**Hackers vs Universities: Workshop takeaways and next steps**

The ECSS 2026 workshop “Hackers vs Universities: Who Trains Better Cyber Talent?”, held on 27 October 2026, explored how universities and informal learning environments can work together to develop cybersecurity talent.

The interactive panel featured Jonas Čeponis, Kaunas University of Technology, Lithuania; Birgy Lorenz, Senior Research Fellow, Tallinn University of Technology, Estonia; Muhammad Mudassar Yamin, NTNU, Norway; and Jens Myrup Pedersen, Aarhus University, Denmark. Gert Jervan, Tallinn University of Technology, moderated the session, engaging the audience through live Mentimeter polls, quizzes and Q&A.

**The main message was clear: respondents favour universities working with cyber communities, combining strong theoretical foundations with practical experience. They also expect universities to take a clear lead in teaching the critical use of AI.**

**Key takeaways (on a scale 0-5):**

- **Preserve strong foundations while updating curricula faster.** Respondents valued the theoretical foundations provided by universities, with an average agreement score of **4.0**, while the statement that curricula keep pace with developments scored **2.5**. These responses suggest retaining foundational knowledge while renewing practical content more frequently. Respondents also strongly supported preparing students to challenge current industry practices, which scored **4.7**.
- **Use CTF achievements as one part of a broader assessment of ability.** The statement that a strong Capture the Flag record reveals more about practical ability than university grades scored **4.0**. However, respondents also recognised that competitions can reward speed over careful investigation, scoring this statement **3.9**. Competitions should therefore sit alongside realistic tasks that assess investigation, documentation and communication.
- **Keep pathways open to beginners.** The statement that students without prior hacking experience have a fair chance to succeed in university cybersecurity programmes scored **4.4**. This supports maintaining accessible entry routes and ensuring that previous competition experience does not become an informal prerequisite.
- **Develop AI capabilities while checking independent understanding.** Respondents recognised that AI can accelerate beginners’ learning (**4.1**) but expressed stronger concern that it can conceal gaps in understanding (**4.6**). Support for demonstrating core cybersecurity skills without AI before assessment with AI tools scored **4.4**. Assessment should establish whether learners can explain, verify and independently demonstrate their knowledge.

© Informatics Europe, 2026, CC BY-SA 4.0 

- **Make critical evaluation of AI an explicit learning outcome.** University responsibility for teaching students to evaluate AI-generated cybersecurity advice received the highest average agreement score, **4.8**. The AI skills word cloud also highlighted **agentic AI** and **cybersecurity for AI**, pointing to the importance of understanding and securing AI systems alongside using AI in cybersecurity work.
- **Build closer university–community partnerships.** The statement that joint programmes would develop stronger talent than universities or informal communities working alone scored **4.1**. Shared mentoring and practical challenges offer concrete opportunities to connect their strengths.

The talent word cloud prominently featured **curiosity, creativity, persistence and thinking outside the box**. These responses suggest recognising potential through opportunities to explore and solve unfamiliar problems, alongside grades and knowledge of specific tools.

Expectations also changed across the career journey. Universities received the most selections for **finding talent (14)** and **upskilling talent (12)**, while industry associations led for **keeping employees' skills current (12)**. This suggests a continuing role for universities, with industry taking greater responsibility during employment.

These results reflect the views of workshop respondents. Agreement scores describe audience perceptions, while the responsibility questions allowed respondents to select up to three options.

**The principal next step: we are going to launch an Informatics Europe Working Group on Cybersecurity**

Building on these findings, **we are going to launch an Informatics Europe Working Group on Cybersecurity** to coordinate sustained cooperation across European informatics departments and connect them with cyber communities and industry.

The proposed group's initial priorities would be to:

1. **Develop joint learning opportunities.** Support university–community partnerships offering mentoring, practical challenges and accessible pathways for both beginners and advanced learners.
2. **Strengthen curricula and assessment.** Exchange approaches that combine theoretical foundations with realistic cybersecurity tasks, including careful investigation and clear explanations. Develop assessment practices that establish competence both with and without AI assistance.

© Informatics Europe, 2026, CC BY-SA 4.0 

3. **Share reusable resources across Europe.** Bring together teaching materials, exercises and examples of effective talent development, drawing on relevant initiatives such as CyberHubs and cybersecurity competition communities.
4. **Evaluate and share what works.** Encourage participating institutions to pilot approaches and report evidence about learning, participation and progression into professional practice.

We thank the panellists and everyone who contributed. We invite colleagues across the European informatics community to help shape this proposed working group and contribute their experience, resources and ideas.