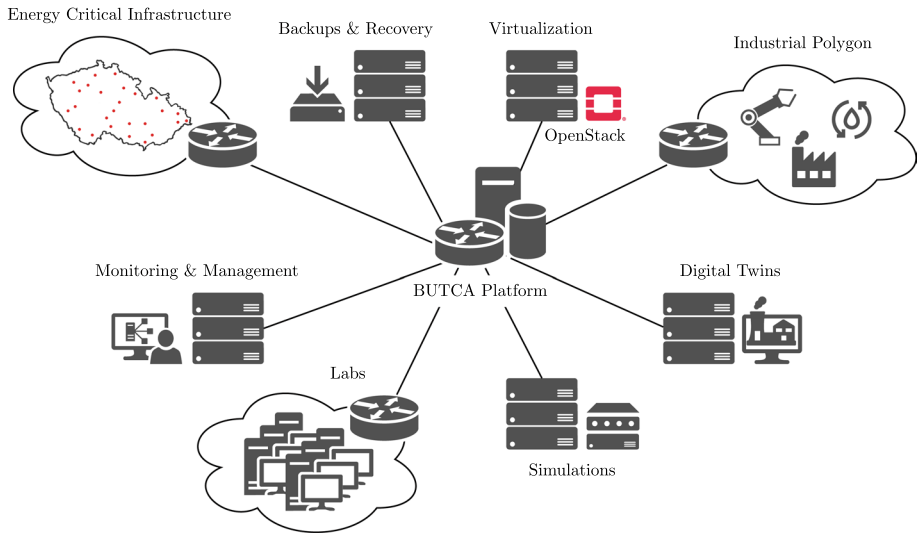


Fig. 2 Cyber-physical environment of the BUTCA platform

according to the user's needs, which is further enhanced by the possibility of creating completely customized scenarios at the level of a given user group (Lazarov et al., 2023). One of the main benefits of the application of this platform at different levels of education is remote access without the need to have its own infrastructure, and the technical requirements for users are therefore minimal.

In applying this platform, we have used the Capture the Flag (CTF) concept at all levels of education for hands-on training. The goal of CTF is to get the flag that represents the correct solution for a given task (challenge). The flag can be anything in the context of the training scenario, for example, decrypted text, IP address, password, etc. McDaniel et al. (2016). Students enter the solution in the form of a flag into the cyber range platform. If needed, students are provided with hints during the solution, which may be penalized by a loss of points.

3.1 Higher Education

We have applied the cyber range concept through the BUTCA platform at 5 different universities across three countries – Czechia, Finland, and United States (U.S.). Since teaching in each setting varies in Europe and the U.S., but also within states and at each university, we have divided the approaches to teaching cybersecurity into the sections below, where they are described in detail. The methodology is primarily based on the educational settings of each university and the author's experience with the methods, tools, and platforms used to teach cybersecurity. Each approach presents different perspectives but also

common challenges, from which we summarize lessons learned in higher education at the end of this section.

In general, technical universities offer bachelor's and master's degree cybersecurity study programs. The curriculum in these programs is designed in such a way that students attend optional theoretical lectures, which are often followed by practical laboratory exercises (ENISA, n.d.). Cybersecurity courses may also include semester projects, seminars, and invited lectures from experts in the field. It is important to note that the curricula are fully directed by the universities and can vary significantly across institutions.

3.1.1 Approach No. 1—Brno University of Technology (Czechia)

For hands-on cybersecurity training at Brno University of Technology, we started to use virtualization on the VMware platform (Broadcom, n.d.), where each student, according to the assignment of a laboratory task at the beginning of the class, imported a virtual machine (VM) and solved the task on a computer in the lab. However, we encountered several drawbacks when using this approach. The first is the limited functionality of the VMware Workstation Player, in particular the inability to take snapshots of virtual machines, due to which students can lose their work due to incorrect VM shutdowns and cannot simply revert to the default settings. With the inability to set up the network appropriately (identical for each student or group of students), the tutorial cannot be unified appropriately, and students make far more mistakes. This puts a lot of demands on the teacher, who is constantly correcting errors in student commands (e.g., wrong IP addresses, interfaces, etc.). Another major disadvantage of using VMware Workstation Player is the frequent version changes that can make part of the task non-functional. The teacher has to choose between an outdated VMware Player or version monitoring on all devices in the lab. In addition, testing the lab before the start of the lesson is also time consuming.

In order to improve the performance of lab assignments, we decided to partially replace PDF assignments with assignments in the CTFd platform (CTFd LLC, n.d.), which provides an easy way to create CTF scenarios through a web interface. However, the disadvantage of this solution is the inability to restrict the sandbox environment to individual students, who may interact with each other. In other words, the CTFd platform is more usable for simple games and also primarily for practicing offline experiences (e.g., forensics, password cracking, etc.). Setting the privileges for individual users and the visibility of platform elements is not entirely intuitive and places considerable knowledge on the user.

After years of experience with virtualization on lab computers, we decided to apply cyber range as a replacement for this method of hands-on training. This proved to be a suitable solution, as it minimized the activities of the lecturers who had to test the lessons in advance and solve any technical problems with the virtual machines. The BUTCA platform eliminates this necessity by automating the deployment of the sandbox environment, restoring it for other students, or destroying it after the end of the lesson. This allows lecturers to give more attention to students without having to solve local technical problems. We introduced this approach to other universities, namely the University of Defence and the University of Hradec Králové.

Based on their interest, we started to integrate the BUTCA platform into their cybersecurity curricula.

Based on the experience described above, we summarize the lessons learned from using virtualization and cyber range platforms as follows:

- The dependency of lab assignments on virtualization platforms brings challenges related to the maintenance of VMs and the need to handle potential technical issues.
- Automated deployment, recovery, and destruction of sandbox environments reduce the technical demands associated with preparing the lab lessons.
- CR platforms facilitate the preparation and supervision of hands-on cybersecurity training, which allows lecturers to give more individual attention to students.

3.1.2 Approach No. 2—University of Defence (Czechia)

To provide further experience with virtualization, we present the perspective of the University of Defence, where the VMware virtualization platform was previously implemented for hands-on training. In this context, similar drawbacks were identified as previously described. Additionally, the high management and maintenance requirements of the environment, coupled with the VMware licensing policy, prompted a shift towards a combination of two different methods of hands-on training. We created smaller standalone labs using Oracle VM VirtualBox (Oracle, [n.d.](#)), while freely available gaming platforms designed for cybersecurity hands-on training were also utilised, including HtB (Hack The Box, [n.d.](#)), picoCTF (Carnegie Mellon University, [n.d.](#)), and THM (TryHackMe, [n.d.](#)).

The first method of virtualizing standalone labs using Oracle VM VirtualBox showed several advantages. It was possible to create custom labs according to specific requirements. This approach was particularly useful when working with the military to implement the lessons learned in the training of future cybersecurity professionals. In addition, the use of snapshots and the ability to try different approaches to solving tasks without fear of loss or corruption of the data were beneficial. Technical issues were minimal during the transition to the new version of VM VirtualBox. Conversely, we were not able to monitor student activity across all labs, centrally assess student activity, and thus optimize the course of further training. It was also necessary to manually distribute new labs to all lab stations and solve technical problems individually. These disadvantages increased the demands on lab administration and trainer activity.

The second method used to provide cybersecurity lectures and labs at the University of Defence in parallel with the first one was the usage of third-party cloud CTF platforms, in particular the well-known Hack The Box and TryHackMe, alongside, for example, picoCTF developed by the American Carnegie Mellon University. The advantages were undoubtedly the low demand for own hardware and the availability of technological and documented exercise scenarios. On the other hand, the possibility to deploy our own scenarios tailored to the specific needs of training future professional soldiers, IT specialists, was lacking.

The advantages and disadvantages of the two methods did not complement each other. The benefits of one method did not cover all the drawbacks of the other, and vice versa. However, one key aspect was missing from both methods, namely some automation to save time on infrastructure deployment and configuration management using open source tools such as Ansible (Red Hat, [n.d.](#)), Terraform (HashiCorp, [n.d.](#)),

Kubernetes (Cloud Native Computing Foundation, [n.d.](#)), or Jenkins (LF CHARITIES, [n.d.](#)).

Through experiments in the preparation and delivery of hands-on cybersecurity training, the University of Defence has identified four aspects that are crucial to the quality of cybersecurity professionals training:

1. Use of a centralized learning platform.
2. The ability to create custom scenarios.
3. Automation of deployment and management.
4. Undemanding on students' hardware.

These requirements can be met by applying cyber range, which is why we ended up following the Brno University of Technology approach described above.

3.1.3 Approach No. 3—Tampere University (Finland)

In Tampere University, information security is offered as advanced studies in master's degrees and as a minor for different degrees through the university. The basic cybersecurity course (Cybersecurity I) is mandatory for all ICT students. The more advanced course (Cybersecurity II) is mandatory only for information security students and has a perspective of cybersecurity as a profession. There are also some adult learners in these courses. The advanced courses in Tampere University cover topics such as cryptography, security protocols, side-channel attacks, and more, as these are the university's research focus. Tampere University also offer a basic cybersecurity course of the lower and more general level, which is available to all students at Tampere University regardless of their field of study.

We integrated two different difficulty level scenarios from BUT Cyber Arena as part of our Cybersecurity I and Cybersecurity II courses. The idea was to complement the course content by adding CTFs as voluntary practical exercises. Students could earn extra course points by participating in the CTFs. We did not track student performance in the scenarios but instead collected their learning experiences of using cyber range through surveys.

Overall, the student experience has been very positive. Students have expressed engagement and excitement during gameplay. Also, successful problem solving has been very satisfactory, especially if the student had some problems and then finally the task was resolved. Some students who started with the beginner scenario also signed up to play the more advanced one, as they considered the first scenario so engaging that they wanted to try the more difficult one. Some students have also asked if we could provide more scenarios as they have found learning efficient and fun with these scenarios.

However, we also had students for whom the scenarios have been too difficult. This has led to situations where the student uses all the hints the task offers but still cannot solve the problem. The student then takes the last hint, which gives the flag to proceed, but feels frustrated as the task did not succeed, and the student necessarily does not understand what went wrong. Based on our experience, the lab teacher should recognize these situations and offer more help to solve the problem instead of using a given flag. If this helps to solve the problem, the student is less frustrated and is able to feel achievement, which would not happen if the student proceeded with the given flag. The hint structure of the scenario could also take into account these types of situation. Instead of automatically offering the correct flag as the last hint, it could tell the student to ask for help from the teacher (if he/she is presented in the lab).

Overall, we see the cyber range as a very good way to complement cybersecurity teaching and to add practical elements to teaching, in a student-engaged manner. According to survey data from Tampere University, participating in CTFs builds students' self-efficacy related to the tasks at hand and increases knowledge and skills related to tasks (Lazarov et al., 2023). CTFs can offer students feelings of achievement that traditional lectures and exercises do not necessarily promote as strong. Based on this approach from Tampere University, we present the following lessons learned:

- Cyber range scenarios can be utilized in a non-competitive manner to support cybersecurity learning and self-efficacy.
- In a non-competitive setting, the teacher can guide students who have difficulties with the tasks to ensure learning and the feeling of achievement.
- Some students need encouragement to try new tools; in a non-competitive setting, teachers can provide the necessary support.

3.1.4 Approach No. 4—Penn State (United States)

PSU prepares students in all facets of the education process, from education theory (theoretical) to practice (practical learning); necessary for learning the requisite skills needed for employment after graduation in a career within the cybersecurity domain. To ensure students are academically prepared, PSU deploys a systematic approach to teaching the cybersecurity curriculum that includes integrating classwork, research, hands-on labs, cyber certifications, and an industry internship into the framework of the cybersecurity degree. One method that has historically proven successful and popular with high student engagement is hands-on activities that provide cyber labs and practical cybersecurity exercises. This directed training for a specific education goal introduces the theory (education) first, then directs the students to demonstrate proficiency of the education in a hands-on lab practical.

To compare different approaches to hands-on cybersecurity training, PSU has engaged in an initial research collaboration with the Brno University of Technology. In this preliminary investigation, a control group of cybersecurity undergraduate students from the Penn State Schuylkill campus worked with the PSU research team in evaluating several different methods for learning cyber skills through hands-on labs and exercises. In this project, students would compare Practice Labs (ACI Learning, n.d.), CYRIN (Architecture Technology Corporation, n.d.), Infosec Institute (Infosec, n.d.), and the BUTCA cyber range platform (Brno University of Technology, n.d.) (conducted by PSU student cohort at BUT in March 2024 in Czechia). Students (and faculty) provided direct feedback on hands-on labs and cyber activities, focusing specifically on the challenges they faced, things they liked/disliked, suggestions for improvements, and suggestions for change. Over the first three months of the academic semester (January 2024–March 2024), students were given hands-on labs and online cyber activities in a traditional setting with the assignments scored using standard metrics for evaluating skill mastery. Faculty instructors teaching cyber and information technology (IT) courses using these platforms were also included to solicit feedback on the engagement from an academic perspective.

Hands-on activities were conducted in class as online projects, homework assignments, quizzes, and labs. After each assignment was completed, feedback and discussions were completed with both student participants and faculty about their shared

experience(s). The Practice Labs platform uses a VPN (students had a choice of (Oracle Virtual Box, VMWare, or Parallels) and requires students to access the lab assignment inside the VPN once connected to the external Practice Labs server. Students stated they “enjoyed the individual labs and the task objectives” they were assigned, however, students complained about issues that degraded their overall experience. Major issues identified by student’s using the Practice Labs environment include: (1) connectivity problems with the Practice Labs network, (2) external load balancing issues that reduced the speed and efficiency of the Practice Labs environment, (3) consistent issues within the Practice Labs environment when trying to download lab files in the VPN when using the designated VM, and (4) problems authenticating individual accounts using 2FA inside the Practice Labs environment using the VM.

Student use of the InfoSec Institute platform as a learning tool was also met with negative results similar to those experienced from using Practice Labs. Students stated that using the InfoSec Institute platform “felt less like a hands-on lab exercise and more like an online learning platform.” Students noted that while the individual lab assignments were time-consuming to complete, they possessed almost no academic challenge as each lab assignment included a full complement of self-paced activities containing full instructions and steps to take for successful task completion. Similar to Practice Labs, students did not feel challenged at all while performing the lab assignment as completion required very little critical thinking. Furthermore, use of the InfoSec Institute platform requires a high per-student cost. Each student needs to purchase platform access for each specific course they are enrolled in (separate courses have separate licenses), and repeat the process for each course, every semester the student is enrolled.

From the U.S. compliment, the CYRIN platform received the most positive feedback and the highest praise from both student participants and faculty advisers. The platform uses a dedicated IP address that students access directly online and then enter into a predetermined lab scenario. Here, students are first guided through the steps to learn the materials in a similar way as Practice Labs. However, the CYRIN platform provides more resources that are easily noticeable when completing the lab assignment(s), including increased bandwidth allocation to ensure students do not experience network, connectivity, or platform interface errors or concerns. Students were also afforded the ability to complete the lab assignments in sections; individual parts of a lab activity could be completed by the student over time and in separate sections so the student could research any areas within the lab activity they did not know how to do.

Students also liked that while the first iteration of the lab assignment provided the necessary information (steps) to complete the lab, teaching the students as they successfully navigated the activity, the second iteration of the training provided the students with only an outline of the tasks to complete without any instructions at all. In this manner, students needed to apply critical thinking, problem-solving, analysis, and troubleshooting skills to complete the lab successfully. Overall, student and faculty feedback from the CYRIN platform has been promising with CYRIN having been received in a much more positive manner than both Practice Labs and the InfoSec Institute. However, there were some negative comments received during feedback. As the CYRIN platform is custom-built and presents curated lab assignments, there is limited faculty access to the server or platform on the backend of the platform. Additionally, there was only limited access to make changes to the scenarios presented and minimal ways for faculty to provide support for any tech issues (or related) student tech concerns since CYRIN labs are hosted on the CYRIN platform; hosted online (external) by a third-party vendor. Lastly, while there is a student cost to use the CYRIN platform for the

lab assignments, the per-student, per-use cost is much less than Practice Labs and the InfoSec Institute.

Compared with the other options (Practice Labs, InfoSec Institute, CYRIN), the BUTCA platform was regarded by students and faculty as the cyber platform (range) they preferred to use in this project for (1) ease of use; (2) learning the skills they need to know; and (3) the fun nature of the exercises while completing tasks. In BUTCA, the scenarios were curated based on custom input from students and faculty and could be created in a relatively short amount of time. Additionally, while the students were completing the scenarios individually, the scores are assessed in a CTF-style with leveling and time bonus enhancements so students, even though they are getting evaluated individually, competed with other students based on level and time overall to "win" the event. The BUTCA model was accepted as an exciting way to learn and develop the cyber skills they needed, while the other methods were seen more as a duty to complete a task they needed to do to get a grade only. However, this experience is based on short-term testing and further research will be required, particularly focusing on testing a wide range of cybersecurity scenarios.

Based on feedback from students and faculty, the BUTCA platform received the highest feedback. The ability to change scenarios based on need and preference allows the platform to be tailored to specifically challenge the students on new cyber threats as they become known. Moreover, the platform can be modified for industry use by practitioners for proprietary training and education for their staff, as well as personalized hands-on training for students getting close to graduation who will work for that company when they are done school. This allows the university to work directly with industry to identify new threats they are facing, and combined with updated skills students will need, to personalize training based on the changing cyber landscape ahead. Lastly, for educators, the BUTCA platform provides an option that allows easy student feedback and provides a simple mechanism for skills assessment and task completion without providing step-by-step instructions to students. Overall, both students and faculty benefitted from using the cyber range for advancing their cybersecurity education and training posture and will continue to use the platform in the future for skill proficiency and maintenance. To summarize this experience, we highlight the key points of lessons learned from testing different online learning platforms:

- Despite facilitating learning process, online platforms can pose technical issues, such as problems with connectivity, load balancing, and downloading learning assets.
- Little or no challenge of lab tasks reduces the overall quality of hands-on exercise.
- The CTF-style scenarios offer an interactive and gamified experience that can positively enhance the learning experience.

3.1.5 Summary of Lessons Learned in Higher Education

The lessons learned from the integration of cybersecurity education in higher education reveal both advantages and challenges across various approaches. Offering practical exercises and hands-on training is important for increasing students' knowledge and experience in cybersecurity domains. However, there are technical and quality related issues to consider. For example, if online platforms are used for training, they can pose issues, such as problems with connectivity, load balancing, or downloading learning assets. On the other

hand, local virtualization can bring challenges related to the maintenance of VMs and the need to handle potential technical issues.

The quality of cybersecurity training requires an appropriate level of challenge in lab tasks to facilitate learning. For this, the ability to create custom scenarios is important. A centralized learning platform and management can improve quality, as automated deployment, recovery, and destruction of sandbox environments reduce the technical demands associated with the preparation of lab lessons. Additionally, it is also important that the training is not demanding on the student's hardware.

From a teaching perspective, CR platforms facilitate the preparation and supervision of hands-on cybersecurity training, allowing lecturers to provide more individual attention to students. CR platforms can host CTF-style scenarios, which offer an interactive and gamified experience that can positively enhance learning. In CTF scenarios, students have the opportunity to test their cybersecurity skills and compete against others. On the other hand, CR scenarios can also be used in a non-competitive manner to support cybersecurity learning and student self-efficacy, where the teacher can guide students who face difficulties with the tasks, ensuring both learning and a sense of achievement. Thus, by considering students' needs and flexibly using CR scenarios, it is possible to support students who require encouragement in trying new tools.

3.2 Secondary Education

Cybersecurity education can also be encountered at the secondary level of education, especially in technical secondary schools in ICT fields of study. Although we have had experience in teaching cybersecurity in higher education as described in the sections above, we still found the process challenging. Introducing the cyber range application to secondary school students for hands-on training was difficult, especially because of the younger age group and different technical background of the students. To safely validate the concept of cyber range at the secondary level of education, we performed the following steps:

1. Created a less difficult gamified training scenario and organized pilot testing with a smaller group of 12 sary school students.
2. Obtained feedback by adjusting the scenario based on students' experience and testing it a second time with more students (40).
3. Prepared additional training scenarios and iteratively tested them during practical lessons in secondary schools with more than 100 students.

Table 1 Testing cybersecurity scenarios with secondary school students

Scenario	Students	Time limit (min)	Duration (avg.) (min)	Points (avg.)
Cybersecurity fundamentals	96	90	69.48	91.12
Offensive security	43	90	68.59	76.11
Cyber range tutorial	11	60	40.77	79.42
Hash functions	75	90	74.19	87.33
Smart metering	32	120	76.12	83.93
Windows firewall	16	90	85.60	72.66
Denial of service (DoS)	14	120	98.75	92.50

4. Started the full integration of the BUTCA platform into cybersecurity education in technical secondary schools.

Our experience at secondary education is currently built primarily on extensive testing with secondary school students and full integration of the BUTCA cyber range platform into the Secondary Technical School in Třebíč, Czechia. For an overview, we list all scenarios tested with secondary school students in Table 1, where the time limit for most scenarios was set to 90 min, which corresponds to the duration of practical lessons. Despite using hints, the students scored on average above 70 out of 100 points. More detailed student feedback is provided in Sect. 4.4.

Based on our experimental testing with secondary school students, we find two distinct approaches to applying cyber range to secondary education. The first is the direct deployment of the cyber range into study programs at technical schools that include cybersecurity courses in their curricula, and thus the cyber range can significantly support students' practical skills. The second case is that of non-technical schools where cyber range is more essential for cybersecurity awareness through one-time or multiannual opportunities to undertake interactive awareness training.

As we addressed in Sect. 2, operating a cyber range can be expensive and requires technical staff in addition to extensive infrastructure, which may make it impossible to deploy a cyber range to schools or universities if they do not have these resources. We have eliminated this problem by using the BUTCA platform, as all processes are automated and the sandbox environment for teaching and training is deployed and managed in the BUTCA cloud. There are minimum technical prerequisites for schools or universities and they can access the entire environment remotely from their classrooms.

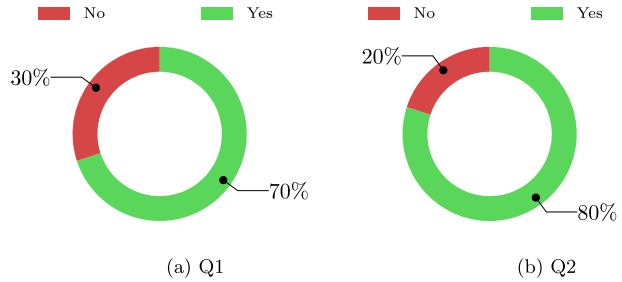
3.3 Primary Education

For the application of the cyber range at the primary level of education, we had to choose a completely different approach than for the secondary schools, mainly because of students' limited understanding of ICT areas without much technical background that is needed for advanced training scenarios. As pointed out in Sect. 2, primary school students can be perceived as ordinary internet users. Therefore, we found it more useful and meaningful to educate them about cybersecurity basics than to train them on advanced topics such as penetration testing or malware analysis. For this reason, we decided to prepare an awareness scenario focused on the safe use of the internet.

Although the awareness scenario for primary school students did not deal with advanced topics, it was designed as a CTF on the cyber range platform, thus ensuring interactive and gamified learning as in previous cases. The scenario was divided into 8 practical tasks containing the following cybersecurity topics:

1. Risks associated with downloading software from unofficial sources.
2. Finding compromised passwords in open databases.
3. Leaks of sensitive data through HaveIBeenPwned.
4. Password security and how to create a strong password.
5. Fake social media profiles and how to recognize them.
6. How to verify the accuracy of information on the internet (fake news).

Fig. 3 Questions asked to primary school students after they completed the scenario: **a** Has your awareness of potential risks on the internet increased? **b** Will you be more careful when using the internet after completing the scenario?



7. Scams on online marketplaces (theft of a credit card).
8. Social engineering attacks and their impacts.

We tested the awareness scenario with 40 students from two primary schools in Brno, Czechia (Antonínská and Jana Babáka). The completion time limit was set to 1 hour and the students completed individual tasks independently. After completing the scenario, we asked the students whether their awareness of internet risks had increased after completing the scenario (Q1) and whether they would be more cautious when using the internet from now on (Q2). Their answers are shown in Fig. 3.

For question Q1, 70% of the responses were positive (their awareness has increased), and for Q2, 80% of the students responded that they will be more careful on the internet after competing the scenario. These results align with the literature discussed in Sect. 2.1.1, where interactive and gamified approaches have proven effective in raising awareness among children. The increase in awareness and caution levels demonstrates that cybersecurity education, even at the primary level, can enhance children's understanding of online risks.

Based on this experience, we found the cyber range useful for cybersecurity awareness but not suitable for hands-on training, especially considering the lower age group of primary school students and the lack of technical background in their studies. However, we do not perceive this limitation negatively, as primary education is inherently general and students only choose fields of study in the later stages of their studies before moving on to secondary school. A basic understanding of cybersecurity is important for all users and it is therefore desirable to educate users as early as possible.

4 Stakeholders' Perspective

This section details the perspectives of the two main user groups using the cyber range in the context of our application of the BUTCA platform in primary, secondary, and higher education. These groups include teachers and students, whose perspectives are shown in Fig. 4 and described in more detail in Sects. 4.1 and 4.2.

4.1 Teacher Perspective

As shown in Fig. 4, teachers in the cyber range first conduct a preparatory phase in which they create a scenario. This involves setting basic parameters such as time limit,

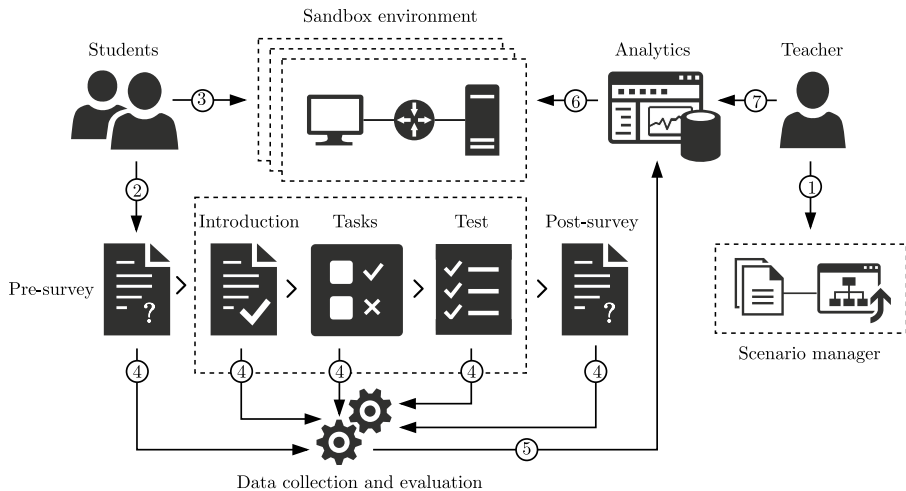


Fig. 4 The cyber range environment: (1) Teacher prepares a learning or training scenario in the scenario manager module and defines a sandbox environment; (2) Students complete a pre-survey before running the scenario, sequentially solve the scenario tasks, a test, and complete a post-survey (if present); (3) Students interact with the sandbox environment as needed while solving the scenario tasks; (4) Data collection and evaluation are performed during the whole process; (5) Collected and further processed data are stored in the database for analysis; (6) The sandbox environment and the scenario progress are monitored; (7) Teachers analyze the results during or after the scenario

prerequisites, and introduction. This is followed by the definition of scenario tasks including assignment, difficulty, topics, points, hints, and attachments. Then a test is defined that is related to the tasks and verifies the student's acquired knowledge upon completion. If the scenario requires devices with which students work, the teacher defines a sandbox topology including one or more virtual machines that will be available to the students (i.e., client, server, or network devices). Optionally, teachers can then assign pre- and post-surveys to the scenario for further analysis.

During the active learning process, teachers can monitor student progress through the analytics module. This includes tracking which task they are currently on, their current score, hints used, user input logs, and activity performed in the sandbox. Once the scenario is complete, teachers have access to individual student scores, pre- and post-surveys, and statistical reports for further analysis, which can be followed by scenario modification.

4.2 Student Perspective

Most of the possibilities in the cyber range, presented within our application of the BUTCA platform, are related to activities performed in a learning or training scenario. After running the scenario, students read the introduction and then sequentially perform the tasks. Each task contains an assignment whose solution leads to the correct answer. Since we used the CTF concept, the correct answer is a flag that the user must obtain by solving the challenge in the given task. If needed, students are also provided with hints; the use of which is penalized by a certain loss of points, with the last hint revealing the solution.

Most cyber range scenarios also allow students to use a sandbox environment, especially for solving practical challenges. In this case, each student is assigned a sandbox that is isolated from the others. A sandbox consists of one or more virtual machines, which are further divided into client, server, and network devices. In a typical scenario, a sandbox consists of two devices communicating in client–server mode, with the client device being accessed by the student (e.g., Kali Linux, Ubuntu, Windows OS, etc.).

After the last task of the scenario is completed or the time limit expires, students are given a test to verify their knowledge. The test questions are directly related to scenario tasks in the form of single correct, multiple correct, or open-ended answers. When the entire scenario is completed, the student receives an evaluation consisting of a score for solving the tasks, a penalization for the hints used, the results of a test, a scorecard comparing the student to others, and an overall summary of the scenario.

4.3 Survey

To determine the importance, need, usefulness, and perceptions of the opportunities that the cyber range offers, we conducted a survey asking teachers and students a set of questions divided into 4 groups:

1. The usefulness of the cyber range for various forms of education and the helpfulness of the platform in dealing with the technical aspects of the preparation and implementation of teaching.
2. Perceptions of the positive impact of gamification and interactivity on learning in a cyber range platform.
3. The importance of the user interface, cyber range scenarios, the analytics module, and the use of real industrial devices versus virtual ones.
4. What cybersecurity topics do teachers and students think are the most needed?

We collected responses from the Brno University of Technology, Tampere University, Pennsylvania State University, University of Defence, University of Hradec Králové, Secondary Technical School in Třebíč, and Grammar School Brno. We had separate surveys for teachers and students and the invitations were sent to teachers and students who had participated in CTFs. Surveys had Likert-5 type questions and also open responses, where we asked responders to give reasons for their ratings.

The survey results were analyzed by calculating means and standard deviations for the Likert-type questions. We also calculated percentages of Likert-responses. Open responses were grouped based on response on Likert-scale, e.g. whether the responder had agreed or disagreed, and then further grouped based on similarity and themes presented in open responses. By this, we investigated for example reasons for agreement or disagreement for penalizing hint usage in CTF scenarios. In the end of the survey, we also asked responders to select the most important cybersecurity topics based on their opinion. We received responses from 19 teachers, 70 university students, and 40 sary school students.

Tables 2 and 3 present the respondents' background. The visual presentation is in Appendix A and B. The most represented age groups of teachers were 36–45 (42.1%) and 26–35 (36.8%), while the students were 19–25 (77%), 15–18 (23.6%), and above 26 (6.4%). The teachers' backgrounds in their previous studies were mostly in cybersecurity (47.4%) and computer science (36.8%). Similarly, the majority of respondents from the

Table 2 University and secondary school students' background

Group	1	2	3	4	5	6	7
<i>N</i>	35	7	17	10	1	39	1
<i>Age</i>							
15–18	1	0	0	0	0	24	1
19–25	33	5	15	9	0	15	0
Above 26	1	2	2	1	1	0	0
<i>Focus of studies</i>							
Cybersecurity	26	2	16	10	0	0	0
Computer science (IT)	8	3	1	0	0	33	1
Other	1	2	0	0	1	4	0
<i>Cybersecurity is studied as</i>							
A main topic	23	3	15	10	0	3	0
A secondary topic	3	1	2	0	1	29	0
As individual courses or part of other courses	8	3	0	0	0	7	0
Not at all	1	0	0	0	0	0	1

Groups:

1—Brno University of Technology

2—Tampere University

3—Pennsylvania State University

4—University of Defence

5—University of Hradec Králové

6—Secondary Technical School in Třebíč

7—Grammar School Brno

second group were students of cybersecurity (50.9%) or computer science (30.9%). We further present and discuss the survey results in Sect. 4.4.

4.4 Results and Discussion

Based on the responses and the group of respondents, we grouped and divided the responses into two tables. The responses of the analyzed teachers survey are presented in Table 4, while the students' responses are presented in Table 5. In addition, we provide a detailed commentary in which we interpret the results presented. The mean (M) and standard deviation (SD) were calculated from all responses of a given question from the tables below.

Both students and teachers think the cyber range is useful for training or teaching cybersecurity. The mean was 4.39 ($SD = 0.778$) for university students, 4.25 ($SD = 0.742$) for secondary school students, and 4.89 ($SD = 0.315$) for teachers and instructors. Students have more variation in their answers; for example 50% of university students and 37.5% of secondary school students strongly agree, but for teachers the percentage is 89.5. The participants also see cyber range as useful for cybersecurity awareness, the mean was 4.16 ($SD = 0.857$) for university students, 4.20 ($SD = 0.816$) for secondary school students, and 4.27 ($SD = 0.562$) for teachers and instructors. Further, students and teachers see cyber range useful for competitions, the mean was 4.34 ($SD = 0.857$) for university students,

Table 3 Teachers' background

	University ^a	Secondary school	Grammar school
<i>N</i>	17	1	1
<i>Age</i>			
21–25	1	0	0
26–35	6	1	0
36–45	7	0	1
46–55	2	0	0
Above 55	1	0	0
<i>Focus of previous studies</i>			
Cybersecurity	9	0	0
Computer science (IT)	6	1	0
Education/teaching	1	0	1
Other	1	0	0
<i>Cybersecurity courses in your organization</i>			
Mandatory study subjects	16	1	1
Security seminars	10	1	0
Free time courses	6	0	0
Cybersecurity competitions	8	1	0
None	1	0	0

^a Number of responders in universities: Brno University of Technology 8; Tampere University 3; University of Defence 2; University of Hradec Králové 4

3.92 ($SD = 0.722$) for secondary school students, and 4.67 ($SD = 0.594$) for teachers and instructors.

From the students' point of view, they agree that the cyber range helps them through practical tasks better than conventional approach, the mean was 4.37 ($SD = 0.982$) for university students, and 4.18 ($SD = 0.747$) for secondary school students. Feedback from cyber range scenarios is also important for students, as 77% of university students and 63% of secondary school students see it important or very important. Further, 66% of university students consider that using real industrial devices for cybersecurity education is important or very important. For secondary school students, the percentage is lower (38%).

From the teachers' point of view, they consider that the cyber range helps them to pay more attention to individual students during lessons than the conventional approach. The mean was 4.53 ($SD = 0.612$). Teachers also agree that cyber range solves technical challenges, makes scenario creation process faster, and that sandboxing is more essential than maintaining virtual machines in the lab. Further, teachers mostly consider the analytical functions of cyber range important or very important, and 57.9% of teachers consider using real industrial devices for cybersecurity education and training important or very important.

Considering the learning process, we asked the respondents' opinions about whether gamification in the cyber range positively affects the learning process (1 very unlikely to 5 very likely). The mean was 4.39 ($SD = 0.778$) for university students, 4.25 ($SD = 0.742$)

Table 4 Teachers survey results

Question	<i>M</i>	<i>SD</i>
The cyber range is useful for teaching/training cybersecurity. ¹	4.89	0.315
The cyber range is useful for cybersecurity awareness. ¹	4.74	0.562
The cyber range is useful for cybersecurity competitions. ¹	4.67	0.594
The cyber range helps teachers/instructors to give more individual attention to students during lessons than the conventional approach (PDF instructions, VMs on lab devices,...). ¹	4.53	0.612
The cyber range solves the technical challenges of running lab exercises for teacher/instructor. ¹	4.39	0.698
Creating training scenarios in a cyber range platform is faster than manually (preparing VMs and instructions on your own device). ¹	4.22	0.878
The sandboxing in the cyber range is more essential to teacher/instructor than deploying and maintaining virtual machines on computers in the lab. ¹	4.24	0.831
The gamification in the cyber range affects the learning process positively. ²	4.79	0.419
The interactivity in the cyber range affects the learning process positively. ²	4.68	0.478
How important is the design of the cyber range user interface to you? ⁴	3.95	0.705
How important do you see analytical functions in the cyber range? ⁴	4.37	0.895
How important is it to use real industrial devices instead of their full virtual versions for cybersecurity education and training? ⁴	4.00	0.943

Possible answers:

¹ (1) strongly disagree to (5) strongly agree

² (1) very unlikely to (5) very likely

³ (1) very unhelpful to (5) very helpful

⁴ (1) very unimportant to (5) very important

for secondary school students, and 4.79 ($SD = 0.419$) for teachers and instructors. University and secondary school students who think gamification in cyber range affects the learning process positively very likely or likely mention the reason being fun or enjoyment. In addition, university students mentioned more reasons, such as getting help in understanding and getting hands-on experience of tools. For teachers, the main reasons mentioned are mostly the improvement of student engagement and motivation.

We also asked whether interactivity in the cyber range affects the learning process positively. The mean was 4.43 ($SD = 0.791$) for university students, 4.15 ($SD = 0.700$) for secondary school students, and 4.68 ($SD = 0.478$) for teachers and instructors. Students who think interactivity in cyber range affects the learning process positively very likely or likely mention reasons that learning by doing is effective and interactivity allows usage of the real tools in real-like situations. University students also mention that interactivity complements passive learning, such as watching tutorial videos or reading study materials. For teachers, the main reasons most often mentioned are that interactivity helps students acquire cybersecurity and problem-solving skills and allows active learning.

Thus, although both students and teachers see gamification of the cyber range as likely to positively affect the learning process, the reasons are a bit different. Students consider the fun aspect important for learning, but teachers focus more on engagement and motivation. When designing scenarios for the cyber range, teachers should remember that if the student considers the scenario fun, it may also promote other learning goals. Regarding interactivity, both students and teachers appreciate that the cyber range offers a place

Table 5 University and secondary school students survey results

Question	University		Secondary	
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
The cyber range is useful for teaching or training cybersecurity. ¹	4.39	0.778	4.25	0.742
The cyber range is useful for cybersecurity awareness. ¹	4.16	0.857	4.27	0.816
The cyber range is useful for cybersecurity competitions. ¹	4.34	0.857	3.92	0.722
The cyber range helps students to navigate through practical tasks better than the conventional approach (PDF instructions, less interactive labs,...). ¹	4.37	0.982	4.18	0.747
The gamification in the cyber range affects the learning process positively. ²	4.34	0.778	4.08	0.797
The interactivity in the cyber range affects the learning process positively. ²	4.43	0.791	4.15	0.700
How do you perceive the task hints in the CR platform? ³	4.03	0.884	3.70	0.687
Do you agree with the scoring of tasks in the CR platform? ¹	3.81	0.967	3.97	0.891
Do you agree with penalisation of using hints in the CR platform? ¹	3.74	1.176	3.80	1.114
How important is the design of the cyber range user interface to you? ⁴	3.71	0.919	3.80	0.823
How important is the feedback from the cyber range scenarios to you? ⁴	4.03	0.851	3.60	1.008
How important is it to use real industrial devices instead of their full virtual versions for cybersecurity education and training? ⁴	3.89	0.986	3.18	0.844

Possible answers:

¹ (1) strongly disagree to (5) strongly agree

² (1) very unlikely to (5) very likely

³ (1) very unhelpful to (5) very helpful

⁴ (1) very unimportant to (5) very important

for practical skills acquisition, which is very important in cybersecurity. Students see that “learning by doing“ helps understanding the theoretical concepts, realizing their meaning in the real world, and also helps memorizing them.

We also asked students’ opinions about the usefulness of task hints (1 very unhelpful to 5 very helpful), and do they agree on the scoring of tasks and penalizing using task hints (1 strongly disagree to 5 strongly agree). The mean of task hint helpfulness was 4.03 ($SD = 0.884$) for university students, and 3.70 ($SD = 0.687$) for secondary school students. Thus, secondary school students experienced hints slightly less helpful than university students. In open responses, students mention that hints can be helpful, prevent them from getting stuck for a long time, avoid frustration, and can enhance learning. However, there were also neutral opinions mentioning that hints can be confusing, and students want to solve the task on their own and not rely on hints. It is also worth pointing out that while hints were reported as “helpful“ for secondary school students, their technical skills and knowledge may differ from university students that did not need as much, or as many, hints.

Agreeing on scoring of the tasks and penalization of using hints also aroused neutral and negative opinions. The mean for agreeing on the scoring of the tasks was 3.81 ($SD = 0.967$) for university students, and 3.97 ($SD = 0.891$) for secondary school students. Students who agreed felt that the scoring was fair and that it is appropriate to reward students who perform better than others. However, while students with neutral opinions mentioned the negative impact of scoring penalties from using hints, the students recognized they are in a learning situation and do not yet know everything. The same reason was also visible

in agreeing on the penalization of using hints. The mean of the responses was 3.74 ($SD = 1.176$) for university students, and 3.80 ($SD = 1.114$) for secondary school students. University students who agreed felt that the penalty was fair and made students try the task harder before giving hints. However, students with neutral or negative opinions mentioned that points should not be lost because they need help in learning situations, and penalization can be demotivating.

Based on these results, scoring, hints, and penalization for using hints have positive and negative aspects, and different students can experience them in different ways. On the other hand, scoring promotes competition, which according to the results, students see as positive. However, there are also students who find it stressful and stress situations do not necessarily improve learning in the best ways. Regarding task hints penalization, students see it fair and necessary, as it promotes trying and prevents rushing through scenario just by taking hints. Furthermore, students see that they are in a learning situation and it may be demotivating to get a penalty for needing help while trying to learn. In open responses, students also presented ideas for solving this problem; for example, it was proposed that the first hints could be without penalty, so the student who does not know how to begin would get a push to the right direction. Scoring and hint usage penalization are issues that teachers must consider against learning goals while using cyber range scenarios. For example, the course could contain competitive (test-like) scenarios where scores are measured. However, scenarios can also be used without competition just to practice skills. The teacher can also encourage students to ask for help before using the hints.

At the end of the survey, we asked students and teachers to select the most important cybersecurity topics based on their opinion. Network security and penetration testing are the most prevalent for all groups. There was a larger disparity for operational technology (OT) security, which teachers consider to be more important, while less important by students, however, university students consider it more needed than secondary school students. The opposite proportion can be seen for malware analysis, where students perceived the importance of this topic more than teachers. It is also interesting that university students seem to consider digital forensics more needed than teachers and secondary school students. On the other hand, secondary school students consider cryptography to be more needed than university students and teachers, but incident response is less needed than other groups. The resulting percentage ratios are shown in Fig. 5.

We also asked if teachers had any concerns or problems using the cyber range in teaching. About half of the teachers (9/19) mentioned some concerns, such as the possibility of student misconceptions or differences in students' skills, scenario to real-world correspondence, ethical issues when teaching offensive techniques, and administrative and maintenance issues related to cyber range. Finally, we summarize the main findings from the teacher and student surveys:

1. Students and teachers see gamification of the cyber range likely affecting the learning process positively:
 - Students consider the fun aspect important for learning.
 - Teachers focus more on student engagement and motivation.
2. Interactivity is valued by teachers and students:
 - The cyber range platform is a place for the acquisition of practical skills.

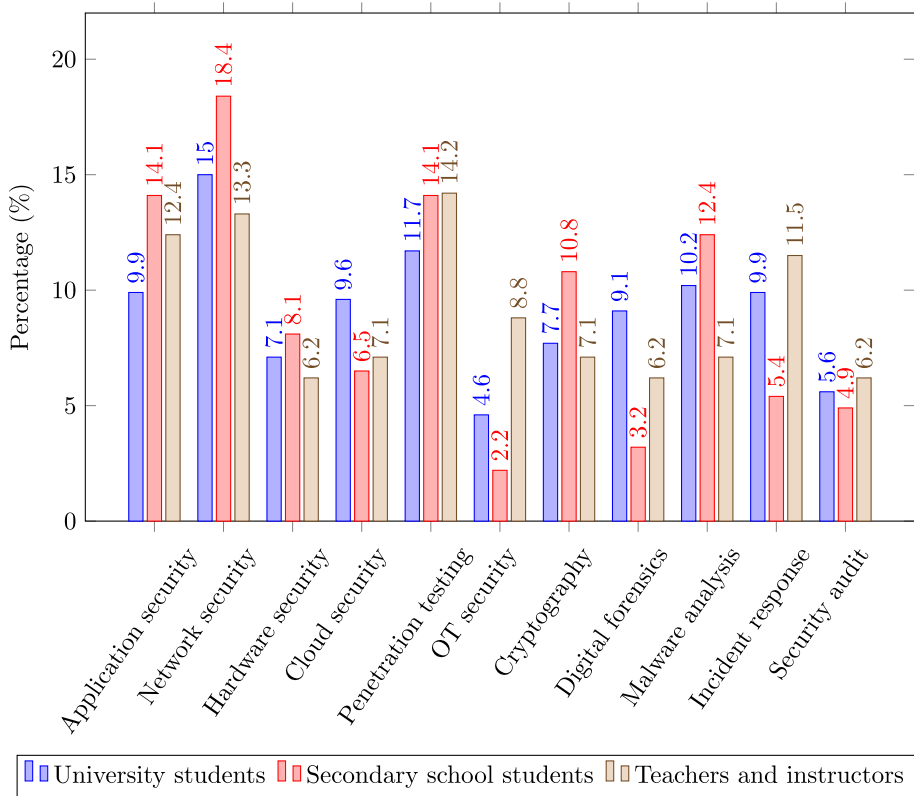


Fig. 5 What cybersecurity topics do you see as most needed?

- For students, learning by doing helps understanding the theoretical concepts, realizing their meaning in the real world, and also helps memorizing them.
3. Scoring promotes competition, which students see as positive, but there are also students who find competition stressful:
 - Competitions can motivate students to solve tasks thoroughly.
 - Being actively compared to others can be stressful for some students.
 4. The penalization of task hints has positive and negative aspects:
 - The presence of penalized hints can support task solving efforts.
 - It can be demotivating to get a penalty for needing help while trying to learn.

4.4.1 Survey Limitations

Despite collecting survey data from three countries, the geographical diversity of the survey is limited. In the student survey, majority of the university student respondents were from Czech universities (66%). Only 24% of the respondents were from the United States and 10% from Finland. Another geographical limitation is that the secondary school data

was only available from Czech secondary schools. More data from other countries would have allowed more detailed analysis.

The limitations in geographical diversity impacted the students survey analysis. In this study, we presented several approaches (see Sect. 3) from different universities and countries. The approaches had variation in how the CTF sessions were applied, and it is possible that this has an effect on students' responses. Thus, it would have been interesting to analyse responses also based on approaches. However, due to relatively low respondent numbers in some approaches, we could not perform that detailed analysis. Instead, we have analysed the university student survey responses as one group.

In the teachers survey, 89% were university teachers and 82% were from Czech universities. Thus, the responses mostly present university teacher opinions. More data from the secondary school teachers should be collected, if the scenarios are utilized in cybersecurity teaching in secondary schools. Due to lack of secondary school teacher participants, we were not able to analyse the possible differences between university and secondary school teachers' perspectives from this data, though that would be valuable knowledge for further development of cyber arena and scenarios to better respond also to secondary school educational needs.

4.4.2 Recommendations

Based on our interpretation of the results of both surveys and our experience, we present the following recommendations for the use of cyber range in teaching cybersecurity:

- Adjust the parameters and content of the CR platform as needed to meet the requirements of cybersecurity awareness, education, and training program.
- Consider evaluating scoring and hints against the learning goals. For example, the cyber range platform can be used to test students' knowledge and ability to apply theoretical concepts in practice in a test-like manner or to complement other teaching methods without a primary focus on student scores.
- Based on data and feedback from learning, determine how best to support students who have difficulties with the scenario to ensure learning and feelings of achievement.
- Remember the importance of the game aspect and student engagement, as it can also promote other learning goals. This can be achieved by designing CTF-based scenarios for interactive and gamified learning.

The deployment and operation of CR platforms impose high technical requirements and thus higher financial costs. Based on our results and experience, we provide recommendations for utilizing the cyber range in non-technical educational settings and for underfunded institutions:

- Building a cyber range: To create and manage CTF scenarios, use an open source solution that can be self-hosted on a single device (e.g., CTFd). For virtualization, use computers in the lab classrooms or clients' own devices.
- Cyber range as a service: Use a cloud-based CR platform that offers individual user access in a free version (e.g., TryHackMe, Hack The Box, etc.) or non-commercial licenses for educational institutions.

Overall, CR platforms offer a wide range of applications, and the needs may vary depending on the type of the organization and its requirements. While our approach is primarily focused on the educational environment, it can be adapted to other sectors with similar requirements, such as government, industry, or the military.

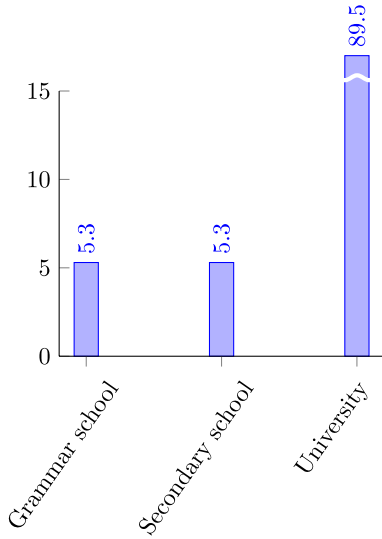
5 Conclusion

In this paper, we have presented various applications of cyber range for teaching and training cybersecurity at different levels of education. In higher and secondary technical education, we find a significant benefit in using the cyber range for hands-on training. In addition, for non-technical fields of study and primary schools, cybersecurity awareness is more suitable. We further discussed the potential for using a cyber range platform for cybersecurity education based on the perspectives of teachers and students. This is supported by the survey conducted with a total of 129 respondents. Based on the analyzed survey responses and feedback from students and teachers, we verified and substantiated the positive impact of gamification and interactivity on cybersecurity education, as well as the overall usefulness of cyber ranges for learning, training, awareness and competitions in cybersecurity.

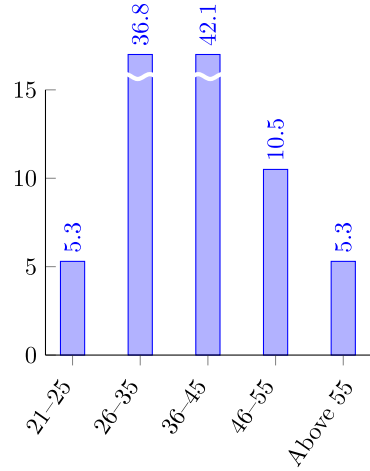
Although our survey included 129 respondents, it had its limits. The majority of students were from Czech universities, which reduced diversity in terms of geography and educational level. In the future, we plan to expand our approach with pre- and post-surveys to explore the impact of cyber range on cybersecurity education in hands-on training with secondary school and university students while increasing the number of respondents from other countries. This could better compare findings based on different backgrounds and identify other factors that affect this type of training.

Background of Teacher Respondents

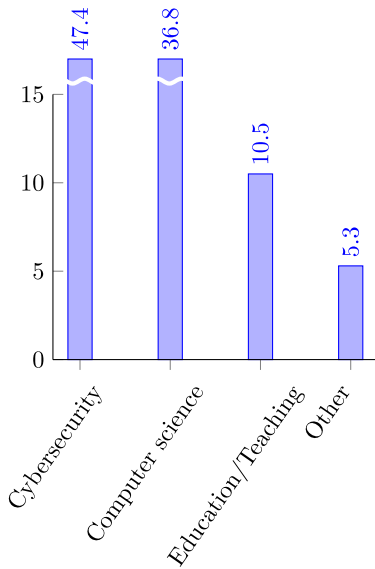
See Fig. 6.



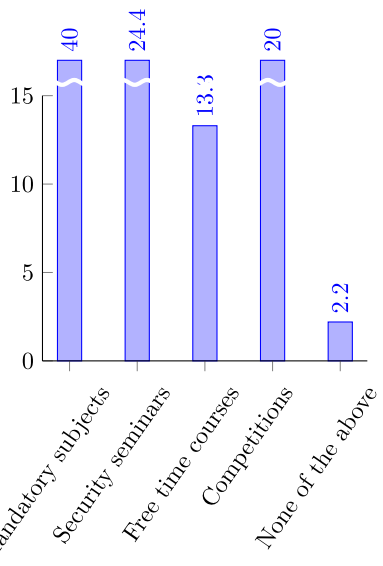
(a) What is the type of your organization



(b) What is your age?



(c) What was the focus of your previous studies?

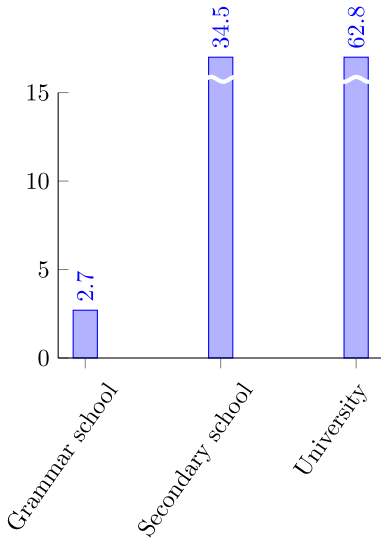


(d) What cybersecurity courses are available in your organization?

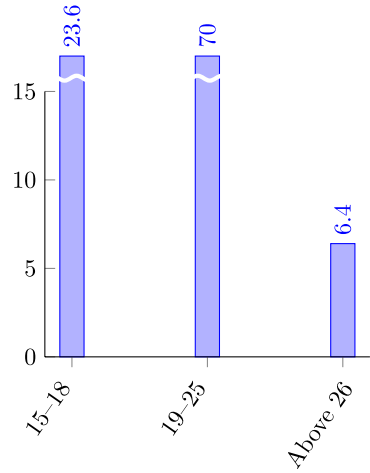
Fig. 6 Survey responses—teachers background

Background of Student Respondents

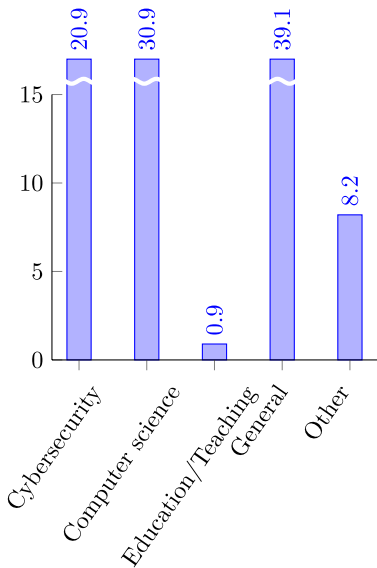
See Fig. 7.



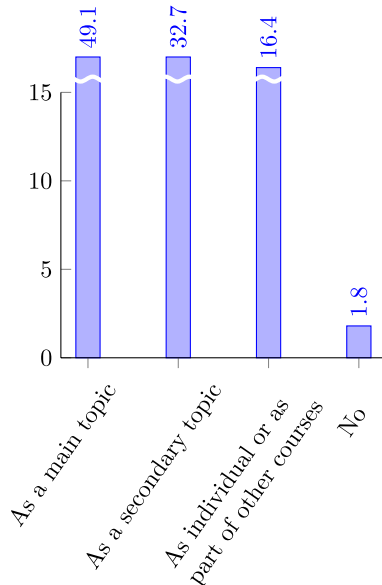
(a) What is the type of your organization?



(b) What is your age group?



(c) What is the focus of your current studies?



(d) Does your studies include cybersecurity?

Fig. 7 Survey responses—students background

Acknowledgements The authors thank the teachers and students who participated in the study.

Funding This publication was supported by the project “The Energy Conversion and Storage”, funded as project No.CZ.02.01.01/00/22 008/0004617 by Programme Johannes Amos Comenius, call Excellent Research.

Data Availability Statement Due to privacy and ethical concerns, the data are not made available in a public repository. Access can be requested through the authors.

Declarations

Conflict of interest The authors declare no conflict of interest regarding the publication of this paper.

Consent to participant This study received informed consent from all participants.

Consent for publication The author accepts responsibility for releasing this material to be published.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abu-Amara, F., Hosani, R. A., Tamimi, H. A., & Hamdi, B. A. (2024). Spreading cybersecurity awareness via gamification: Zero-day game. *International Journal of Information Technology*, 16(5), 2945–2953. <https://doi.org/10.1007/s41870-024-01810-4>
- ACI Learning (n.d.). *Practice Labs | Hands-on Learning for Digital & IT Skills*. <https://www.acilearning.com/products/practice-labs/>. Accessed on April 5, 2024
- Ahmad, A., Maynard, S. B., Motahhir, S., & Anderson, A. (2021). Case-based learning in the management practice of information security: An innovative pedagogical instrument. *Personal and Ubiquitous Computing*, 25(5), 853–87. <https://doi.org/10.1007/s00779-021-01561-0>
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>
- Architecture Technology Corporation (n.d.). *CYRIN*. <https://cyrin.atcorp.com/>. Accessed on April 5, 2024
- Beltran, M., Calvo, M., & Gonzalez, S. (2018). Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs. In *2018 International conference on computational science and computational intelligence (CSCI)* (pp. 574–579). IEEE.
- Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., & Olayinka, O. (2022). Can gamification help to teach cybersecurity? In *2022 20th International conference on information technology based higher education and training (ITHET)* (pp. 1–9).
- Bin Ibrahim, A. D., Ashrofi Hanafi, A. H., Rokman, H., Ahmad Zawawi, M. N., Ibrahim, Z.-A., & Rahim, F. A. (2020). Comparative analysis on student’s interest in cyber security among secondary school students using CTF platform. In *2020 8th International conference on information technology and multimedia (ICIMU)* (pp. 73–77). IEEE.
- Bioglio, L., Capecechi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2019). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies*, 12(4), 456–469. <https://doi.org/10.1109/TLT.2018.2881193>
- Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, 67, 101769. <https://doi.org/10.1016/j.techsoc.2021.101769>
- Boom-Cárcamo, E., Buelvas-Gutiérrez, L., Acosta-Oñate, L., & Boom-Cárcamo, D. (2024). Gamification and problem-based learning (PBL): Development of creativity in the teaching-learning process

- of mathematics in university students. *Thinking Skills and Creativity*, 53, 101614. <https://doi.org/10.1016/j.tsc.2024.101614>
- Brno University of Technology (n.d.). *BUTCA – CYBER ARENA*. <https://butca.vut.cz/en/> (Accessed on March 27, 2024)
- Broadcom (n.d.). *Vmware - delivering a digital foundation for businesses*. <https://www.vmware.com/>. Accessed on March 27, 2024
- Bulgurcu, C. B. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523. <https://doi.org/10.2307/25750690>
- Carnegie Mellon University (n.d.). Picoctf-cmu cybersecurity competition. <https://picoctf.org/>. Accessed on April 20, 2024
- Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1), tyz001. <https://doi.org/10.1093/cybsec/tyz001>
- Chothia, T., Novakovic, C., Radu, A.-I., & Thomas, R. J. (2019). Choose your Pwn adventure: Adding competition and storytelling to an introductory cybersecurity course. In *Transactions on edutainment XV* (Vol. 11345, pp. 141–172). Springer.
- Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*. <https://doi.org/10.3390/app11041809>
- Cloud Native Computing Foundation (n.d.). *Production-grade container orchestration*. <https://kubernetes.io/>. Accessed on March 27, 2024
- Cole, S. V. (2022). Impact of capture the flag (CTF)-style vs. traditional exercises in an introductory computer security class. In *Proceedings of the 27th ACM conference on on innovation and technology in computer science education* (Vol. 1, pp. 470–476). ACM.
- CTFd LLC (n.d.). *Ctfd : The easiest capture the flag platform*. <https://ctfd.io/>. Accessed on March 27, 2024
- CyberChallenge.IT (n.d.). *Training the New Generation of Cyberdefenders*. <https://cyberchallenge.it/en>. Accessed on October 14, 2024
- Cybersecurity in Application, Research, and Education (CARE) Lab (n.d.). *Social Engineering Competition*. <https://sites.temple.edu/socialengineering/>. Accessed on October 14, 2024
- De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7. <https://doi.org/10.1016/j.giq.2017.02.007>. (Open Innovation in the Public Sector).
- Deng, Y., Zeng, Z., Jha, K., & Huang, D. (2022). Problem-based cybersecurity lab with knowledge graph as guidance. *Journal of Artificial Intelligence and Technology*. <https://doi.org/10.37965/jait.2022.0066>
- ENISA (n.d.). *CYBERHEAD-cybersecurity higher education database*. <https://tools.enisa.europa.eu/topics/education/cyberhead/>. Accessed on October 14, 2024
- European Cybersecurity Challenge (n.d.). *The european cybersecurity challenge*. <https://ecsc.eu/>. Accessed on October 14, 2024
- Hack The Box (n.d.). *Level up your hacking skills*. <https://www.hackthebox.com/hacker/hacking-labs>. Accessed on April 20, 2024
- Hadlington, L., & Murphy, K. (2018). Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. *Cyberpsychology, Behavior, and Social Networking*, 21(3), 168–172. <https://doi.org/10.1089/cyber.2017.0524>
- HashiCorp (n.d.). *Automate infrastructure on any cloud with terraform*. <https://www.terraform.io/>. Accessed on March 27, 2024
- He, W., Kshirsagar, A., Nwala, A., & Li, Y. (2014). Teaching information security with workflow technology—A case study approach. *Journal of Information Systems Education*, 25(3), 201–210.
- Infosec (n.d.). *Cybersecurity training and certifications*. <https://www.infosecinstitute.com/>. Accessed on April 5, 2024
- Karagiannis, S., & Magkos, E. (2021). Adapting CTF challenges into virtual cybersecurity learning environments. *ICS*, 29(1), 105–132. <https://doi.org/10.1108/ICS-04-2019-0050>
- Katsantonis, M. N., & Mavridis, I. (2021). Evaluation of HackLearn COFELET game user experience for cybersecurity education. *International Journal of Serious Games*, 8(3), 3–24. <https://doi.org/10.17083/ijsg.v8i3.437>
- Katsantonis, M. N., Manikas, A., Mavridis, I., & Dimitrios, G. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, 22(4), 1005–1027. <https://doi.org/10.1007/s10207-023-00680-4>

- Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). "Shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1), 29–37. <https://doi.org/10.1145/2738210.2738216>
- Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management and Computer Security*, 18(5), 316–327. <https://doi.org/10.1108/09685221011095236>
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, 25(4), 29–289. <https://doi.org/10.1016/j.cose.2006.02.008>
- Kumar, P., Vitak, J., Chetty, M., Clegg, T. L., Yang, J., McNally, B., & Bonsignore, E. (2018). Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children* (pp. 67–79). ACM.
- Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, 23(2), 361–373. <https://doi.org/10.1007/s10796-019-09977-z>
- Lateş, I., & Boja, C. (2023). Cyber range technology stack review. In *Education, research and business technologies* (pp. 25–40). Springer.
- Lazarov, W., Stodulka, T., Schafteitl-Tähtinen, T., Helenius, M., & Martinasek, Z. (2023). Interactive environment for effective cybersecurity teaching and learning. In *Proceedings of the 18th international conference on availability, reliability and security*. Association for Computing Machinery.
- Leune, K., & Petrilli, S.J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 47–52). Rochester New York USA: ACM.
- LF CHARITIES (n.d.). *Jenkins*. <https://www.jenkins.io/>. Accessed on March 27, 2024
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Malone, M., Wang, Y., James, K., Anderegg, M., Werner, J., & Monrose, F. (2021). To gamify or not?: On leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention. *Proceedings of the 52nd ACM technical symposium on computer science education* (pp. 1135–1141). ACM.
- Matovu, R., Nwokeji, J. C., Holmes, T., & Rahman, T. (2022). Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. In *2022 IEEE frontiers in education conference (FIE)* (pp. 1-9).
- McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. In *2016 49th Hawaii international conference on system sciences (HICSS)* (pp. 5479–5486).
- Mouheeb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. In Z. Pan, A. D. Cheok, W. Müller, M. Zhang, A. El Rhalibi, & K. Kifayat (Eds.), *Transactions on edutainment XV* (pp. 93–107). Springer.
- Mountrouidou, X., Vosen, D., Kari, C., Azhar, M.Q., Bhatia, S., Gagne, G. & Yuen, T. T. (2019). Securing the human: A review of literature on broadening diversity in cybersecurity education. In *Proceedings of the working group reports on innovation and technology in computer science education* (pp. 157–176). Association for Computing Machinery.
- Oracle (n.d.). *Oracle vm virtualbox*. <https://www.virtualbox.org/>. Accessed on March 27, 2024
- Park, M., Lee, H., Kim, Y., Kim, K., & Shin, D. (2022). Design and implementation of multi-cyber range for cyber training and testing. *Applied Sciences*. <https://doi.org/10.3390/app122412546>
- Peker, Y., Ray, L., & Da Silva, S. (2018). Online cybersecurity awareness modules for college and high school students. In *2018 national cyber summit (NCS)* (pp. 24–33). IEEE.
- Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., & Bonders, M. (2024). *Try to esCAPE from cybersecurity incidents! A technology-enhanced educational approach: technology, knowledge and learning*. <https://doi.org/10.1007/s10758-024-09769-8>
- Plass, J. L., Homer, B. D., Mayer, R. E., & Kinzer, C. K. (n.d.). 1 Theoretical foundations of game-based and playful learning. In Plass, J. L., Mayer, R. E., & Homer, B. D. (Eds.), *Handbook of game-based learning*.
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- Qusa, H., & Tarazi, J. (2021). Cyber-hero: A gamification framework for cyber security awareness for high schools students. In *2021 IEEE 11th annual computing and communication workshop and conference (CCWC)* (pp. 0677–0682). IEEE.
- Red Hat (n.d.). *Red hat ansible automation platform*. <https://www.ansible.com/products/automation-platform>. Accessed on March 27, 2024

- Ros, S., González, S., Robles, A., Tobarra, L., Caminero, A. C., & Cano, J. (2020). Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. *IEEE Access*, 8, 97718–97728. <https://doi.org/10.1109/ACCESS.2020.2996361>
- Salazar, M., Gaviria, J., Laorden, C., & Bringas, P. G. (2013). Enhancing cybersecurity learning through an augmented reality-based serious game. In *2013 IEEE global engineering education conference (EDU-CON)* (pp. 602–607). IEEE.
- Sağlam, R. B., Miller, V., & Franqueira, V. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, 66(3), 274–286. <https://doi.org/10.1109/TE.2022.3231019>
- Shivapurkar, M., Bhatia, S., & Ahmed, I. (2020). Problem-based learning for cybersecurity. *Education*, 7(1), 6.
- Shulha, O., Ianenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modeling. *Journal of Open Innovation Technology Market and Complexity*. <https://doi.org/10.3390/joitmc8020080>
- Srinivasan, M., Wilkes, M., Stevenson, F., Nguyen, T., & Slavin, S. (2007). Comparing problem-based learning with case-based learning: Effects of a major curricular shift at two institutions. *Academic Medicine*, 82(1), 74–82. <https://doi.org/10.1097/01.ACM.0000249963.93776.aa>
- TryHackMe (n.d.). *Hacktivities*. <https://tryhackme.com/hacktivities>. Accessed on April 20, 2024
- Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*. <https://doi.org/10.3390/s20247148>
- Valcke, M., Bonte, S., De Wever, B., & Isabel, R. (2010). Internet parenting styles and the impact on internet use of primary school children. *Computers and Education*, 55(2), 454–464. <https://doi.org/10.1016/j.compedu.2010.02.009>
- Vanderhoven, E., Willems, B., Hove, S. V., & All, A. (2015). Wait and see? Studying the teacher's role during in-class educational gaming. In *European conference on games based learning* (pp. 540–547).
- Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, 4, 862221. <https://doi.org/10.3389/fdgh.2022.862221>
- Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud and Security*, 2019(5), 9–12. [https://doi.org/10.1016/S1361-3723\(19\)30052-1](https://doi.org/10.1016/S1361-3723(19)30052-1)
- Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers and Security*, 88, 101636. <https://doi.org/10.1016/j.cose.2019.101636>
- Yuan, X., Jiang, K., Murthy, S., Jones, J., & Yu, H. (2010). Teaching security management with case studies: Experiences and evaluation. *Journal on Education, Informatics and Cybernetics (JEIC)*, 2(2), 25–30
- Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. *Journal of Systems and Software*, 210, 111946. <https://doi.org/10.1016/j.jss.2023.111946>
- Zwilling, M., Klien, G., Lesjak, D., Wiecheteck, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97. <https://doi.org/10.1080/08874417.2020.1712269>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Willi Lazarov¹  · Tiina Schafeitel-Tähtinen²  · Joseph Squillace³  ·
Zdenek Martinasek¹  · Aneta Coufalikova⁴  · Marko Helenius²  · Petr Gallus⁴  ·
Radek Fujdiak¹ 

✉ Willi Lazarov
lazarov@vut.cz

Tiina Schafeitel-Tähtinen
tiina.schafeitel-tahtinen@tuni.fi

Joseph Squillace
jms10943@psu.edu

Zdenek Martinasek
martinasek@vut.cz

Aneta Coufalikova
aneta.coufalikova@unob.cz

Marko Helenius
marko.helenius@tuni.fi

Petr Gallus
petr.gallus@unob.cz

Radek Fujdiak
fujdiak@vut.cz

¹ Brno University of Technology, Antonínská 548/1, 60200 Brno, Czechia

² Tampere University, Kalevantie 4, 33100 Tampere, Finland

³ Pennsylvania State University, State College, University Park, PA 16802, USA

⁴ University of Defence, Kounicova 65, 66210 Brno, Czechia