A Taxonomy for Learning Cybersecurity with Artificial Intelligence

Mihai-Nicolae DULGHERU[1], Andrei-Cătălin NICA[2], Cătălin-Alexandru TRANDAFIRIDIS[3]
[1]The Bucharest University of Economic Studies
[2]The Bucharest University of Economic Studies
[3]National University of Science and Technology POLITEHNICA Bucharest
dulgherumihai19@stud.ase.ro, nicacatalin19@stud.ase.ro, alexandru@trandafiridis.ro

The article explores the area of adaptive learning and proposes a taxonomy for supporting STEM teaching in schools and universities. The approach is based on the hypothesis that AI can improve the learning process by mapping the curriculum on a taxonomy that is used to create an individual knowledge map for each learner. The authors provide a detailed proposal of such a taxonomy for the area of cybersecurity at an undergraduate and master's level. It is based on a proposed EU taxonomy for cybersecurity.

Keywords: *STEM, personalized learning, artificial intelligence, automated feedback*

1 Introduction

In these modern times, there is a very fast evolution of digital technologies. These technologies are starting to have components that are more and more developed using artificial intelligence. This is one of the reasons why education also needs to be updated regarding the methods of teaching and the technologies used. Also, taking into consideration the level of automation that can be seen everywhere, a new need for learning subjects like cybersecurity starts to grow. The progress that has been made in the past few years has opened new opportunities for the development of adaptive learning systems. These systems have a major importance in the efficiency analysis because they can analyze student performance in real time, generate personalized feedback, and improve student engagement, besides reducing the teacher's responsibilities.

The concept of adaptive learning in cybersecurity education needs a multilayered taxonomy. This taxonomy would work in a beneficial way for anyone who uses it. It would organize the content in a better manner, and it would adapt to the needs/ level of the student. The taxonomy proposed in the study is based on three main pillars: NIST CSRC taxonomy, ACM Classification System, and the cognitive learning models (e.g., Bloom and Anderson). The first pillar is supposed to help by offering a robust thematic structure in the industry standards, while the second pillar is supposed to help with the academic rigor and proper coverage on this topic.

By adding these three pillars into a single framework, we are going to create a tool for an infrastructure system that is able to deliver personalized instructions, be scalable for automating assessments, tracking learner progress, and ensuring compliance with international regulations (e.g., GDPR or NIS Directives).

Taking all of these into consideration, this taxonomy is going to act as a bridge between technical proficiency and pedagogical information, helping both students and teachers and making them both more engaged in the process of education.

2 Literature review

This section contains a summary regarding the state-of-the-art in adaptive learning. We have identified a series of representative articles and a relevant taxonomy supported at the EU level.

An extremely complex task is assessing student knowledge in higher education. This requires the combination of traditional methods and technology-enhanced tools. The former are represented by projects,

portfolios, and presentations. The latter refers to e-portfolios, simulations, and automated feedback systems used to achieve optimal outcomes. Combining these two categories of methods opens new pathways for assessment, interactivity, and adaptability. By aligning assessment tools with learning objectives and understanding the challenges associated with each method, educators can gain a comprehensive view of students' competencies [1].

Student assessment is important both individually, for students to understand their progress, and collectively, to obtain a clear overview of the group's current knowledge status. It is often impossible to implement an effective feedback system that genuinely benefits students. In the academic environment, this is the result of a large number of students per professor and limited resources, especially time. Additionally, occurrences of human error are to be expected when student work assessments are performed by human evaluators. This results in students forming a mistaken perception of feedback, which leads them to perceive it as a burden or judgment rather than an opportunity to improve their skills.

In the case of classic feedback provided via online platforms, all the answers given to students are identical and lack personalization. Such feedback fails to pinpoint the exact mistake made by a student, hindering their ability to understand precisely what went wrong or how they might avoid the mistake in the future. Typically, an expert in the field must provide these general answers.

In contrast, feedback generated by an LLM is automatically produced based on students' answers in real time. It specifically addresses each student's questions and identifies their mistakes. Additionally, it offers precise guidance on avoiding similar errors without expert intervention. This method can also be combined with cognitive taxonomies. This results in providing tailored feedback at various cognitive levels.

Furthermore, metrics generated from LLM feedback are personalized. These enable the lesson content to be adapted based on student performance [2].

LMS platforms can effectively support students' cognitive progress through explanatory and formative feedback. These provide clear explanations, often accompanied by additional helpful resources. The simple feedback merely states whether an answer is correct or incorrect. In contrast, explanatory feedback actively engages students in the learning process, clarifies concepts, and uses specific, real-time examples. These are generated by LLMs to help students comprehend their mistakes clearly and precisely.

The real-time feedback provided to evaluated students can greatly assist the platform in identifying concepts that students have not yet mastered, enabling adaptation of lesson content according to each student's needs [3].

Utilizing artificial intelligence-generated feedback can be significantly more relevant, timely, and efficient for students. Besides the fact that students who repeatedly review their knowledge tend to achieve better results compared to those who review only once, AI-generated feedback also relieves human evaluators of extra effort, saving a considerable amount of their time [4].

Adaptive learning systems have recently become increasingly popular due to their ability to customize the learning experience to the individual needs of each student by utilizing advanced algorithms for data analysis and performance monitoring. Previous research has demonstrated that artificial intelligence-based adaptive learning systems significantly improve students' educational outcomes. An example of this is provided by the article (Sari et al., 2024), which conducts a study involving 300 students and 50 teachers across primary to higher education, with a varied demographic structure. This study highlights that adaptive learning systems such as Smart

Sparrow and IBM Watson Education led to an increase in average assessment scores from 68.4 to 82.7 and improved course completion rates [5].

It is an educational method that is based on technology to personalize the learning process of students. This method, together with artificial intelligence and the support of machine learning algorithms, adjusts the teaching methods and the content of the lessons that are displayed to the student within the platform, to offer him an educational experience that helps him understand much more easily all the concepts for which the feedback obtained from the evaluation was not positive.

The Adaptive Learning method is based on several information accumulated during the evaluation by students. Among the information is information such as the current level of the student, his behavior at the time he receives feedback, or monitoring the answers to be able to observe any progress [6].

Knowledge can be modeled through a taxonomy, meaning hierarchical sets of models used to classify learning objectives according to their complexity level. Over time, multiple taxonomies have been developed and implemented to best accommodate various educational contexts. Due to their widespread popularity thus far, the taxonomies proposed by Bloom, Anderson, and Wilson have significantly impacted the academic world. However, due to the complexity of human beings and the human brain, there is a need to propose a new holistic taxonomy model of human thinking, which may necessitate further exploration in this field [7].

This hierarchical classification of learning objectives guides curriculum design and helps teachers formulate clear objectives that allow for the assessment of students at the cognitive level.

The synthesized taxonomy allows for a non-linear and adaptive assessment of student progress, not only at the collective but also at the individual level. The integration of such a taxonomy within an educational platform offers the possibility of adapting the content it makes available to the student, depending on the feedback obtained by him [8].

Using this mathematical method, two or more results of the evaluation stages can be combined, and a final score can be calculated to have an accurate assessment of the level the student is at. After obtaining the weighted average, an analysis can be made on the results obtained, and the content displayed to the student further on the educational platform will be adapted so that the average is as high as possible from one lesson to another [9].

3 ACM Classification System

The ACM (Association for Computing Machinery) taxonomy is used in computer science as a standardized classification system. It can be used to organize and label research topics, subfields, and subject areas. Researchers, academic journals, and digital libraries that index and facilitate the search and classification of scientific content are the main actors who use it very often [10].

The ACM taxonomy had a first version in 1998. Later, the 2012 version appeared, which was developed as a poly-hierarchical ontology that can be used for semantic web applications. The previous version, which was in 1998, was used as a standard classification system for the field of computer science. It is based on a semantic vocabulary with a single source of categories and concepts and is prepared for structural changes that may be made in the future. ACM offers the possibility of using a tool within the virtual display format. This helps to apply the CCS categories to future work and ensures that it remains current and relevant. On the virtual display, users can see both interactive views and views of the classification tree [11]. The ACM taxonomy is organized so that general categories are presented first, followed by subcategories that are increasingly specific and focused on the desired topic. It presents several main

categories that are very relevant and cover major areas of computer science. These categories are as follows: (1) General and Reference, (2) Hardware, (3) Computer Systems Organizations, (4) Networks, (5) Software and its engineering, (6) Theory of Computation, (7) Mathematics of Computing, (8) Information systems, (9) Security and privacy, (10) Human-Centered computing, (11) Computing methodologies, (12) Applied Computing, (13) Social and professional topics. Using these main categories, those who want to use the information can have much easier access to it in the desired area. For example, if someone wants to access information about 3D Integrated Circuits, they must access the main category Hardware, then access the subcategory Integrated Circuits. Users can follow this example for each information need they have regarding a specific topic in the field of computer science [12]. One of the primary functions of the ACM taxonomy is to support efficient indexing and retrieval of scholarly content. When submitting an article to an ACM journal or conference, authors must select the relevant classification codes that best describe the subject matter of their work. These codes are then used by digital libraries (such as the ACM Digital Library) to categorize publications, making it easier for users to find material that is relevant to their interests [13]. Taxonomy also helps editors assign reviewers with expertise in the right fields, thereby improving the peer-review process. In addition, it is a valuable tool for students and researchers who want to identify relevant areas of research or explore existing classifications in a particular field [14].

The ACM taxonomy is a key element in standardizing the language used in computer science research. The way it is used is to promote a common vocabulary to make communication between researchers easier and to make a clearer documentation of scientific contributions. At the same time, it offers the possibility of analyzing research trends by examining the distribution of publications as benchmarks of taxonomy codes[15]. The ACM taxonomy is very often used in the development of automatic tools that classify academic works using natural language processing (NLP) techniques. The indexing process for publishers and digital platforms is much simplified because algorithms can analyze the content of a scientific article and suggest appropriate ACM classification codes [16].

This is a tool of increasing importance in the academic and research environment of computer science. Through the coherent and hierarchical organization of the field, the indexing, analysis, and discovery of scientific content is supported. The existence of a classification system such as the ACM CCS is crucial in times of exponential data growth. These are the ability to maintain clarity and efficiency in scientific communication [17].

4 NIST CSRC Taxonomy

An essential basis for developing a structured taxonomy is the use of standardized classification systems. The taxonomies created by the National Institute of Standards and Technology (NIST) through its Computer Security Resource Center (CSRC) are one of the best-known in the field of cybersecurity [10]. The NIST CSRC taxonomy provides a comprehensive framework that covers several dimensions of cybersecurity. It contributes to making understanding, research, and development in this field easier. Furthermore, it helps identify research areas that are already well established while guiding future research directions by highlighting those that are under-explored.

There are six dimensions (topics) that form the basis of this taxonomy: (1) Security and privacy, (2) Technologies, (3) Applications, (4) Laws and regulations, (5) Activities and products, and (6) sectors [18]. The first one covers topics such as data science for

security, cybersecurity, and the social and human side of cybersecurity. It attracts input from disciplines such as management and psychology, showing the field's interdisciplinary nature [19]. The second dimension includes a wide range of technologies, among them 5G and 6G networks, and points to the need for ongoing research to address emerging vulnerabilities [20]. The Applications dimension focuses on the practical use of security measures in different sectors. It highlights the importance of context in developing solutions and encourages exploration of areas that have been little studied [21]. The laws and regulations dimension refers to the legal framework that governs cybersecurity practices. This varies by jurisdiction, and emphasizes the need for compliance and for regulations that can adapt to new threats [22]. The fifth dimension separates activities such as research, technological development, and public policy making, and underlines their dynamic character [19]. The last dimension classifies security efforts by industry, which comes with tailored approaches for recognizing that each sector faces specific challenges and rules [20].

In adaptive learning, using the NIST taxonomy provides a wide range of advantages, especially on platforms based on artificial intelligence. It allows a structured modelling of knowledge, which is the basis for building individual learner maps that can be linked to learning goals and automatically adapted to their performance and difficulties. The taxonomy also supports targeted feedback: an AI model can connect learners' errors not only to the wrong answers, but also to specific knowledge areas, for example, distinguishing between an error in the logic of a cryptographic protocol and one related to identity-federation policy. As a result, feedback becomes more precise and educationally relevant.

The NIST taxonomy also helps align the proposed AI-based STEM learning taxonomy with structures recognized worldwide. According to the report published by the Joint Research Centre (JRC) of the European Commission, titled "A Proposal for a European Cybersecurity Taxonomy" (2019), the NIST CSRC model was one of the most influential sources in shaping the European knowledge framework in the field [10].

The European taxonomy expands the NIST framework by integrating new rules. These consist of the GDPR and NIS Directive, which suit the legal and sector-specific needs of the European Union. The GDPR regulates how personal data is processed in the EU, stressing legality, transparency, and accountability [23], and applies to all entities that handle data about EU residents [24]. The NIS Directive, on the other hand, aims at the security of networks and information systems, placing security requirements and reporting duties on providers of essential and digital services [25].

The taxonomy we propose for learning in cybersecurity mixes elements from the NIST framework, the European model, and the ACM taxonomy. This aims to combine technological coverage, regulatory compliance, and sector relevance. The detailed structure of the NIST taxonomy is an ideal basis for AI learning platforms. It enables the assignment, adaptation, and dynamic assessment of educational modules. Additionally, it also makes it possible to link cognitive taxonomies (such as Bloom or Anderson) with thematic classifications in cybersecurity. Thus, learning management systems can adapt content not only to the field of expertise (for example, malware analysis) but also to the cognitive level involved (application versus evaluation).

In conclusion, the NIST CSRC taxonomy is a fundamental model for organizing adaptive learning experiences in cybersecurity. Its multidimensional structure fits the goals of personalized learning, automated feedback, and knowledge

assessment. Despite originating from an American context, its relevance and solid design make it a valuable reference for creating a global educational framework in cybersecurity.

5 Our proposed taxonomy

To support adaptive learning in cybersecurity education, we propose a hierarchical taxonomy integrating core elements from the NIST CSRC Taxonomy and the ACM Classification System. This structured AI-compatible model enables personalized knowledge maps aligned with STEM goals at undergraduate and master's levels.

There are three levels of taxonomy:

- Core domains
- Learning subdomains
- Cognitive learning objectives

This structure allows curriculum content to be mapped to knowledge checkpoints. As a result, it facilitates AI-driven formative and personalized feedback.

5.1 Core domains

The selected core domains reflect comprehensive and interdisciplinary cybersecurity challenges. The NIST CSRC and ACM Classification System serve as the foundation, addressing key technological and sector-specific issues relevant globally:

1. Cryptography
2. Identity and access management
3. Security operations and incident response
4. Network security
5. Privacy and data protection
6. Human factors and security behavior
7. Software and systems security

5.2 Learning subdomains

The second level consists of concise, practical subdomains designed for quick learning modules (approximately 2 hours each). This is based on reflecting immediate workforce needs and current organizational challenges, such as:

1. Cryptography
    a. Digital signatures and hashing
    b. Encryption techniques
2. Identity and access management
    a. Multi-factor authentication
    b. Authorization and access control models
3. Security operations and incident response
    a. Incident detection and reporting
    b. Digital forensics basics
4. Network security
    a. Firewalls and VPN
    b. Wireless and mobile security
5. Privacy and data protection
    a. GDPR compliance
    b. Anonymization techniques
6. Human factors and security behavior
    a. Phishing and social engineering awareness
    b. Usability and security practices
7. Software and systems security
    a. Secure coding practices
    b. Vulnerability scanning and management

5.3 Cognitive learning objectives

At this level, each subdomain includes two clear objectives. These facilitate practical learning and highlight different skills:

- An "Apply" objective promotes immediate practical skills.
- An "Analyze/Evaluate" objective encourages complex situation analysis and critical thinking.

Examples of objectives include vulnerability analysis, configuring firewall rules, applying anonymization techniques, and evaluating GDPR compliance. These support automated assessment and personalized learning paths through AI platforms.

Table 1. Cognitive learning objectives in cybersecurity education

Subdomain	**Objective 1 (Apply)**
	Objective 2 (Analyze/Evaluate)
Digital signatures and hashing	Apply hashing for data integrity
	Compare SHA-256 and SHA-1 algorithms
Encryption techniques	Apply symmetric encryption for files
	Evaluate AES versus DES vulnerabilities
Multi-factor authentication	Configure MFA in real scenarios
	Analyze SMS authentication risks
Authorization and access control	Apply RBAC rules in real systems
	Compare RBAC and ABAC
Incident detection and reporting	Identify incidents using logs
	Analyze incidents via firewall logs
Digital forensics basics	Collect digital evidence
	Evaluate the validity of digital evidence
Firewalls and VPN	Configure basic firewall rules
	Analyze VPN configuration-related incidents
Wireless and mobile security	Set up secure Wi-Fi networks
	Analyze wireless protocol vulnerabilities
GDPR compliance	Identify sensitive personal data
	Evaluate GDPR compliance in web forms
Anonymization techniques	Apply anonymization methods
	Compare anonymization and pseudonymization
Phishing and social engineering	Identify phishing emails
	Analyze the effectiveness of anti-phishing campaigns
Usability and security practices	Implement basic security controls
	Analyze usability impacts on security
Secure coding practices	Apply OWASP principles to application code
	Analyze code for OWASP Top 10 vulnerabilities
Vulnerability scanning and management	Conduct vulnerability scanning
	Evaluate the identified vulnerabilities' criticality

The proposed taxonomy integrates seamlessly with AI-driven adaptive learning platforms. Each taxonomy element serves as a personalized learning checkpoint. This allows immediate and targeted feedback based on identified gaps. Thus, the taxonomy becomes a robust tool for rapid and personalized learning improvement.

6 Conclusion

This study proposes an integrative taxonomy designed to support adaptive learning in cybersecurity education, addressing a critical need for personalized, scalable, and cognitively aligned instructional systems. By unifying elements from the NIST CSRC taxonomy, the ACM Classification System, and cognitive learning models, we construct a robust framework capable of guiding both the development of content and the automation of formative assessment within AI-based educational platforms.

The taxonomy's hierarchical structure - comprising core domains, focused subdomains, and cognitive learning objectives - enables the construction of individualized learning maps that respond dynamically to student performance. Through this structure, educators and systems alike can more effectively deliver targeted feedback, monitor conceptual understanding, and adjust instructional strategies in real time. Importantly, the taxonomy supports alignment with regulatory standards such as the GDPR and the NIS Directive, ensuring that the educational content is not only pedagogically sound but also compliant with legal and ethical requirements relevant to cybersecurity.

Future research should focus on empirical validation of this taxonomy through real-world deployment in university-level courses or professional training programs. Additionally, further iterations may explore expansion into related domains such as data science, digital ethics, or critical infrastructure protection. Through these next steps, the taxonomy can evolve from a conceptual proposal to a scalable standard for adaptive learning in cybersecurity and beyond.

References

[1] D. M. Djamalovna, "METHODS AND TOOLS FOR ASSESSING STUDENT COMPETENCIES," Current Research Journal of Philological Sciences, vol. 5, no. 10, pp. 19–24, Oct. 2024, doi: 10.37547/PHILOLOGICAL-CRJPS-05-10-04.

[2] A. Kinder et al., "Effects of adaptive feedback generated by a large language model: A case study in teacher education," Computers and Education: Artificial Intelligence, vol. 8, p. 100349, Jun. 2025, doi: 10.1016/J.CAEAI.2024.100349.

[3] S. Huskisson, T. O'Mahony, and S. Lacey, "Improving student outcomes using automated feedback in a first-year economics class," International Review of Economics Education, vol. 47, p. 100303, Dec. 2024, doi: 10.1016/J.IREE.2024.100303.

[4] M. Cooper-Stachowsky and M. Cooper-Stachowsky, "Enhancing Learning via AI-Generated Feedback and Resubmission of Formative Assessments," Proceedings of the Canadian Engineering Education Association (CEEA), Dec. 2024, doi: 10.24908/pceea.2024.18540.

[5] H. E. Sari, B. Tumanggor, and D. Efron, "Improving Educational Outcomes Through Adaptive Learning Systems using AI," International Transactions on Artificial Intelligence, vol. 3, no. 1, pp. 21–31, Nov. 2024, doi: 10.33050/ITALIC.V3I1.647.

[6] E. du Plooy, D. Casteleijn, and D. Franzsen, "Personalized adaptive learning in higher education: A scoping review of key characteristics and impact on academic performance and engagement," Heliyon, vol. 10, no. 21, p. e39630, Nov. 2024, doi: 10.1016/J.HELIYON.2024.E39630.

[7] M. A. Aripin, R. Hamzah, P. Setya, M. H. M. Hisham, and M. I. Mohd Ishar, "Unveiling a new taxonomy in education field," International Journal of Evaluation and Research in Education (IJERE), vol. 9, no. 3, pp. 524–530, Aug. 2020, doi: 10.11591/IJERE.V9I3.20458.

[8] O. Gun and M. J. Bossé, "Synthesizing cognitive mathematics learning taxonomies," Thinking Skills and Creativity, vol. 57, p. 101796, Sep. 2025, doi: 10.1016/J.TSC.2025.101796.

[9] S. Sarker, M. K. Paul, S. T. H. Thasin, and M. A. M. Hasan, "Analyzing students' academic performance using educational data mining," Computers and Education: Artificial Intelligence, vol. 7, p. 100263, Dec. 2024, doi: 10.1016/J.CAEAI.2024.100263.

[10] I. Nai-Fovino, R. Neisse, J. L. Hernandez-Ramos, N. Polemi, G. Ruzzante, and M. Figwer, "A Proposal for a European Cybersecurity Taxonomy," 2019, doi: 10.2760/106002.

[11] "Computing Classification System." Accessed: May 30, 2025. [Online]. Available: https://dl.acm.org/ccs

[12] "HOW TO CLASSIFY WORKS USING ACM'S COMPUTING CLASSIFICATION SYSTEM".

[13] S. Isukapalli and S. N. Srirama, "A systematic survey on fault-tolerant solutions for distributed data analytics: Taxonomy, comparison, and future directions," Computer Science Review, vol. 53, p. 100660, Aug. 2024, doi: 10.1016/J.COSREV.2024.100660.

[14] D. Carreira-Flores, M. Rubal, E. Cabecinha, G. Díaz-Agras, and P. T. Gomes, "Unveiling the role of taxonomic sufficiency for enhanced ecosystem monitoring," Marine Environmental Research, vol. 200, p. 106631, Sep. 2024, doi: 10.1016/J.MARENVRES.2024.106631.

[15] J. B. Minani et al., "IoT systems testing: Taxonomy, empirical findings, and recommendations," Journal of Systems and Software, vol. 226, p. 112408, Aug. 2025, doi: 10.1016/J.JSS.2025.112408.

[16] M. P. dos Santos, W. F. Heckler, R. S. Bavaresco, and J. L. V. Barbosa, "Machine learning applied to digital phenotyping: A systematic literature review and taxonomy," Computers in Human Behavior, vol. 161, p. 108422, Dec. 2024, doi: 10.1016/J.CHB.2024.108422.

[17] R. L. Fleurence et al., "A Taxonomy of Generative AI in HEOR: Concepts, Emerging Applications, and Advanced Tools – An ISPOR Working Group Report," Value in Health, vol. 0, no. 0, May 2025, doi: 10.1016/J.JVAL.2025.04.2167.

[18] "NIST Computer Security Resource Center | CSRC." Accessed: May 30, 2025. [Online]. Available: https://csrc.nist.gov/

[19] H. Suryotrisongko and Y. Musashi, "Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective," Proceedings - 2019 IEEE 12th Conference on Service-Oriented Computing and Applications, SOCA 2019, pp. 162–167, Nov. 2019, doi: 10.1109/SOCA.2019.00031.

[20] J. E. Ounza, "A taxonomical survey of 5G and 6G security and privacy issues," https://gjeta.com/sites/default/files/GJETA-2023-0047.pdf, vol. 14, no. 3, pp. 042–060, Mar. 2023, doi: 10.30574/GJETA.2023.14.3.0047.

[21] C. Meadows, "An outline of a taxonomy of computer security research and development," Proceedings New Security Paradigms Workshop, vol. Part F129673, pp. 33–35, Aug. 1993, doi: 10.1145/283751.283770/ASSET/8949DF88-571F-4546-B40C-C23C8C7007E4/ASSETS/283751.283770.FP.PNG.

[22] G. M. NIST, "NIST Privacy Workforce Taxonomy," 2024. doi: 10.6028/NIST.CSWP.38.ipd.

[23] Andrew Cormack, "An Introduction to the GDPR (v2)," vol. 1, no. 5, 2021.

[24] "General Data Protection Regulation," A Guide to Financial Regulation for

Fintech Entrepreneurs, pp. 187–194, Mar. 2018, doi: 10.1002/9781119436775.CH18.

[25] M. D. Cole and S. Schmitz, "The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape," SSRN Electronic Journal, Dec. 2019, doi: 10.2139/SSRN.3512093.

Mihai-Nicolae DULGHERU completed his studies at the Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest University of Economic Studies, in 2022. He then earned a master's degree in eBusiness at the same institution and is currently a first-year doctoral student at the Doctoral School of Economic Informatics, where he also serves as an associate teaching assistant in the Department of Economic Informatics and Cybernetics. His doctoral research focuses on **Artificial-Intelligence-based adaptive learning technologies**, with a thesis titled "Design and development of AI-driven adaptive learning solutions". Beyond academia, he has three years of professional experience as a full-stack web developer, possessing solid expertise in object-oriented and functional programming, modern web frameworks, distributed systems, and cloud-native architectures. His broader research and teaching interests include educational technology, intelligent information systems, and software engineering.

Andrei-Cătălin NICA graduated from the master's program in Online Marketing at the Bucharest University of Economic Studies in 2024. He has been a PhD student since 2024 within the Doctoral School of Economic Informatics at the Bucharest University of Economic Studies, currently enrolled in the second year. He has conducted Economic Informatics seminars for seven student groups from the Faculties of Business and Tourism, and International Economic Relations. At present, he works as a programmer in a company specializing in robotics equipment and software development in the educational field. He has professional experience in the fields of STEM, artificial intelligence, and educational robotics. Among his works is the article: "Supporting Hybrid and Remote Learning through Virtual Infrastructures Integrated with Cyberquest and Raspberry Pi" (2025).

Cătălin-Alexandru TRANDAFIRIDIS graduated from the Faculty of Transport Engineering, University Politehnica of Bucharest, with a specialization in Electronics, Remote Control and Telecommunications. He pursued a master's degree in Intelligent Transport Systems within the same institution, focusing on the integration of cybersecurity measures in modern transportation infrastructures. Professionally, he has contributed to digital infrastructure and ITS-related projects in collaboration with the Romanian Ministry of Transport and European initiatives such as DATEX and NAPCORE. He is the founder and managing partner of a technology and digital marketing company and teaches computer science at the high school level within an international academic environment. His work focuses on applied cybersecurity, system architecture, and educational technologies.