DOI: 10.47743/eufire-2025-1-22

GAMIFICATION MEETS AI: EXPLORING SYNERGISTIC TECHNOLOGIES FOR CYBERSECURITY EDUCATION IN BUSINESS SCHOOLS

DANIELA POPESCUL
Alexandru Ioan Cuza University of Iaşi
Iaşi, Romania
rdaniela@uaic.ro

RALUCA-PETRONELA MAHU
Alexandru Ioan Cuza University of Iaşi
Iaşi, Romania
mahuraluca00@gmail.com

Abstract
The growing complexity of cybersecurity threats and countermeasures, combined with the low awareness on this topic, demands innovative approaches to education and training. Recent literature highlights the potential of gamification and artificial intelligence (AI) to enhance learner engagement and knowledge retention in the field of cybersecurity. This article offers a critical review of current applications of AI and gamification in cybersecurity education, with a focus on university-level teaching.
Building upon this theoretical foundation, the study explores students' and experts' perceptions of AI and gamification use, aiming to contribute to a better understanding of how emerging technologies can enhance motivation and engagement in cybersecurity education. The insights obtained through a mixed-methods approach may support the development of more engaging and relevant cybersecurity higher education practices.
Keywords: *gamification; cybersecurity; artificial intelligence; higher education; motivation.*
JEL Classification: I23; M15; D83.

1. INTRODUCTION

Last decade's technology evolution has impacted students' educational process, and their connection to the labour market. Due to the rise of artificial intelligence (AI), expectations have changed regarding the knowledge needed to remain adaptable in a dynamic economy and job market. Moreover, the continuous escalation of cybersecurity threats has made specialists in this field a critical asset in both public and private sectors (European Union Agency for Cybersecurity (ENISA), 2023), and created a steady demand for workforce in the sector (Tummala and Bottomley, 2024; Maennel and Maennel, 2024). The United

States already has a shortage of 265,000 security professionals in 2025 (Fourrage, 2025). CyberSeek shows that in 2024, only 83% of security jobs are filled in the United States (Dice Staff, 2024). According to a 2024 report by the World Economic Forum, the global cybersecurity industry needs 4 million specialists in order to fill the growing workforce gap (Meineke, 2024). Recent studies have shown that cybersecurity job growth is expected to reach 33% between 2023 and 2033 (Kelly, 2025).

According to IBM, information security is *the protection of important information from unauthorized access, use, disclosure, modification, or disruption*. This protection applies to all types of information assets, including digital files, paper documents, physical storage media, and verbal communications. Across the entire data lifecycle, information security (InfoSec) addresses infrastructure, software, testing, auditing, and archiving (Holdsworth and Kosinski, 2024).

Often, the term InfoSec (the abbreviation used for information security) is used interchangeably with CyberSec (the abbreviation used for cybersecurity). This is due to a simple confusion or a partial overlap of the two concepts. Information security is defined as guaranteeing and maintaining the confidentiality, integrity and availability of information (Taherdoost, 2022). Cybersecurity refers to *the protection of exclusively digital information systems* (Merriam-Webster, 2025).

The demand for qualified professionals in information security is linked to the level of awareness regarding the importance of information assets' protection. According to (Scholl, 2023), information security awareness should be regarded as an integral component of any organization, as it serves as a foundational requirement for effective information security management and for its operationalization. Creating awareness in any field is not an easy task, especially for higher-education students. Low motivation is a major factor in the limited engagement with security-related content, which is consistent with the general trend among students. To address this emerging issue, educational institutions are increasing their efforts to implement innovative teaching strategies to enhance student engagement and motivation.

One solution that has been studied extensively in recent years is gamification as a pedagogical instrument, aimed at making learning more engaging and fun. Gamification has proven particularly effective in higher education by combining theoretical concepts with real-life applications through immersive, scenario-based learning. Incorporating elements such as leaderboards, collaborative tasks and post-activity debriefings, gamified experiences foster student engagement and encourage active learning (Christopoulos and Mystakidis, 2023; Zourmpakis *et al.*, 2023).

The Cambridge Dictionary defines gamification as *the practice of transforming activities so that they resemble games, to make them more attractive*

and increase participant engagement (Cambridge Dictionary, 2025). Gamification refers, broadly speaking, to technological, economic, cultural and social developments, through which reality becomes more similar to a game, allowing for greater accumulation of skills, motivational benefits, creativity, involvement and, in general, happiness and constructive development (Hamari, 2019).

Recent meta-analysis studies show that gamification can significantly impact academic performance. Li *et al.* (2023) examined 41 studies in this field (with 5071 participants) and concluded that gamified instructional strategies can substantially enhance student learning outcomes in higher education. Another study focusing on the Kahoot! platform confirmed a moderately positive effect on academic performance, based on a meta-analysis of 43 empirical studies related to gamification (Özdemir, 2025).

In 2024, Zeng *et al.* (2024) conducted a meta-analysis on gamification in education, which investigated 22 experimental studies, carried out between 2008 and 2023. Using a random-effects model, the findings indicated that gamification had a moderately positive impact on student's academic achievement, providing valuable insights regarding the selection and utilization of the right game design elements.

Another obvious and relevant solution is the use of AI, which could contribute to increased engagement and motivation among students, if implemented correctly (Zourmpakis *et al.*, 2023; Lee *et al.*, 2024). Britannica defines AI as the ability of a digital computer to perform tasks commonly associated with intelligent beings (Copeland, 2025).

According to Robert Jenay, the higher education community is optimistic about the role of AI in teaching and learning: the survey they conducted shows that out of 730 respondents, 69% of them expect AI to be increasingly used for learning analytics, while 68% and 66% believe it will improve accessibility for students and faculty (Robert, 2024). Regarding motivation and engagement, AI has been shown to enable their enhancement, by offering personalized learning experiences, providing immediate feedback and fostering a supportive environment where learners feel more confident and less anxious (Batista *et al.*, 2024).

2. THE SYNERGETIC USE OF AI AND GAMIFICATION IN TEACHING AND LEARNING CYBERSECURITY

The *integration of AI in cybersecurity courses and trainings* represents an emerging approach, offering new possibilities for innovation in the educational system. Dwight (2023) proposes a scenario-based tabletop exercise (TTX) focused on cybercrime as an active learning method for students in the field of cybersecurity. The approach is based on the NIST Test, Training, and Exercise methodology and involves collaboration with industry professionals. It aims to

enhance students' practical skills while offering professionals an effective way to contribute to education, even with limited resources. The author also suggests the use of generative AI to assist in drafting the documentation required for TTX exercises. Given the increasing complexity of cybersecurity, Maennel and Maennel (2024) propose an integrated human-AI training model for exercises such as blue/red teaming, simulations, tabletop, and capture-the-flag. The model combines AI, learning analytics, and pedagogy to enhance cybersecurity education. It aims to teach learners how to collaborate with AI, detect misuse, and leverage AI tools, especially for analysing learning data. The authors show that multimodal analytics (e.g., facial recognition, eye-tracking) help transform raw data into insights on learning, retention, and behaviour, enabling personalized paths and real-time feedback. Won *et al.* (2024) present an innovative approach implemented during a summer camp intended to spark U.S.' high school students' interest in cybersecurity. The organizers used radio-controlled autonomous cars to integrate cybersecurity and AI concepts through hands-on activities and interactive projects. Students strengthen their technical skills and build confidence by training AI models for the cars or simulating cyberattacks. Pre- and post-camp surveys show a clear increase in students' interest and self-efficacy in computing, cybersecurity, and AI, encouraging early engagement with STEM careers.

Recent studies suggest that *combining AI and gamification* can enhance the quality of teaching and learning in higher education. The fusion of AI's adaptive capabilities with gamification's motivational mechanics can transform passive learning environments into interactive educational systems (Limonova *et al.*, 2023). Their study also highlights the time needed for teachers and professors to adapt to the new approaches, underlining the importance of continuous professional development, institutional support, and pedagogical training to ensure effective integration of AI and gamification into existing curriculum.

According to (Arteaga and Granados Guzmán, 2024), the combination of AI content with gamified narratives and storytelling can improve the overall experience of students. Escape rooms or quizzes integrated into platforms like Genially, Canva, Blooket and Quizizz, support personalized learning through instant feedback and positive competition, and offer engaging experiences that improve understanding and retention among students.

Besides already existing applications where gamification and AI can be integrated, researchers also explored the possibility of creating new and personalized platforms for students. Regarding this topic, Tan and Cheah, (2021) present an AI-enabled, gamified online learning application designed to enhance interactivity, personalize content, and maintain student engagement over time. They integrated AI algorithms and gamification elements into the app, the results indicating improvement in user satisfaction and engagement, but also in knowledge retention and learning effectiveness.

Zia and Noor (2024) argue that both gamification and AI can lead to improved educational outcomes, by making learning more interactive, customized and engaging for students. Their study highlights that AI's capabilities, combined with game elements, such as points, badges, leaderboards and challenges, can generate dynamic learning experiences.

An explicit use of AI in gamified learning systems is presented in the article "Developing a gamified AI-enabled online learning application to improve students' perception of university physics" (Tan and Cheah, 2021). The authors have implemented an AI mechanism that can analyse student behaviour and performance to adjust game mechanics, such as difficulty levels, rewards, and pacing. The results showed that most participants expressed willingness to use the tool, they believed that it could increase engagement among students, with 92% of them agreeing that it encouraged them to persist, even if they felt uncertain or stuck.

In 2023, Yang *et al.* (2023) conducted an experiment with 53 participants: 18 and 19 from two experimental groups and 16 from the control group. The experimental groups included students who interacted with an AI gamified model, while the control group was taught with traditional practices. The results show that the gamified AI model significantly improved students' learning outcomes, motivation, flow experience, problem-solving tendency, and reduced the cognitive load of learning, compared with the control group.

Beuran *et al.* (2023) discuss two AI-driven applications in cybersecurity education and training - a field that, compared to domains like threat detection or risk prediction, has received limited attention from an AI perspective. First, they introduce the AutoPentest-DRL framework, which employs Deep Reinforcement Learning to automate penetration testing, supporting the hands-on study of offensive security techniques. Second, the CyATP platform applies Natural Language Generation to create cybersecurity awareness content automatically, using sources such as Wikipedia and DBpedia. The platform integrates gamified learning tools, including quizzes and crossword puzzles, to engage non-technical users in foundational cybersecurity concepts.

As presented above, combining AI and gamification can create a powerful tool for increasing student engagement, enhancing motivation, and creating meaningful learning experiences. Still, the synergy between these two strategies has been documented in few literature articles and is still in its early stages of academic exploration.

To address that gap, our article proposes an investigation of both students' and professionals' perspectives on the implementation of AI and gamification (either separately or in combination) within university-level education and professional/organizational contexts, respectively.

3. RESEARCH DESIGN AND METHODOLOGY

For our study we used a mixed research approach, combining quantitative and qualitative techniques. For the quantitative component, we applied a Google Forms survey among students enrolled in information security courses at the Faculty of Economics and Business Administration, Alexandru Ioan Cuza University of Iași, Romania, and cybersecurity specialists. The Likert-scale items refer to the perceived utility of AI, gamification and combined elements introduced in teaching or learning techniques. We defined utility as the capacity to contribute to a better understanding of the content, the improvement of practical skills, increased student engagement, and the alignment of the course with current industry requirements. The scale used in the survey ranged from 1 to 5 (not at all useful, slightly useful, moderately useful, useful, very useful).

The items evaluated are:

- ***For AI**:* Study Unit: Introduction to AI; Study Unit: Fundamentals of Machine Learning (ML); Study Unit: Applications of AI and ML in Cybersecurity; Study Unit: Ethical and Social Implications of AI; Project: AI Solutions in Cybersecurity; AI Assistance in the Discussion of Cybersecurity Scenarios; Capture-the-Flag activities, defence simulations, blue/red team exercises in hybrid (human-AI) teams; Use of an educational chatbot to answer course content-related questions; Automated generation of test questions based on course materials; Automatic detection of AI-generated content in student projects – as identified in (Dwight 2023; Maennel and Maennel, 2024; Tummala and Bottomley, 2024).
- ***For gamification***: Progress tracking elements (progress bar/circle, checklist, roadmap, timeline, etc.); Rewards (badges, trophies, medals, certificates, other benefits, etc.); Points; Avatars; Stories/Narratives/Scenarios; Leaderboards. These elements were chosen based on the literature review, taking into consideration the most known, used and trending ones;
- ***For AI and gamification combined***: Use of applications/platforms that combine AI and gamification during teaching sessions; Automatic creation of personalized gamified activities for each student using AI; Adjustment of difficulty level, tasks, or rewards based on students' performance, automatically analysed by an AI system.

In the qualitative component of the study, an open question was meant to reveal the respondents' own perspective on the preferred AI/gamification/both elements to be used in their learning endeavour. By providing an answer to the question ("*Propose ways in which AI and gamification could be incorporated (separately and/or together) into course and seminar/laboratory activities for cybersecurity/information security subjects (university level)*"), participants were encouraged to reflect upon the innovative ways of teaching and learning. Their

responses offer insight into emerging trends, personal preferences regarding learning and teaching processes, and highlight potential implementation strategies.

The survey was addressed to: (1) undergraduate students who pursued information security courses and laboratories, and (2) specialists in the information security field.

(1) The students were enrolled in one of two specializations within the Faculty of Economics and Business Administration at Alexandru Ioan Cuza University of Iași: Accounting and Management Information Systems (2nd year) and Economic Informatics (3rd year). Both specializations include courses in information security: Protection and Security of Information Systems (for the former) and Information Systems' Security (for the latter).

(2) The specialists are professionals with information and cyber-security backgrounds, currently working in the private and/or academic sectors. They hold roles such as Software Solution Manager, Legal Advisor, Ethical Hacker, and Cybersecurity Consultant, with experience ranging from 1 to 20 years.

The survey was distributed to all students enrolled in the two previously mentioned specializations. The participation was voluntary, and the survey was made available via the institutional Microsoft Teams platform. It was also briefly introduced during the course sessions, with the goal of inviting them to respond. There was no restrictive selection criteria applied. The nature of the recruitment process (non-random and based on accessibility) classifies the sample as a convenience sample. Even though it is not statistically representative of a broader population, it offers relevant perspectives within the context of students studying information security in business-related programs at the undergraduate level. Regarding the information security specialists, they did not disclose their institutional affiliations.

We had a total of 149 students who responded to the survey, while only 4 specialists participated.

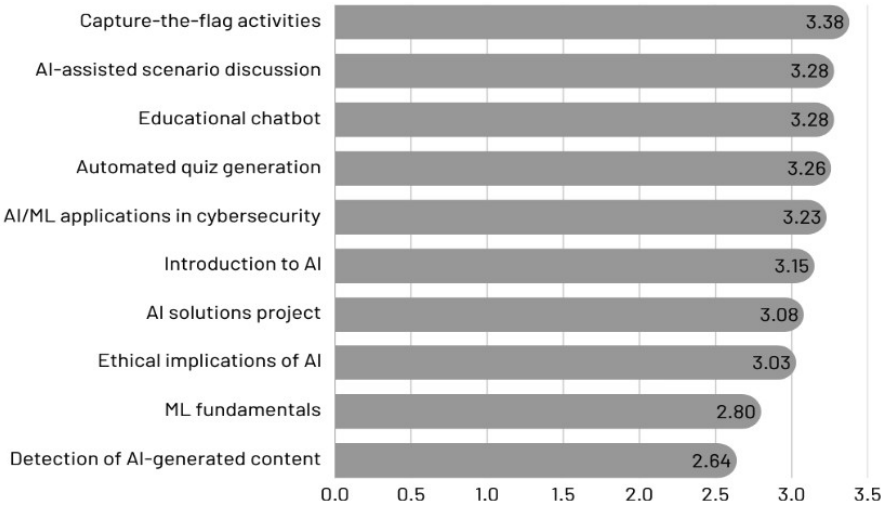
4. RESULTS AND DISCUSSION

This section presents the results of both quantitative and qualitative analyses, based on the responses gathered through surveys administered to students and specialists survey. For the quantitative part, we recoded the data from 0 to 4 for the purpose of statistical processing in Microsoft Excel. This technique did not affect the interpretation of the results.

To explore their preferences and perceptions, mean scores were calculated for each item, and open-ended responses were thematically analysed.

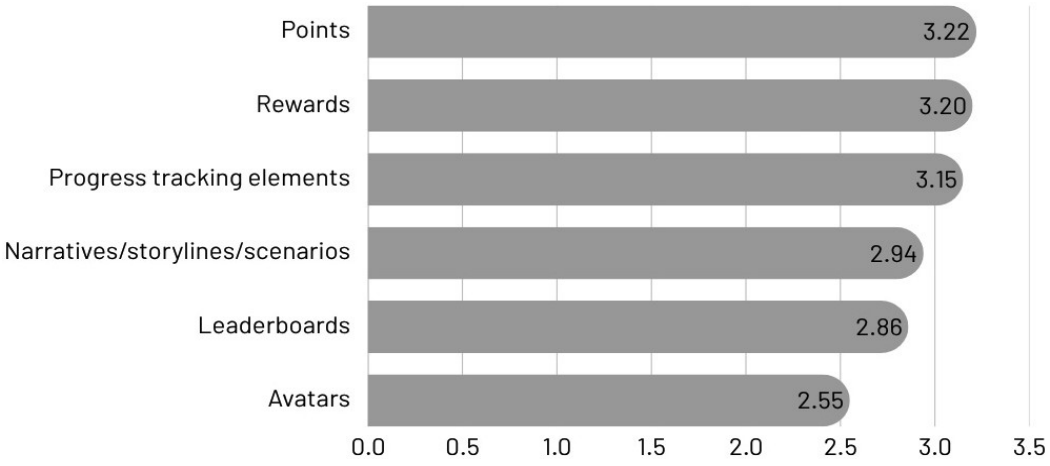
4.1. Quantitative analysis of survey results

The most appreciated AI-supported learning activity was the Capture-the-Flag exercise, with a mean score of 3.38, followed by AI-assisted scenarios and the use of educational chatbots, both scoring 3.28 (Figure 1). These results possibly suggest a strong preference for interactive and applied activities. Automated test generation (3.26), AI-supported cybersecurity activities (3.23), and general AI topics (3.15) were also positively received. In contrast, items such as machine learning fundamentals (2.80) and AI-generated content detection in student work (2.64) were rated lower, possibly due to perceived complexity or concerns over control and surveillance (Figure 1).



Source: own representation

Figure 1. Students' perceived utility of AI elements



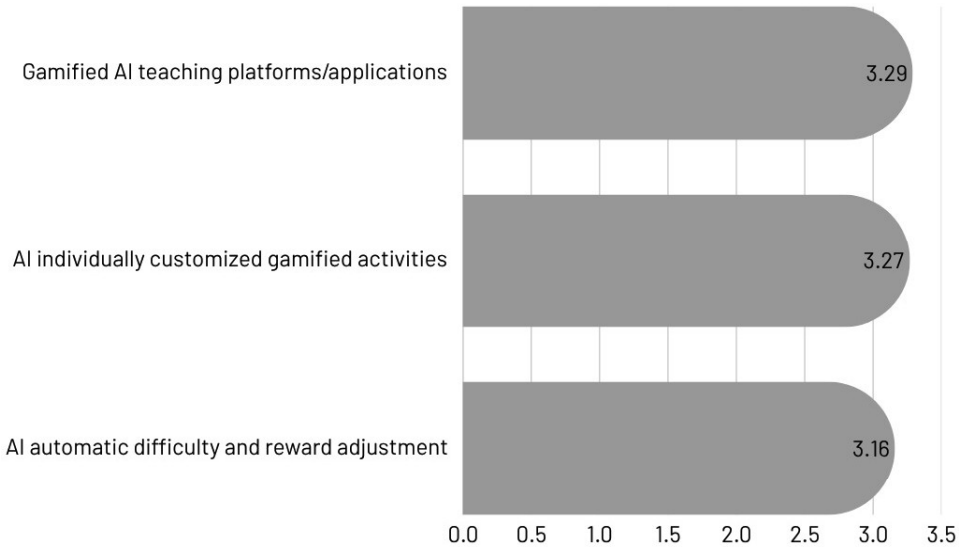
Source: own representation

Figure 2. Students' perceived utility of gamification elements

When evaluating classical gamification elements, students gave the highest scores to points (3.22), rewards (3.20 – e.g., badges, trophies, certificates), and progress tracking systems (3.15) (Figure 2). These findings reflect continued appreciation for traditional motivational mechanisms based on clear feedback and progress. Elements like avatars (2.55) and leaderboards (2.86) received the lowest ratings, suggesting that personalization and competitive ranking are less motivating in this context. Narrative elements such as storylines and scenarios were rated slightly above average (2.94), indicating a moderate interest in contextualized learning (Figure 2).

Students expressed particularly positive views toward the integration of AI into gamified educational platforms. Gamified AI-based teaching systems received the highest rating (3.29), followed by automatically personalized activities (3.27) and adaptive adjustments of difficulty and rewards (3.16) (Figure 3). This highlights a clear preference for systems that combine intelligent automation with motivational design, offering both personalization and engagement.

Overall, the results show a consistent pattern: students value educational tools that enhance interactivity, personalization, and adaptability. Traditional elements such as points and rewards remain relevant, while features perceived as symbolic or non-functional tend to be rated lower. These insights may support the development of future AI-enhanced gamification strategies tailored to learners' actual preferences.

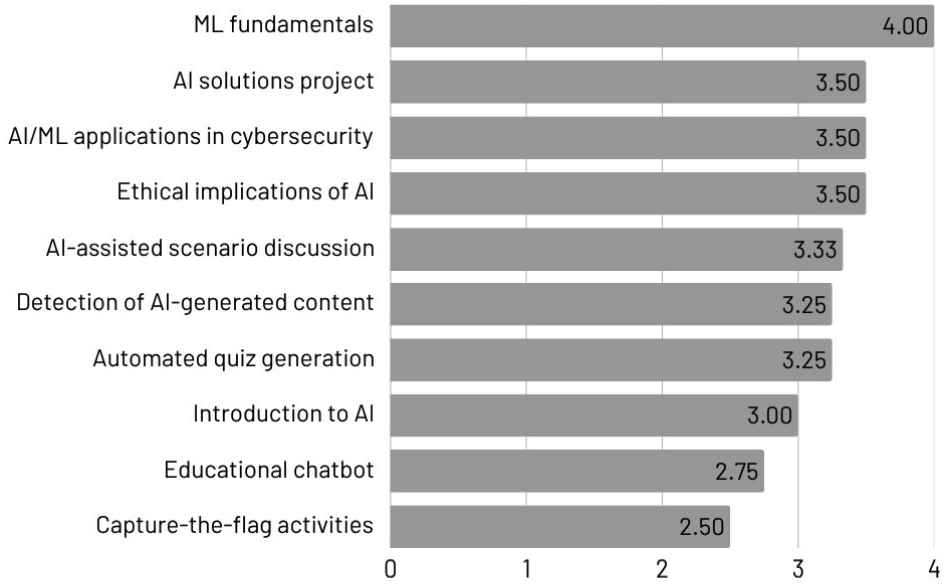


Source: own representation

Figure 3. Students' perceived utility of AI and gamification elements

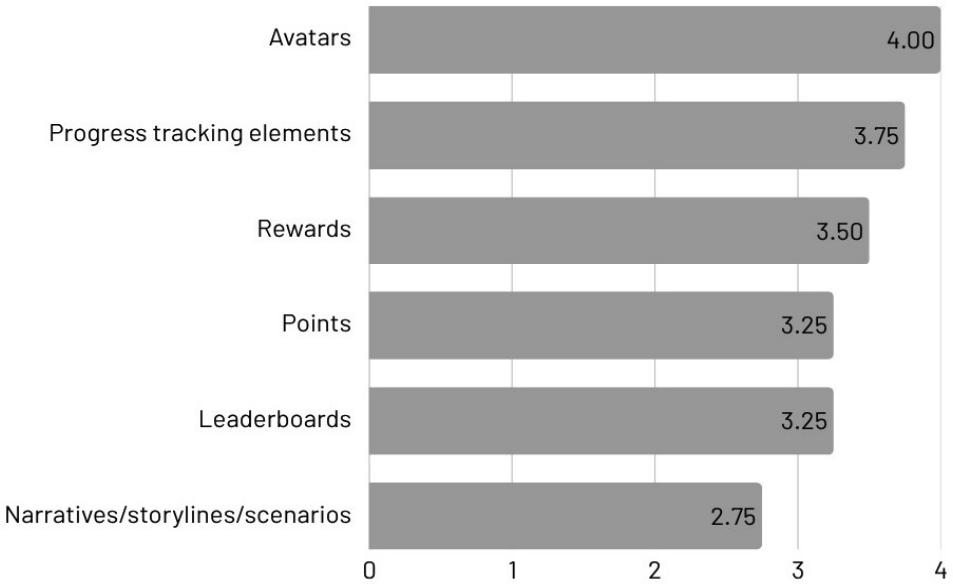
The responses provided by cybersecurity specialists offer an alternative perspective on the perceived utility of AI and gamification elements in education.

Like students, specialists evaluated each item on a scale from 0 to 4, and the results are represented using bar charts.



Source: own representation

Figure 4. Specialists' perceived utility of AI elements



Source: own representation

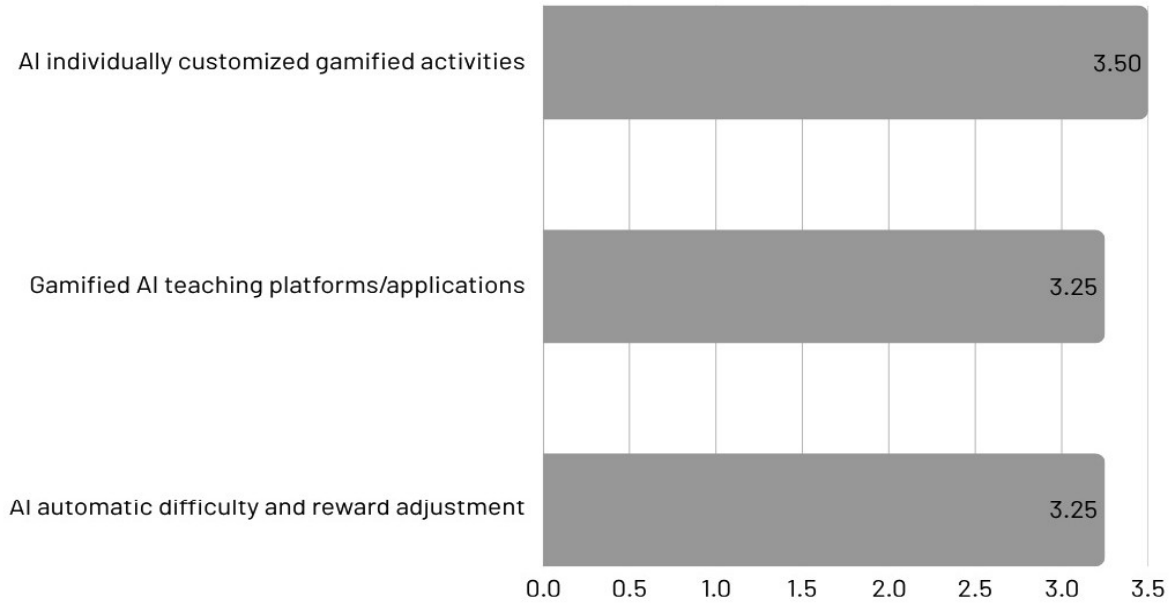
Figure 5. Specialists perceived utility of gamification elements

In terms of AI-related educational elements, the highest rating was given to machine learning fundamentals, which received a perfect score of 4.00 (Figure 4). AI solutions projects, ethical implications of AI, and AI/ML applications in

cybersecurity were also highly appreciated, each with an average score of 3.50. These results reflect a strong alignment with the specialists' technical background and their interest in ethical and applied aspects of AI. Other elements such as AI-assisted scenario discussions and automated content detection received moderate scores (Figure 4). Interestingly, Capture-the-Flag activities, which were rated highest by students, received the lowest rating among specialists (2.50), suggesting different priorities in evaluating practical applications.

When it comes to traditional gamification components, avatars received the highest score (4.00), followed by progress tracking elements (3.75), and rewards (3.50) (Figure 5). This indicates that specialists may value personalization and structured feedback systems more than students. Points and leaderboards were both rated at 3.25, while narratives and storylines received the lowest score (2.75), reinforcing a lower perceived relevance for narrative-driven learning among this group (Figure 5).

In terms of AI-supported gamification, specialists rated individually customized gamified activities highest (3.50), followed by AI-based teaching platforms and adaptive difficulty/reward systems, both at 3.25 (Figure 6). These results confirm that experts recognize the potential of AI to personalize and optimize the learning process through gamified elements, although their enthusiasm appears more tempered compared to student responses.



Source: own representation

Figure 6. Specialists perceived utility of AI and gamification elements

Overall, the results suggest that specialists place greater emphasis on foundational AI concepts, personalization, and structured feedback mechanisms.

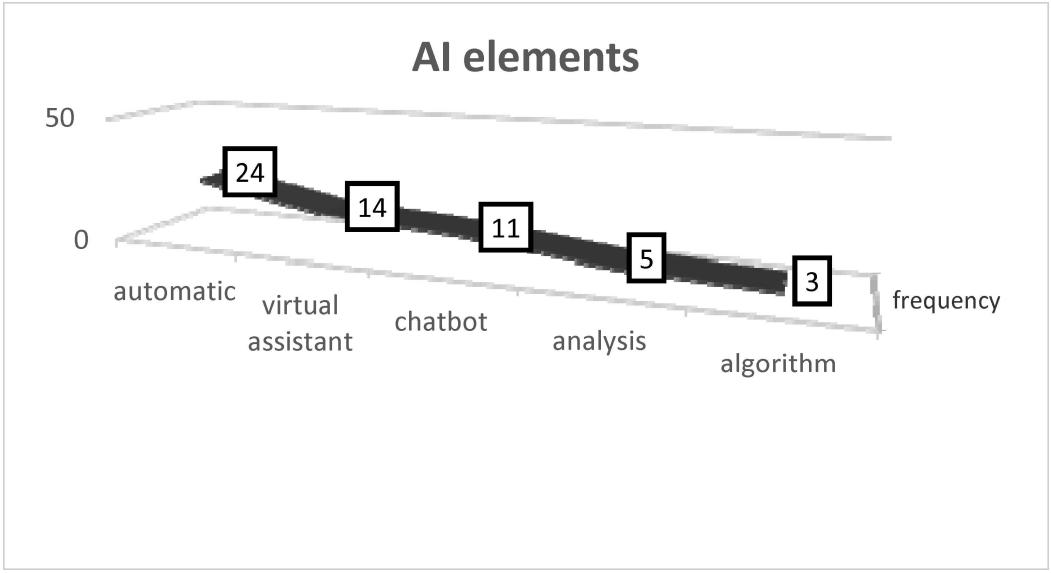
While they acknowledge the value of gamification and adaptive systems, their preferences are shaped by practical, technical, and ethical considerations rather than by interactivity or game-like experiences alone.

4.2. Key themes identified in qualitative responses

To gain a more detailed understanding of the thematic directions proposed by students, three charts were developed to synthesize the frequency of key terms extracted from open-ended responses. These terms were grouped into three categories: AI elements, gamification elements, and areas or activities within the field of information security where students would like to see these elements implemented, either separately or in combination.

The most frequently mentioned terms related to AI were "automatic/automation" (n = 24), "virtual assistant" (n = 14), and "chatbot" (n = 11) (Figure 7). This reflects a strong interest in interactive and automated tools that could support the learning process. Although the term "artificial intelligence" appeared 57 times in the responses, it was excluded from the chart due to its overly general usage, which would not contribute meaningfully to the analysis (Figure 7).

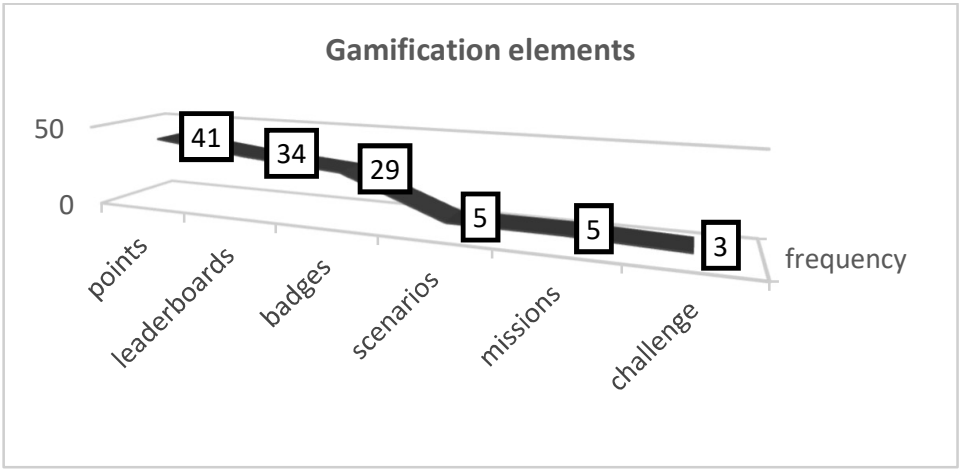
The emphasis on assistants and chatbots suggests a desire for continuous, on-demand support during the learning process. Moreover, the frequent reference to automation implies that students value efficiency and responsiveness in how content is delivered and personalized.



Source: own representation

Figure 7. Frequency of AI-related terms used by students

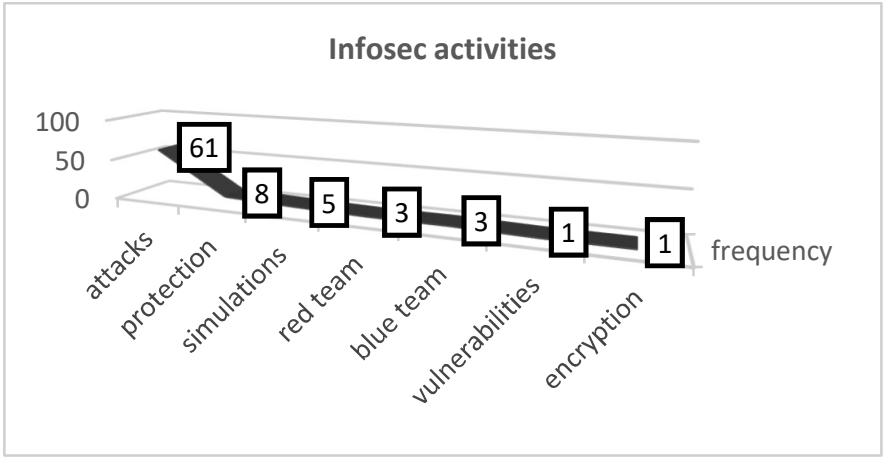
Gamification-related terms were dominated by familiar mechanics such as "points" (n = 41), "leaderboards" (n = 34), and "badges" (n = 29) (Figure 8). These terms suggest that students are used to reward and progress tracking systems and perceive them as helpful for maintaining engagement and motivation. Similar to the case of AI, the word "gamification" was mentioned frequently (n = 88) but was intentionally omitted from the visualization (Figure 8).



Source: own representation

Figure 8. Frequency of gamification-related terms used by students

In terms of security-focused activities, students showed a clear inclination toward practical scenarios. The term "attacks" was by far the most mentioned (n = 61), followed by "protection" (n = 8), "simulation" (n = 5), "red/blue team" (n = 6), and less frequently "vulnerabilities" and "encryption" (n = 1 each) (Figure 9). This suggests a desire to see both AI and gamified approaches applied to realistic, scenario-based cybersecurity education.



Source: own representation

Figure 9. Frequency of gamification-related terms used by students

In their open responses, students often linked gamification to mechanisms such as points, leaderboards, badges, missions, and scenarios. These tools were seen as means of tracking progress, staying motivated, and receiving rewards.

AI was frequently described as a valuable tool for personalized learning. Students mentioned the usefulness of chatbots and virtual assistants to answer questions at any time, underlining AI's potential to provide immediate feedback and ongoing support.

The combination of AI and gamification was one of the most referenced ideas in the responses. Approximately 100 out of 149 answers made simultaneous mention of both, indicating high interest and expectations regarding their integration into university-level cybersecurity education.

Overall, most responses reflect a desire for a more practice-oriented, interactive, and engaging learning process, enabled either by gamification, AI, or an integration of both.

Specialists have proposed a series of pedagogical innovations that combine AI with gamification strategies to enhance cybersecurity education at the university level. These proposals can be categorized into four primary thematic areas:

1. AI supported scenario development

Experts suggest leveraging AI, particularly large language models (LLMs), to assist instructors in designing complex, realistic cybersecurity scenarios. These include the generation of vulnerable code, the creation of adaptive challenges for laboratory exercises, and the development of competition-style environments tailored to student skill levels.

2. Gamified reward and motivation systems

Specialists advocate for the integration of gamification elements such as point-based systems and digital badges (e.g., "Ethical Hacker") to reinforce student motivation. These systems are intended to recognize progress and performance, fostering sustained engagement through virtual rewards and performance-based feedback mechanisms.

3. Interactive and role-based learning activities

A key proposal involves the use of interactive platforms (most notably Capture the Flag (CTF) environments) and the implementation of structured team-based games. In these activities, students assume defined roles such as attackers or defenders, simulating real-world cybersecurity operations in a collaborative learning context.

4. AI driven cyberattack simulations

Finally, specialists recommend using AI to simulate various types of cyber threats, including phishing attacks, malware propagation, and distributed denial-of-service (DDoS) scenarios. These simulations aim to expose students to realistic threat conditions and improve their ability to detect, analyse, and respond to cyber incidents.

5. LIMITATIONS

While the study provides valuable insights into the integration of AI and gamification in cybersecurity education, several limitations should be noted.

The number of specialist respondents was low, which narrows the range of expert perspectives represented in the analysis. Additionally, the study did not include empirical validation of the proposed methods, relying instead on participant feedback and perceived usefulness.

Among the surveyed students, the response rate was approximately 70%, indicating a satisfactory level of engagement but leaving room for potential response bias.

The design of the survey may have also influenced the nature of the qualitative data: since participants were first presented with Likert-scale questions rating the utility of specific AI and gamification elements, their subsequent open-ended responses may have reflected those predefined examples rather than introducing entirely original ideas. As a result, the creative scope of some responses may have been limited by the structure of the survey itself.

6. CONCLUSIONS

The findings of this study highlight a clear preference among students for educational technologies that combine adaptive, personalized support with motivational structures derived from gamification. Quantitative results show that both AI-enhanced tools and classical gamification elements are perceived as valuable, especially when they contribute directly to learning outcomes and engagement. While students showed strong enthusiasm for interactive elements like chatbots, simulations, and AI-assisted tasks, more symbolic features such as avatars or leaderboards were viewed as less effective.

In contrast, specialists emphasized foundational AI knowledge, structured feedback, and personalization, placing less importance on interactive or game-like experiences. This divergence may reflect their more practical and professional orientation, grounded in technical and ethical considerations.

The qualitative data reinforced these insights, revealing recurring references to automation, virtual assistance, and familiar gamification mechanisms. Students recognized the utility of these tools and expressed a desire for their integration into realistic cybersecurity training scenarios.

Overall, the results support the potential of integrating AI and gamification into higher education, especially in fields such as information security, where practice-oriented and dynamic learning environments are essential. Future implementations should focus on balancing personalized automation with engaging motivational elements, aligning technological innovation with pedagogical value.

References

1) Arteaga, D. and Granados Guzmán, B. (2024). *Using AI to create engaging educational games for humanities students*, *THE Campus Learn, Share, Connect*. [online] Available at: https://www.timeshighereducation.com/campus/using-ai-create-engaging-educational-games-humanities-students [Accessed: 25.06.2025].
2) Batista, J., Mesquita, A. and Carnaz, G. (2024). Generative AI and Higher Education: Trends, Challenges, and Future Directions from a Systematic Literature Review. *Information*, 15(11), p. 676. https://doi.org/10.3390/info15110676.
3) Beuran, R., Zhenguo H., Youmeizi Z. and Yasuo, T. (2023). Artificial Intelligence for Cybersecurity Education and Training. In: T. Sipola, T. Kokkonen and M. Karjalainen (eds.), *Artificial Intelligence and Cybersecurity*, pp. 103–23. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-15030-2_5.
4) Cambridge Dictionary (2025). *gamification*. [online] Available at: https://dictionary.cambridge.org/dictionary/english/gamification [Accessed: 5.06.2025].
5) Christopoulos, A. and Mystakidis, S. (2023). Gamification in Education, *Encyclopedia*, 3, pp. 1223–1243. https://doi.org/10.3390/encyclopedia3040089.
6) Copeland, B.J. (2025). *Artificial intelligence (AI) | Definition, Examples, Types, Applications, Companies, & Facts | Britannica*. [online] Available at: https://www.britannica.com/technology/artificial-intelligence [Accessed: 25.06.2025].
7) Dice Staff (2024). *Cybersecurity Hiring Likely to Pick-Up in 2025, But Challenges Remain*, *Dice Insights*. [online] Available at: https://www.dice.com/career-advice/cybersecurity-hiring-likely-to-pick-up-in-2025-but-challenges-remain [Accessed: 25.06.2025].
8) Dwight, J. (2023). Collaborate, Design, and Generate Cybercrime Script Tabletop Exercises for Cybersecurity Education, *International Conference on Computers in Education*. https://doi.org/10.58459/icce.2023.1406.
9) European Union Agency for Cybersecurity (ENISA) (2023). *ENISA Threat Landscape 2023*. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [Accessed: 25.06.2025].
10) Fourrage, L. (2025). *How is the Cybersecurity job market expected to evolve in 2025?*, *Nucamp*. [online] Available at: https://www.nucamp.co/blog/coding-bootcamp-cybersecurity-2025-how-is-the-cybersecurity-job-market-expected-to-evolve-in-2025 [Accessed: 25.06.2025].
11) Hamari, J. (2019). Gamification. In: *The Blackwell Encyclopedia of Sociology*. John Wiley & Sons, Ltd, pp. 1–3, https://doi.org/10.1002/9781405165518.wbeos1321.
12) Holdsworth, J. and Kosinski, M. (2024). *What Is Information Security? | IBM*. [online] Available at: https://www.ibm.com/think/topics/information-security [Accessed: 9.06.2025].
13) Kelly, J. (2025). *Here Are The Top 5 Skills To Learn In 2025*, *Forbes*. [online] Available at: https://www.forbes.com/sites/jackkelly/2024/12/31/here-are-the-top-5-hard-skills-to-learn-in-2025/ [Accessed: 25.06.2025].
14) Lee, D. *et al.* (2024). The impact of generative AI on higher education learning and teaching: A study of educators perspectives, *Computers and Education: Artificial Intelligence*, 6, p. 100221. https://doi.org/10.1016/j.caeai.2024.100221.

15) Li, M., Ma, S. and Shi, Y. (2023). Examining the effectiveness of gamification as a tool promoting teaching and learning in educational settings: a meta-analysis, *Frontiers in Psychology*, 14, p. 1253549. https://doi.org/10.3389/fpsyg.2023.1253549.
16) Limonova, V. *et al.* (2023). The Research Context of Artificial Intelligence and Gamification to Improve Student Engagement and Attendance in Higher Education, *Journal of Distance Education and eLearning,* https://doi.org/10.34627/REDVOL6ISS2E202309.
17) Maennel, K. and Maennel, O.M. (2024). Human-AI Collaboration and Cyber Security Training: Learning Analytics Opportunities and Challenges. In: *2024 17th International Conference on Security of Information and Networks (SIN)*, Sydney, Australia: IEEE, pp. 01–08. https://doi.org/10.1109/SIN63213.2024.10871610.
18) Meineke, M. (2024). *The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap*, *World Economic Forum*. [online] Available at: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/ [Accessed: 25.06.2025].
19) Merriam-Webster (2025). *Definition of cybersecurity*. [online] Available at: https://www.merriam-webster.com/dictionary/cybersecurity [Accessed: 9.06.2025].
20) Özdemir, O. (2025). Kahoot! Game-based digital learning platform: A comprehensive meta-analysis. *Journal of Computer Assisted Learning*, 41(1), p. e13084. https://doi.org/10.1111/jcal.13084.
21) Robert, J. (2024). *The Future of AI in Higher Education*, *EDUCAUSE*. [online] Available at: https://www.educause.edu/ecar/research-publications/2024/2024-educause-ai-landscape-study/the-future-of-ai-in-higher-education [Accessed: 24.06.2025].
22) Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, 215, pp. 483–487. https://doi.org/10.1016/j.procs.2022.12.050.
23) Tan, D.Y. and Cheah, C.W. (2021). Developing a gamified AI-enabled online learning application to improve students' perception of university physics, *Computers and Education: Artificial Intelligence*, 2, https://doi.org/10.1016/j.caeai.2021.100032.
24) Tummala, V. and Bottomley, K. (2024). Empowering AI Leaders: Educational Modules for Developing Core Competencies in Ethical AI and Cybersecurity. In: *Proceedings of the LA 2024International Leadership Association ILA2024. November 7-10, 2024.* Chicago, Illinois.
25) Won, M. *et al.* (2024). A Cybersecurity Summer Camp for High School Students Using Autonomous R/C Cars. In: *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1. SIGCSE 2024: The 55th ACM Technical Symposium on Computer Science Education*, Portland OR USA: ACM, pp. 1435–1441. https://doi.org/10.1145/3626252.3630758.
26) Yang, Q.-F., Lian, L.-W. and Zhao, J.-H. (2023). Developing a gamified artificial intelligence educational robot to promote learning effectiveness and behavior in laboratory safety courses for undergraduate students. *International Journal of Educational Technology in Higher Education*, 20(1), p. 18. https://doi.org/10.1186/s41239-023-00391-9.

27) Zeng, J. *et al.* (2024). Exploring the impact of gamification on students' academic performance: A comprehensive meta-analysis of studies from the year 2008 to 2023. *British Journal of Educational Technology*, 55(6), pp. 2478–2502. https://doi.org/10.1111/bjet.13471.
28) Zia, U. and Noor, K. (2024). The synergy of gamification and artificial intelligence: Enhancing student engagement and learning outcomes in educational environments. *EasyChair Preprint* No. 15392.
29) Zourmpakis, A.-I., Kalogiannakis, M. and Papadakis, S. (2023). Adaptive Gamification in Science Education: An Analysis of the Impact of Implementation and Adapted Game Elements on Students Motivation', *Computers*, 12(7), p. 143. https://doi.org/10.3390/computers12070143.