

ANALYSIS OF CYBERSECURITY TRAINING PLATFORMS AND SIMULATION ENVIRONMENTS AND OPPORTUNITIES FOR THEIR INTEGRATION INTO HIGHER EDUCATION

Dimitar TASHKOV*, Elitsa PAVLOVA, Veselina GAGAMOVA*, Violeta VASILEVA*****

***Rakovski National Defence College, Sofia, Bulgaria**

****University of National and World Economy (UNWE), Sofia, Bulgaria**

*****Future Innovation Labs, Sofia, Bulgaria**

d.tashkov@rndc.bg, v.gagamova@rndc.bg, epavlova@unwe.bg, violetta.ziv@gmail.com

Abstract: Cybersecurity training is gaining key importance in the context of growing threats in cyberspace. Educational institutions are looking for effective methods for providing theoretical and practical knowledge in cybersecurity. This report examines the challenges universities face in building educational programs and highlights the importance of popular platforms that can be integrated into bachelor's and master's programs. Attention is drawn to the need for cooperation between the academic community, business and government institutions to build a comprehensive strategy for the development of cyber competencies in higher education.

Keywords: cybersecurity, cyber competencies, simulation platforms, higher education

1. Introduction

Cybersecurity has become one of the most critical areas in today's digital world. Educational institutions are increasingly dependent on digital platforms, and the frequency and sophistication of cyberattacks are growing exponentially. The rapid pace of change in technology and cyberthreats creates a number of challenges for educators and students. This necessitates the need for qualified cybersecurity professionals who can address and mitigate these threats, and higher education institutions are an integral part of developing this skilled workforce. Modern learning platforms, from virtual training grounds to massive online courses, offer a variety of opportunities for flexible and interactive learning [1]. The purpose of this report is to systematize the main types

of simulation cybersecurity learning platforms, present their characteristics and advantages, and offer guidelines for their effective implementation in higher education.

The research in the report will be used for subsequent comparative analysis of four main types of platforms: Cyber Range, Massive Open Online Courses (MOOCs), Learning Management Systems (LMS), Gamification and Capture the Flag (CTF). The evaluation criteria included interactivity, accessibility, practical orientation, level of difficulty, and certification opportunities. The analysis is based on a literature review and good practices from academic institutions.

Cybersecurity covers a wide range of specialist areas and job roles. This includes an understanding of basic computer

architectures, data, cryptography, networking, secure coding principles, as well as operating system skills, proficiency in programming languages and knowledge of cybersecurity management approaches and standards. Theory is only the foundation, but practical application in a controlled environment is crucial for the effectiveness of the preparation [2]. In this context, technological platforms play a central role in modernizing training, through simulations, exercises and interactive methods.

2. Types of Cybersecurity Training Platforms

Combining research on cybersecurity training platforms and simulation environments with the analysis of the interoperability of communication and information systems (CIS) in a coalition environment, it becomes clear that the integration of modern technological solutions in higher education is essential for the preparation of personnel capable of operating effectively in the modern digital and multinational environment. Simulation training platforms provide flexible, realistic and scalable conditions for the development of practical skills necessary for the management of complex and interconnected information systems. In the context of coalition operations, where interoperability between different national and organizational structures is critical, training environments must model real-world scenarios with multi-layered communication architectures and standards. This not only achieves the acquisition of technical competencies, but also the development of strategic thinking, consistent with the requirements of security and joint operational activity in an international environment [3]. There are a number of training platforms that share common awareness topics, but what sets them apart is their effectiveness and how they are applied in the workplace. The study Changing the landscape of

cybersecurity education in the EU analyzed several training platforms with cybersecurity content. The findings show that Coursera includes about 50 cybersecurity courses, while the edX platform offers only 30 courses. The LinkedIn platform hosts about 120 cybersecurity courses, half of which are aimed at intermediate skills. Cybrary offers about 500 courses aimed at professionals who want to develop their careers in the field. ISACA provides courses at various levels in information security and courses for cybersecurity auditors. Modern cybersecurity training platforms, such as cyberwiser.eu, offer innovative solutions for capacity building and cybersecurity culture enhancement through cyber threat simulations and hands-on training [4]. The web-based platform allows users to take on the roles of attackers and defenders in various scalable and configurable scenarios representing an organization's IT infrastructure. The platform is designed to be an independent reference point for professional cybersecurity training in the European Union and offers different levels of training. The three main pilot applications of the platform cover different sectors: the energy sector, higher education and the transport sector, demonstrating its applicability in different areas [5].

3. Main groups cybersecurity training platforms

Cybersecurity training platforms can be divided into four main groups:

- 1) Cyber Range platforms are virtual environments that simulate real-world networks and attacks, where learners respond to incidents in a controlled environment. These platforms offer scenarios with escalating complexity, monitoring, and automated assessment. Popular platforms include Cyberbit Range, RangeForce, AWS Cloud Range, and Plex Cyber Range. The main advantages of these solutions are their automated performance

assessment, as well as the ability to adapt to different levels of complexity. Their implementation in a university environment requires significant resources: hardware, network infrastructure, trained staff, and regular scenario updates. Cyber Range platforms are proving to be an effective pedagogical tool for conducting labs, practical exams, and certification exams.

2) MOOC platforms are an accessible and flexible way to train in cybersecurity on a global scale. Platforms, such as Coursera, edX, Udemy and FutureLearn, offer a variety of courses on information security, ethical hacking, incident management etc. The main advantages of MOOCs are open access, the ability to learn at your own pace and the availability of certification programs created by leading universities and industry partners. A disadvantage is the lack of practical simulation, which limits their effectiveness in building practical skills. In a university context, MOOC platforms are particularly suitable for supplementary training, theoretical preparation or integration as part of blended curricula [6].

3) LMS are widely used in higher education. Examples of such systems are Moodle, Blackboard and Canvas. The possibilities for integration with external resources and adding exercises in virtual environments make LMS suitable for different levels of training. The main advantage is their compatibility with university infrastructure and the ability to track student progress and assess students. The disadvantage is that without the additional integration of interactive

modules for practical simulations, they provide mostly theoretical knowledge.

4) Gamification is a highly effective approach to cybersecurity education through game-based methods, says the report “How to Gamify Cybersecurity Learning on a Budget” [7]. The author emphasizes that gamification can make learning more interesting and effective by using elements such as challenges, rewards, and progression. An example of this is the ISACA database of questions, answers, and explanations, which includes full-fledged exam tests designed to mimic the real exam process and help candidates manage their time when answering. Platforms such as TryHackMe, Hack The Box, PicoCTF and CTFtime provide interactive challenges that cover topics such as cryptography, ethical hacking, network and application vulnerabilities, malware analysis and others [8]. By solving tasks of increasing difficulty, learners acquire not only technical skills, but also logical thinking, teamwork and confidence. These platforms often use gamified elements such as points, badges and ranking systems, which increase motivation. Despite their undeniable benefits, they are more suitable for intermediate and advanced participants, as they require basic knowledge and independent preparation. In the context of higher education, CTF events can be used as an additional learning tool.

Table 1 shows popular platforms with cybersecurity content, each with a definition of the type it belongs to.

.

Table 1 Popular platforms with cybersecurity content.

Platform	Type of platform	Brief description
AWS Cloud Range	Cyber Range	Cloud infrastructure for simulation and learning by doing.
Blackboard	LMS	University system with the ability to integrate videos, tests, assignments.
Canvas	LMS	Cloud LMS system, often used in English-speaking universities.

Coursera	MOOC	Online courses from universities.
CTFtime.org	Gamification/CTF	Catalog and rating of global CTF events.
Cyberbit Range	Cyber Range	Highly realistic environment for simulations and protection; used by universities.
Cybrary	MOOC	Specialized in cybersecurity for different levels.
edX	MOOC	Отворени университетски курсове, често в партньорство с MIT, Harvard и др.
FutureLearn	MOOC	Open university courses, often in partnership with MIT, Harvard etc. European MOOC platform with an academic focus.
Hack The Box	Gamification/CTF	Platform for ethical hacking and preparation for certification exams.
Moodle	LMS	The most widespread academic LMS platform.
Open Security Training	LMS	Collection of free training materials for integration into university courses.
Plex Cyber Range	Cyber Range	Academic platform used at Plovdiv University.
RangeForce	Cyber Range + Gamification	Online platform with interactive modules and simulated attacks.
TryHackMe	Gamification/CTF	Learning through games and challenges.
Udemy	MOOC	Courses from individual instructors.

Source: A gamification framework to enhance students' intrinsic motivation on MOOC [9, 11]

The analysis shows that Cyber Range is best suited for practical courses, MOOC for theoretical basis, LMS for institutional purposes, and CTF for advanced and motivational training. The combination of several platforms can provide comprehensive training.

4. Conclusions

In conclusion, it can be summarized that despite the outlined prospects for the application of information technologies and Cybersecurity Training Platforms and Simulation environments in the education of cadets and students and the consideration of ways to ensure its success, there are still many challenges in the future development of their integration into higher education [10]. These challenges can be indicated as directions for further work and are related

to the development of uniform criteria for teaching and assessment in alternative forms of education, development of test systems, selection of appropriate technology and software and use of a help system built into the software etc.

Acknowledgements

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030 and was adopted by Decision of the Council of Ministers No. 731 of October 21, 2021.

References

- [1] Tymoshchuk, D., Yatskiv, V., Tymoshchuk, V., & Yatskiv, N. Interactive cybersecurity training system based on simulation environments [Internet]. ResearchGate. 2025. Available from: https://www.researchgate.net/publication/387669672_Interactive_cybersecurity_training_system_based_on_simulation_environments.
- [2] Tymoshchuk, D., Yatskiv, V., Tymoshchuk, V., & Yatskiv, N. Interactive cybersecurity training system based on simulation environments [Internet]. ResearchGate. 2024. Available from: https://www.researchgate.net/publication/387669672_Interactive_cybersecurity_training_system_based_on_simulation_environments.
- [3] Krumova, K. Analiz na aspektite na operativna savmestimost na KIS v koalitsionna sreda. In: Sofia; 2022. 329–38.
- [4] Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training [Internet]. CORDIS. 2025. Available from: <https://cordis.europa.eu/project/id/786668/it>.
- [5] Cyber Range&Capacity Building in Cybersecurity [Internet]. CYBERWISER.eu. 2025. Available from: <https://cyberwiser.eu/>.
- [6] Krumova, K. Kiberefektite v operatsii – proektsia na sila v kiberprostranstvoto. In: Sofia; 2024. 346–56.
- [7] Tan Soon Chew, CISA, CRISC, CISM, CGEIT, CCSP, CISSP, PMP. How to Gamify Cybersecurity Learning on a Budget [Internet]. ISACA. 2023. Available from: https://www.isacajournal-digital.org/isacajournal/2023_volume_6/MobilePagedArticle.action?articleId=1927160.
- [8] Nespoli, P., Albaladejo-González, M., Ruipérez-Valiente, J.A., & Garcia-Alfaro, J. SCORPION Cyber Range: Fully Customizable Cyberexercises, Gamification, and Learning Analytics to Train Cybersecurity Competencies [Internet]. arXiv; 2024 [cited 2025 May 15]. Available from: <http://arxiv.org/abs/2401.12594>.
- [9] Kostadinov, C. Kiberataka – etapi, vidove, tendentsii v protivodeystvieto. In: 2022. 210–8. Sbornik dokladi ot Godishna nauchna konferentsia – Chast III, 110 godini traditsii, kachestvo prestizh, Izd. VA G. S. Rakovski, ISBN 978-619-7478-95-2, 210-218.
- [10] Puig, A., Rodríguez, I., Rodríguez, Á., & Gallego, I. Evaluating Learner Engagement with Gamification in Online Courses. Applied Sciences [Internet]. 2023 Jan; 13(3):1535. Available from: <https://www.mdpi.com/2076-3417/13/3/15>.
- [11] Kostadinov, Ch. Industria 4.0 i predizvikatelstvata pred osiguryavaneto na sigurnost i zashtita v kiberprostranstvoto. Avtomatizatsia na diskretnoto proizvodstvo, Broy 4. Izdatelstvo na TU-Sofia. ISSN: 2682-9584. Sofia. 2022. 184-189.