# 3rd International Workshop on Cyber Security Education for Industry and Academia (CSE4IA 2025)

Vita Santa Barletta[1,†], Federica Caruso[2,*,†], Francesco Greco[1,†], Manuel Angel Serrano[3,†], Hannan Xiao[4,†] and Chaminda Alocious[5,†]

[1]*University of Bari, Via Orabona 4, 70125 Bari, Italy*
[2]*University of L'Aquila, Via Vetoio 1, 67100 L'Aquila, Italy*
[3]*University of Castilla-La Mancha, Paseo de la Universidad 4, 13071, Ciudad Real, Spain*
[4]*King's College London, Strand Campus, Bush House, 30 Aldwych, London, WC2B 4BG*
[5]*University of Hertfordshire, College Ln, Hatfield AL10 9AB*

## Abstract

Cybersecurity education faces significant challenges due to evolving digital threats and a shortage of skilled professionals. Bridging industry, academia, and public administration is crucial for developing innovative training methods and tools that equip students, professionals, and non-experts with the skills needed to effectively address cybersecurity risks. Based on previous editions' success, CSE4IA 2025 will explore how end-user development (EUD), AI-driven learning, and low-code/no-code approaches can enhance cybersecurity education. The workshop will bring together researchers and practitioners to discuss user-centered learning environments that help end-users understand and mitigate security risks. By fostering interdisciplinary collaboration, CSE4IA 2025 seeks to redefine cybersecurity education with innovative, user-friendly solutions that strengthen security awareness and resilience. By offering a dynamic, multidisciplinary platform, the workshop will showcase cutting-edge educational tools and methodologies, empowering both professionals and everyday users to navigate cybersecurity risks in an increasingly digital world confidently.

## Keywords

Cybersecurity, Education, Learning, Training, CSE4IA

## 1. Introduction

The rapid integration of digital technologies has led to a significant rise in cyber threats, from personal data breaches to large-scale attacks on critical infrastructure. These threats, often driven by criminal intent for financial gain or disruption, continue to grow in both frequency and sophistication. While technological countermeasures lay the foundations for cybersecurity, the human element still has a major impact for the success of most cyberattacks [1]. Therefore, organizations should prioritize cybersecurity education, which must go beyond training skilled professionals and must rather address the broader challenge of public awareness.

At the same time, the global job market faces an urgent supply and demand gap in cybersecurity recruitment. The increase in cyber-attacks has intensified the need for qualified professionals, yet traditional education and training programs struggle to keep pace with evolving industry demands. Organizations such as ENISA (European Union Agency for Cybersecurity) emphasize the need for a standardized understanding of cybersecurity roles, competencies, and career pathways. However, more effort is needed to bridge the gap between academic training and real-world business needs, ensuring that professionals and end-users alike develop the necessary skills to mitigate cybersecurity risks effectively.

*Joint Proceedings of IS-EUD 2025: 10th International Symposium on End-User Development, 16-18 June 2025, Munich, Germany.*

[*] Corresponding author.

[†] These authors contributed equally.

vita.barletta@uniba.it (V. S. Barletta); federica.caruso1@univaq.it (F. Caruso); francesco.greco@uniba.it (F. Greco); manuel.serrano@uclm.es (M. A. Serrano); hannan.xiao@kcl.ac.uk (H. Xiao); chamindaucsc@gmail.com (C. Alocious)
0000-0002-0163-6786 (V. S. Barletta); 0000-0002-6167-3896 (F. Caruso); 0000-0003-2730-7697 (F. Greco); 0000-0003-0962-5659 (M. A. Serrano); 0000-0003-2273-6679 (H. Xiao)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

To tackle these challenges, cybersecurity education must embrace innovative approaches that combine technological advancements with practical, hands-on learning [2, 3]. Interactive methods such as Artificial Intelligence-powered training tools, gamified learning experiences, and immersive simulations can enhance skill development by providing realistic cybersecurity scenarios. These approaches not only strengthen professional training but also make complex security concepts more intuitive for non-expert users. Furthermore, as digital transformation accelerates, ensuring that both public and private sector employees are equipped to securely manage sensitive data is crucial. A modern cybersecurity education framework should therefore integrate these advancements to create more effective, accessible, and engaging learning environments.

The 3rd International Workshop on Cyber Security Education for Industry and Academia (CSE4IA 2025) continues the mission of its previous editions [4, 5] by offering a collaborative platform for researchers and practitioners to discuss innovative educational strategies. Co-located with IS-EUD 2025, the workshop will explore how End-User Development (EUD), Human-Computer Interaction (HCI) principles, and emerging technologies, such as Artificial Intelligence (AI) and Virtual Reality (VR), can create more engaging and effective cybersecurity learning environments. Special attention will be given to practical approaches that close the gap between cybersecurity education and real-world applications, equipping professionals and end-users with the necessary skills to navigate today's complex digital landscape.

As in previous editions [4, 5], CSE4IA 2025 aims to redefine cybersecurity education by fostering interdisciplinary collaboration and promoting user-centered training solutions. The workshop will provide a dynamic, multidisciplinary platform for sharing cutting-edge tools and methodologies, empowering both professionals and everyday users to confidently manage cybersecurity risks in an increasingly digital world. We invite researchers, educators, and industry experts to contribute with innovative research, case studies, and best practices that shape the future of cybersecurity education, ensuring a more secure and resilient digital ecosystem for all.

## 2. Topics of Interest

The topics of interest for the 3rd International Workshop on CyberSecurity Education for Industry and Academia (CSE4IA 2025) include, but are not limited to:

- AI-powered tools for Cybersecurity Education
- Generative AI in Cybersecurity Education
- Explainable AI for Cybersecurity Education
- Augmented Reality (AR) and Virtual Reality (VR) for Cybersecurity Education
- Game-based approaches to Cybersecurity Education
- Artistic Approaches to Cybersecurity Education
- Designing Tools and Frameworks for Cybersecurity Education
- Contextual Methodologies for Cybersecurity Education
- Innovative Technologies for Professional Cybersecurity Competencies
- Explainable Security in Public Administration
- Human, Economic, Ethical, and Legal Aspects in Cybersecurity Education
- Innovative Training Programs for Cybersecurity Education
- Warning Dialogues for Cybersecurity Education
- Human Factors for Cybersecurity Education
- Case Studies on Challenges and Practices in Cybersecurity Education
- Data Visualization in Cybersecurity Education
- Accessibility in Cybersecurity educational tools
- User Behavior Analysis in Cybersecurity
- Personalized Learning in Cybersecurity Education

- Conversational Interface in Cybersecurity Education
- Approaches, methods, and techniques for enabling users to create, modify, and customize digital tools and systems while considering cybersecurity issues.
- Case studies and design implications on Cybersecurity issues and practices of end-user development

## 3. Workshop Format

The workshop will take place over a *single full day*. It will begin with an opening session, during which the organizers will welcome participants and outline the schedule.

This will be followed by a ***keynote*** designed to inspire and set the stage for the workshop's discussions. Then the ***presentation sessions*** will start and its schedule will vary based on the type of paper: (i) *Regular papers* (up to 10 pages, excluding references) will have 10 minutes for presentation and 5 minutes for discussion, while (ii) *Extended Abstracts* (up to 4 pages, excluding references) will have 7 minutes for presentation and 5 minutes for discussion. The number of presentation sessions will be tailored to the number and type of accepted submissions. After the presentation sessions, the workshop will culminate in a ***roundtable discussion*** featuring representatives from both academia and industry. This interactive session will explore the future of cybersecurity education, emphasizing innovative technologies, interdisciplinary collaboration, and industry-academia partnerships to address the skills gap. It aims to identify key challenges, opportunities, and actionable strategies, generating ideas to shape future research, policy, and educational practices, ensuring a forward-looking conclusion of CSE4IA 2025.

## 4. Workshop Participants

The target audience for CSE4IA is diverse, reflecting the multidisciplinary nature of cybersecurity education. It includes researchers in fields like computer science, technology-enhanced learning, education, and HCI, cybersecurity professionals from industry, policymakers, tech industry representatives interested in educational trends, and students in computer science and related fields seeking to enhance their skills. This diverse group will foster rich discussions and contribute to the advancement of cybersecurity education. We expect 15 to 35 attendees, invited through direct outreach to academics, industry professionals, and policymakers, and promoted via mailing lists, professional networks, social media, and a dedicated website (https://sites.google.com/view/cse4ia-2025).

## 5. Planned Outcomes of the Workshop

All submissions will undergo a rigorous double-blind peer-review process, focusing on originality, quality, soundness, and relevance, with each paper reviewed by three program committee members. Accepted submissions will be published in the CSE4IA 2025 workshop proceedings (CEUR-WS). As in the previous editions, authors of selected high-quality papers will be invited to submit extended versions for potential publication in a special issue of a leading international journal.

## 6. Workshop Organizing Committee

**Vita Santa Barletta** is an Assistant Professor at the Department of Computer Science at the University of Bari "Aldo Moro". Her research interests include cybersecurity, cyber social security, quantum software engineering, and secure software engineering. In the past, she organized the following workshops: the 1st and 2nd edition of CSE4IA; the 1st and 2nd edition of QP4SE (Quantum Programming for Software Engineering); the 2nd edition of CISE'23 (Computational Intelligence and Software Engineering).

**Federica Caruso** is a post-doc research fellow at the Department of Information Engineering, Computer Science and Mathematics (DISIM) of the University of L'Aquila (Italy). Her primary research interests are in Assistive Technology and Technology-Enhanced Learning. In particular, she is working on methodologies for designing Serious Games and Immersive Virtual Reality-based learning-oriented systems. In the past, she organized the 1st and 2nd edition of CSE4IA.

**Francesco Greco** is a Research fellow and third-year PhD student at the University of Bari "Aldo Moro", where he conducts research on the fields of Usable Security and Human-Centered Explainable AI with the Interaction, Visualization, Usability & UX (IVU) laboratory. During his PhD, he has also been a visiting student at King's College London in the Cybersecurity (CYS) group, under the supervision of Prof. Luca Viganò. He will serve as both the Publicity Chair and the Website Chair for CSE4IA 2025. In this role, he will handle workshop promotion and communication, as well as the creation and upkeep of the website.

**Manuel A. Serrano** is an Assistant Professor at the Escuela Superior de Informática, University of Castilla-La Mancha, Ciudad Real. Regarding his research interests, he is working on cyber security (especially in Big Data and the IoT), quantum software engineering, software quality, and measurement and business intelligence. His scientific production is large, having published more than 50 papers in high-level journals and conferences. He has participated in more than 20 research projects, has conducted several invited speeches, and has worked in several transfer projects with companies. In the past, he organized the following workshops: the 1st and 2nd edition of QP4SE (Quantum Programming for Software Engineering); the 1st edition of E-QSE (Empirical Studies for Quantum Software Engineering).

**Hannan Xiao** is a Senior Lecturer in Computer Science Education in the Department of Informatics, King's College London. She is a Senior Fellow of the Higher Education Academy (SFHEA). She obtained her PhD from the National University of Singapore, and completed her MEng and BEng from the Huazhong University of Science and Technology, China. Before joining King's College London, Hannan held positions as Principal Lecturer at the University of Hertfordshire, UK, Research Fellow at the National University of Singapore, and Assistant Professor at the Huazhong University of Science and Technology, China.

**Chaminda Alocious** is a former Network Security Researcher at the University of Herefordshire, UK, specializing in wireless network security. He obtained his Ph.D. in Network Security from the University of University, UK. Chaminda Alocious is a Senior Software Engineer for Deutsche Bank, UK with over decade of experience in the Software industry, and has specialized in building secure software systems for accessing confidential data and improving secure software design.

## 7. Workshop Program Committee

The program committee members will be selected from both senior and junior researchers working on the topics of CSE4IA 2025. This ensures a high-quality review process while also fostering the integration of junior researchers into the community.

Below is the list of CSE4IA 2025 program committee members:

- Mario Angelelli – University of Salento (Italy)
- Danilo Caivano – University of Bari (Italy)
- Dajana Cassioli – University of L'Aquila (Italy)
- Alessia Catalano - University of Salento (Italy)
- Mirko De Vincentiis - SER&P, University of Bari spin-off (Italy)
- Flaminia Del Conte – Hackable S.r.l. (Italy)
- Samuele Del Vescovo - IMT School Lucca (Italy)
- Giuseppe Desolda – University of Bari (Italy)
- Alessio Di Santo - University of L'Aquila (Italy)
- Leonardo Fazzini - University of L'Aquila (Italy)
- Ilenia Fronza – Free University of Bozen-Bolzano (Italy)

- Tasmina Islam – King’s College London (UK)
- Annita Larissa Sciacovelli – ENISA
- Antonio Piccinno – University of Bari (Italy)
- Valerio Rughetti – LUISS ”Guido Carli” (Italy)
- Walter Tiberti – University of L’Aquila (Italy)
- Luca Viganò – King’s College London (UK)

## Acknowledgments

This workshop is supported by SERICS (Security and Rights in CyberSpace) - CSS - Cyber Social Security, Spoke 3: Attacchi e Difesa(PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

## Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

## References

[1] Verizon, 2024 data breach investigations report, 2024. URL: https://www.verizon.com/business/resources/reports/dbir/#DBIR2024NR, http://www.xbow.com.

[2] V. S. Barletta, M. Calvano, F. Caruso, A. Curci, A. Piccinno, Serious games for cybersecurity: How to improve perception and human factors, in: 2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering, MetroXRAINE 2023 - Proceedings, 2023, p. 1110 – 1115. doi:10.1109/MetroXRAINE58569.2023.10405607.

[3] M. Calvano, F. Caruso, A. Curci, A. Piccinno, V. Rossano, A rapid review on serious games for cybersecurity education: Are “serious” and gaming aspects well balanced?, in: CEUR Workshop Proceedings - Joint Proceedings of the Workshops, Work in Progress Demos and Doctoral Consortium at the IS-EUD 2023 co-located with the 9th International Symposium on End-User Development (IS-EUD 2023), volume 3408, 2023.

[4] V. S. Barletta, D. Caivano, F. Caruso, S. Peretti, V. Rossano, Cybersecurity education for industry and academia - cse4ia, in: Joint Proceedings of the Workshops, Work in Progress Demos and Doctoral Consortium at the IS-EUD 2023, volume 3408 of *WWDD@IS-EUD 2023*, CEUR-WS, 2023. URL: https://ceur-ws.org/Vol-3408/short-s3-00.pdf.

[5] V. S. Barletta, F. Caruso, T. Di Mascio, F. Greco, T. Islam, V. Rossano, H. Xiao, Cybersecurity education for industry and academia (cse4ia 2024), in: Proceedings of the 2024 International Conference on Advanced Visual Interfaces, AVI ’24, Association for Computing Machinery, New York, NY, USA, 2024. URL: https://doi.org/10.1145/3656650.3660536. doi:10.1145/3656650.3660536.