**YEARBOOK OF UNWE (2025), ACADEMIC PUBLISHING HOUSE UNWE**
ISSN (print): 1312-5486; ISSN (online): 2534-8949; http://unwe-yearbook.org/en/
DOI: https://doi.org/10.37075/YB.2025.1.02

# IMPROVING CYBERSECURITY EDUCATION IN MODERN HIGHER EDUCATION

Elitsa Pavlova[1]
*e-mail: epavlova@unwe.bg*

## Abstract

*In the context of the digital environment and growing threats in cyberspace, the need for highly qualified personnel in the field of cybersecurity is becoming increasingly tangible. This report considers cybersecurity as a key priority in modern higher education. It analyses the challenges that universities face in building practically oriented educational programs. It emphasizes the importance of popular technological solutions from the Microsoft ecosystem, which can be integrated into bachelor's and master's programs. It draws attention 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 skills, educational programs, higher education, higher education, Microsoft

**JEL:** O10, O14

## Introduction

Cybersecurity has become one of the most critical areas in today's digital world. Organizations and individuals 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 poses several 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. Universities in Europe are at different stages of their digital transformation, depending on the infrastructure and resources available to them. Digitalization includes changing curricula, changing organizational structures, creating interactive content. Technology giant Microsoft offers an extensive portfolio of tools and educational resources that can help increase competences, develop a stimulating learning and research environment.

[1] Eng., PhD, Department of National and Regional Security, Faculty of Economics of Infrastructure, University of National and World Economy, Bulgaria

Higher education policies do not directly affect innovation, but they do have a connection with the drivers of innovation, says a study conducted in EU universities. Improving university culture, through the "Cybersecurity Policies" methodology of the European Union Agency for Cybersecurity, is key for all stages of education (Baldwin, 2021).

This report is based on a literature review, an analysis of good practices, available tools and resources from Microsoft and other software companies, as well as conceptual modeling of the possibilities for their implementation in Bulgarian universities.

**Challenges for university education**

The rapid development of cybersecurity attacks, combined with the static nature of academia, has contributed to emerging mismatches between the knowledge taught in educational context and the skills expected by employers. The need to build cybersecurity knowledge and skills has led to the creation of competence centers, Concordia (Concordia, 2025) and Cybersec4Europe (European Cybersecurity Competence Centre and Network, 2025), which focus on the cybersecurity education ecosystem in the EU. An ENISA report describes the state of cyber skills development in the EU (ENISA, 2024), highlighting the ever-growing shortage of cybersecurity skills and professionals. A study "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training" reveals what types of competences are required by the industry and how these competences can be acquired through exercises and real-world simulation (Blažič, 2021). Another important piece of information in the study concerns the lack of updated curricula and a mismatch between market demand and knowledge supply. The identified problems stem from insufficient funding, as well as a poor understanding of the cybersecurity job market. Employers are looking for professionals with practical experience who can work with platforms such as Microsoft Azure, Microsoft Defender, SIEM solutions and others. Therefore, universities should provide opportunities for practical exercises and certification.

Another factor that hinders good cybersecurity training is the lack of specialization of teachers. In its study, ECSO also highlighted the need for professionals to understand all the disciplines that make up the field of cybersecurity. Most of these findings lead to the conclusion that there is a need for a clearer definition of the knowledge and skills that a student should possess. The Cybersecurity-4Europe Centre conducted a study on whether there are good facilities in the EU for training and practice for students at bachelor's or master's degrees. The report states that higher education programs should encourage the use of cyber training grounds. It draws attention to the fact that the content of the educational

program should be enriched with topics on organizational or human aspects of cybersecurity. The main challenges described in the study "Universities in the Digital World" are a high degree of age differentiation in terms of opportunities for working with digital technologies, lack of strategic vision regarding cybersecurity training, achieving a balance between increasing societal demands and expectations for higher education (Nguyen, 2018). Attention is drawn to the lack of practical experience of students, which leads to a mismatch of skills between what businesses are looking for in a job candidate and the skills that candidates possess after graduation. "Training should be continuous, and the content should be updated regularly, covering emerging security threats and security controls that are implemented to protect information", says the article "What is security training and why is it important?" (Kaspersky, 2023). That's why universities can use Microsoft cybersecurity tools to improve student learning and raise employee awareness in line with their roles and positions.

**Cybersecurity Content Training Platforms**

As cyber threats increase globally, the need for trained cybersecurity professionals is becoming critical. Higher education is a key factor in developing the necessary knowledge and skills. Cybersecurity encompasses 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, programming language proficiency, 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 training. In this context, technology platforms play a central role in modernizing training through simulations, hands-on work, and interactive methods.

Cybersecurity training platforms can be divided into several main types:

- Cyber Range platforms;
- Massive Open Online Courses platforms;
- Learning Management Systems with cybersecurity content;
- Gamification and Capture the Flag.

The study Changing the landscape of cybersecurity education in the EU analyses several training platforms with cybersecurity content on the market (2022). It shows that Coursera has 33 million users and 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 has 2 million users and offers about 500 courses aimed at professionals who want to develop their careers in the field. IASACA provides online,

offline and combined courses at various levels in both information security and cybersecurity, including courses for cybersecurity auditors. Cyberwiser offers the Cyber Range Platform as a new approach to simulating cybersecurity threats and countermeasures. Table 1 presents the most popular cybersecurity training platforms, as well as an example of its university application.

**Table 1:** Cybersecurity training platforms with examples from university programs

| Platform Name | Functionalities | Suitable for | University programs |
|---|---|---|---|
| Hack The Box | Virtual Machines, Ethical Hacking | Intermediate, Expert | Used by University College London as additional practice |
| RangeForce | Cyber Range Platform, Real Incidents, Protection and Response, DevSecOps. | All Levels | Part of the program at the University of Maryland |
| TryHackMe | Scenarios, Tutorials with guidance, Security tasks. | All Levels | Integrated in Penetration Testing training at many universities |
| Cisco Networking Academy | Network Security Training, CCNA, Certification. | Intermediate, Expert | Part of the program at many universities in the EU |
| Kali Linux & Metasploit | Open-source tools, Hands-on vulnerability training, Hacking. | Advanced | Universities in Germany and the US use them in labs |
| Cyberwiser | Cyber Range platform, Sybersecurity threat simulation and training. | All levels | Part of the program at many universities in the EU |
| EDX / Coursera | Courses from leading universities, Certification. | All levels | Harvard, MIT, Stanford, many universities in the EU |

*Source:* Own research

It is important to note that the cybersecurity education platforms reviewed are aimed at the same market, but they do not have a common competency framework, for example, Google Cloud Skills Boost training platform with practical tasks and simulations in GCP environment and LinkedIn cybersecurity courses with over 9.5 million users and Cybrary.

### The Role of Microsoft Technologies

Microsoft's latest Cyber Signals Report highlights the rising cyberattacks across the higher education sector and K-12 institutions (Inno-Thought Team, 2024). Institutions face an average of 2,507 cyberattack attempts per week globally, with universities being the top targets for malware, phishing, and IoT threats. Over the past year, Microsoft Defender for Office 365 blocked more than 15,000 emails per day targeting the education sector with malicious QR codes. The growing adoption of AI in higher education is adding new levels of sophistication to cyberattacks. In response to these dynamics, Microsoft is delivering innovative solutions that meet changing needs.

A key challenge for higher education institutions is effectively integrating technology into the curriculum. Microsoft technologies are widely used in curricula related to cybersecurity, data science, software development and project management. Universities use Outlook for email and calendar management, Office 365 for communication and collaboration, OneDrive and SharePoint cloud storage for sharing documents and files between students, faculty and administrative staff, as well as Microsoft Teams for distance learning and meetings. New trends related to cybersecurity include developing a risk-based security strategy, cloud infrastructure and high-speed networks, defined cybersecurity processes, cyberattack detection and response systems, etc.

Integrating Microsoft cybersecurity tools requires continuous updates to curricula, training faculty to effectively use new tools and ensuring access for students from different backgrounds. Limited budgets are also a challenge, which is why many universities use only the basic levels of security features included in Office 365 A1/A3 licenses. Licensing tools such as Defender for Endpoint, Microsoft Sentinel is too expensive for small public universities. This leads to misconfigured security policies in M365 and Azure. Security gaps can arise when, for example, a university deploys Microsoft Defender but fails to enable threat intelligence due to a lack of know-how, or security policies deployed through Microsoft Intune do not reach all devices in use. Key messages that ENISA is sending to organizations in this regard include more awareness and education about security at all levels, risk management, collaboration with academia (ENISA, 2025).

Some of the most commonly used Microsoft technologies in European universities are:

- Azure Cloud Platform. Azure provides free access to cloud computing resources, virtual machines, databases, as well as the ability to create virtual environments for training, simulating attacks, testing defenses, and setting up corporate infrastructure. Azure Security Center and Microsoft Defender tools are used to secure cloud environments in cybersecurity courses and give students an insight into security monitoring, vulnerability management,

and threat protection. Students can integrate identity and access management solutions such as Azure Active Directory into a secure corporate environment. Azure Lab Services enables the creation of virtual sandbox environments for cybersecurity training with minimal technical overhead.

- Microsoft Security Tools – Defender, Sentinel, etc. Using Sentinel in an academic environment, students can learn how to identify, analyze, and respond to security threats in real time, monitoring, and automated incident response. Defender Attack Simulations can be used to conduct exercises, including ethical hacking competitions.
- Power BI. Power BI allows students and researchers to create interactive reports and dashboards for data analysis and visualization. Popular in university courses where data science, economics, and business analytics are taught.
- Dynamics 365 is often used to train students in enterprise resource planning (ERP), customer relationship management (CRM), and for research purposes in areas such as marketing, business analytics, and finance.
- Visual Studio and Visual Studio Code are used in computer science and software engineering programs, programming, and software and website development. Both tools support programming in languages such as C++, C#, Python, JavaScript, Python, and HTML/CSS.
- SQL Server is a widely used relational database management system (RDBMS) in universities, especially in courses related to database management, software development, and data analytics.

In addition to the above, Microsoft also offers specific educational tools aimed at improving learning. Some European universities use Microsoft HoloLens, a mixed reality headset, for hands-on learning through 3D models, virtual labs and simulations. The GitHub platform provides open-source resources, tools and labs for learning and development. Microsoft Learn contains free modules focused on the basics of security, network protection, including topics such as Zero Trust, identity management, attack protection and more. Microsoft Learn courses offer certifications for SC-900 (fundamentals of cloud security, identities, data protection), Azure Security Engineer Associate (Microsoft Defender, policy management, cloud protection) AZ-500 and MS-500 which could be used as a supplement to the curriculum. Another option is to include teachers in Microsoft Certified Trainer programs and provide them with access to training materials and licenses.

Universities can collaborate with Microsoft on research projects to advance cybersecurity. Free software access and cloud credits for students make it affordable for universities to implement Microsoft technologies into their curricula. This is a huge advantage for higher education institutions that don't have the budget for expensive cybersecurity tools.

## Conclusion

Implementing innovative cybersecurity training platforms is an essential step towards preparing qualified personnel in the era of digital threats. Cybersecurity education suffers from a lack of practical exercises. Students rarely work with real tools and often graduate without the necessary practical skills. The lack of updated curricula and weak connection with business leads to a mismatch between market demand and the knowledge offered. Employers are looking for specialists with practical experience who can work with platforms such as Microsoft Azure, Microsoft Defender, SIEM solutions and others.

The transformation of cybersecurity training in higher education can be made possible by:

Investments in cloud laboratories and digital resources.

Introduction of laboratories with virtual environments (e.g. VMware platform or Azure Lab Services).

Use of open resources and open-source tools (e.g. Kali Linux, Wireshark, Metasploit).

Expansion of partnerships with industry (e.g. Cisco Networking Academy, Microsoft).

Promotion of certification among students and teachers.

Creating adapted courses based on Microsoft Learn with teaching in Bulgarian and integrating them into existing disciplines.

Holding annual CTF competitions.

The integration of new technologies into cybersecurity educational programs provides a real opportunity for the transformation of education through a practical approach and certification. Universities that invest in technological infrastructure will be better prepared to meet the modern demands of the labour market.

## References

Baldwin, R. G. (2021). Technology in Higher Education, available at: https://education.stateuniversity.com/pages/2496/Technology-in-Education-HIGHER-EDUCATION.html

Blažič, B.J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training, Technology in Society, 67, p. 101769, available at: https://doi.org/10.1016/j.techsoc.2021.101769.

Blažič, B.J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?, Education and Information Technologies (2022) 27, pp. 3011-3036, https://doi.org/10.1007/s10639-021-10704-y

Concordia. (2025.) Concordia, available at: https://www.concordia-h2020.eu/

European Union Agency for Cybersecurity (ENISA). (2024). Cybersecurity Skills Development in the EU, available at: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

European Union Agency for Cybersecurity (ENISA). (2025). ENISA's work with Industry, Operational Communities and Citizens, available at: https://www.enisa.europa.eu/about-enisa/enisa-in-the-eu/enisa-for-the-it-industry

European Cybersecurity Competence Centre and Network. (2025). The European Cybersecurity Competence Centre, available at: https://cybersecurity-centre.europa.eu/index_en

Inno-Thought Team. (2024). Microsoft's latest Cyber Signals Report highlights the rising cyberattacks across higher education sector and K-12 institutions, available at: https://www.inno-thought.com/post/microsoft-s-latest-cyber-signals-report-highlights-the-rising-cyberattacks-across-higher-education-s

Kaspersky. (2023). What Is Security Awareness Training and Why Is It Important?, available at: https://www.kaspersky.com/resource-center/definitions/what-is-security-awareness-training

Nguyen, D. (2018). The University in a World of Digital Technologies: Tensions and Challenges, Australasian Marketing Journal (AMJ), 26(2), DOI: 10.1016/j.ausmj.2018.05.012