Cybersecurity and Human Factors from an Industrial and Ethical Perspective

Training School @ Litochoro, Mountain Olympus

August 27-29, 2025

Venue: Litochoro City Hall, Agiou Nikolaou 15, Litochoro, 60200, Greece

Location: https://maps.app.goo.gl/NSQroBafzA6sTTQ97

Organized by

COST Action CA22104 - Behavioral Next Generation in Wireless Networks for Cyber Security (BEiNG WISE)

Funded by
the European Union

Agenda

Day 1 - Wednesday (August 27)

13.30 - 14.00 Arrival and registration of the participants

14:00 - 14:15 Welcome from Training School Organizers

14:15 - 15:45 Marcin Czerniawski

(Orange Innovation, Poland)

Title: ***Safeguarding Wireless Communications: A Security Perspective***

Abstract: Wireless communications have become the backbone of modern connectivity, powering everything from personal devices to industrial systems. However, the open and shared nature of wireless channels makes them inherently vulnerable to a wide range of attacks—from eavesdropping and spoofing to jamming and man-in-the-middle intrusions. The speech will explore the evolving threat landscape in wireless security, highlighting issues and the way of resolutions.

As Orange Innovation, team which serves as a bridge between the scientific community and industry, Mr. Czerniawski will focus on monetizing innovative scientific ideas. He will share a demonstration using Flipper Zero to illustrate how easily certain vulnerable radio communication systems can be compromised. His presentation would be interactive with certain questions with gifts.

15:45 - 16:15 Networking coffee break

16:15 - 18:00 Nicolas Sklavos

(SCYTALE Group, Computer Engineering and Informatics Department, University of Patras, Greece)

Title: ***Security by Design: Perspectives, Trends and Challenges***

Abstract: As a latest concept, Security by Design can be described as an approach to hardware and software, regarding systems development. Taking into account the rapid growth of attacks and cybercrime in latest years, security cannot be something that is thought of or added late. It targets to make products as free of threats, vulnerabilities, and attacks as possible. Challenges include facts such as that security has not traditionally been included in product design phase, for many applications and services. Methodologies and good approaches applied for Security by Design aims and scopes, include design practices, testing and measures.

Day 2 - Thursday (August 28)

09:15 - 10:45 ***Leo Suret***

(Venabili, France)

Title: ***Toward Integrative Cybersecurity/Empowering Users with AI***

Abstract: Recent cybersecurity literature highlights the limitations of technically driven approaches, particularly regarding the empowerment of citizens facing digital risks. Research points to a persistent gap between the availability of security solutions and their actual adoption by users — stemming from complexity, lack of personalization, and insufficient contextual support. This raises a central question: how can we move beyond a utilitarian and fragmented view of digital security to effectively support long-term individual autonomy?

This presentation aims to demonstrate the relevance of an AI companion—equipped with a simple and intuitive visual interface—to implement a human-centered integrative approach to cybersecurity. It will draw on a theoretical framework that integrates insights from cognitive psychology, human-computer interaction, and behavioral sciences, combining the "3U" methodology (User, Usage, Usability) with the logic of a security alliance.

The proposed approach is structured around three pillars:

1. Individualized risk modeling based on real usage data;

2. Development of an interactive AI companion prototype, enabling self-diagnosis, continuous prevention, and incident response;

3. Qualitative and quantitative evaluation of user adoption across different profiles, conducted on a first pilot panel.

Early exploratory findings suggest that the AI fosters engagement and understanding of security issues, reduces fatigue related to awareness campaigns, and supports the personalization of protective routines. This study provides a foundation for rethinking the integration of cybersecurity into everyday digital life. It invites a reassessment of expert roles, reframes the human-technology relationship, and opens new perspectives on inclusion, proactive prevention, and digital dignity for users.

10:45 - 11:15 **Networking coffee break**

11:15 - 13:00 **Panagiotis Katsaros**

(Aristotle University of Thessaloniki, Greece)

Title: ***Cybersecurity: how it has been transformed in the era of AI***

Abstract: The talk will be focused on the role of AI and ML into the increase of the frequency and intensity of modern cyber threats and into the advent of highly effective AI-powered cyber-defence solutions. We will refer to use cases of practical interest (cyber threat intelligence, anomaly detection, vulnerability management, intrusion detection etc), as well as to the associated threats (adversarial attacks) and defences.

13:00 - 14:30 **Lunch break**

14:30 - 15:30 **Vesna Dimitrova**

(Ss. Cyril and Methodius University, North Macedonia)

Title: ***Security Challenges in Human-AI Collaboration***

Abstract: As AI systems become increasingly integrated into critical domains such as cybersecurity, healthcare, and finance, secure and trustworthy human-AI collaboration is essential. This talk will explore key security challenges arising from the interaction between human decision-making and AI systems. The talk will highlight how these vulnerabilities can compromise system integrity and trust, particularly in collaborative *environments. The goal is to raise awareness and provide participants with practical tools and insights for the secure deployment and management of AI in real-world settings.*

15:30 - 16:30 **Isabella Corradini**

(Themis Research Center, Italy)

Title: ***Organizational culture, human factors, cybersecurity resilience: a psychological perspective***

Abstract: The focus of this talk will be on the concept of "organizational culture" from a work and organizational psychology perspective. The starting point is that cybersecurity culture has to be considered as an integral part of the organizational culture. Analyzing the elements characterizing these concepts, and their connections, it is possible to understand how to prepare organizations against cyber-attacks – involving human factors - and make them more resilient.

16:30 - 17:00 **Networking coffee break**

17:00 - 18:00 **Vesna Dimitrova & Isabella Corradini**

Title: *Interactive Laboratory*

Abstract: Participants will be invited to work on different scenarios on the basis of the topics presented by the two speakers.

Day 3 - Friday (August 29)

09:15 - 10:45 ***Pinar Ugurlar***

(Özyeğin University, Türkiye)

Title: ***Cognitive Biases and Social Dynamics in Cybersecurity Decision-Making***

Abstract: This talk examines how individuals make decisions in complex, high-stakes environments by relying on cognitive shortcuts and mental representations that are often efficient but prone to systematic error. Drawing on research in social and cognitive psychology, the speaker will discuss how biases such as overconfidence, the salience of certain cues, and intergroup dynamics—as well as trust-related judgments—influence decision outcomes. While these processes are generally adaptive, they can lead to suboptimal or risky choices under conditions of uncertainty. Special attention will be given to how such cognitive and social mechanisms shape decisions related to risk, trust, and compliance in cybersecurity contexts. Although the focus is on foundational psychological processes, understanding these mechanisms offers important insights into the human factors contributing to cybersecurity failures.

10:45 - 11:15 **Networking coffee break**

11:15 - 13:00 **Trainees Presentation Session and Discussion**

13:00 - 14:30 **Lunch break**

14:30 - 16:00 **Hartmut Aden**

(Berlin School of Economics and Law - HWR Berlin, Germany)

Title: ***Legality and Ethics by Design for Cybersecurity***

Abstract: This talk will demonstrate how legality and ethics by design can be used for the development of technologies in the context of cybersecurity. It will discuss opportunities and challenges of interdisciplinary cooperation in technology development. The aim of legality and ethics by design approaches is to make compliance with high *standards of fundamental rights' protection and ethics more independent from the users' behavior. If legality and ethics requirement are already designed in the hardware and software architecture, humans will need to pay less attention to compliance with legal and ethics standards while using such systems.*

16:00 - 16:30 Networking coffee break

16:30 - 18:00 SMEs presentation session and discussion

18:00 - 18:15 Concluding remarks and closing session

Bio of speakers

Marcin Czerniawski is a Cybersecurity Expert and Tech Lead at Orange Innovation Poland. He has more than 20 years of experience in IT security, with a background in the telecommunications, retail, and banking sectors. He is a key advisor for business decisions related to IT Security and has participated in global projects and strategic change implementations. Marcin holds a Master's Degree in Cybersecurity and is CISA certified. He has held positions at ADEO as a CISO special advisor and at Nordea AB as a Cybersecurity Expert.

Dr. Nicolas Sklavos is a Professor, with Computer Engineering and Informatics Department (CEID), Polytechnic School, University of Patras, Greece. He is Director of SCYTALE Group. His research interests include Cybersecurity, Hardware Security, Cryptographic Engineering, and Embedded Systems. He has participated to several European\National, research and development projects. He is evaluator\reviewer of project calls, funded by the European Commission, or by National Resources of many countries. He serves in several international boards of task forces and scientific committees. He is editorial board member of scientific journals, and he has participated to the organization of international scientific conferences, of IEEE\ACM\IFIP, serving several committee duties. He has received international scientific awards and recognition, for his contributions to scientific research and education. He has authored technical papers, books, chapters, technical reports etc, in the areas of his research. He has been also keynote/invited speaker for international conferences, forums, summer schools etc. His publications have received a great number of citations, in scientific and technical literature. He is Senior Member of IEEE, and Professional Member of ACM. He is ACM Distinguished Speaker, in the scientific area of security. For more details please visit: www.scytale.ceid.upatras.gr

Leo Suret is a Senior cyber consultant in Venabili (France), former Saint-Cyr officer, human-centric cybersecurity expert. Vacation lecturer (Aix-Marseille), trainer/auditor in ISO 27001, EBIOS RM and ethical cybersecurity.

Panagiotis Katsaros received the Bachelor degree in mathematics from the Aristotle University of Thessaloniki (AUTh), Greece, the Master of Science degree in software engineering from Aston University, Birmingham, and the Ph.D. degree in computer science from AUTh. He is a Professor with the School of Informatics, AUTh. He has published over 110 research papers in international journals and conference proceedings on software engineering and cybersecurity. His research interests include the formal verification of software/systems, software and system security and the simulation-based performance analysis/optimization. He is coordinator (or participates) in national and European research and development projects focusing on the (security) engineering of software/systems for the Internet of Things, space systems, and more recently autonomous systems. Regular updates on his recent research achievements can be accessed online at https://depend.csd.auth.gr

Vesna Dimitrova is currently a Full Professor at the Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University, where she is also the Head of Department for Theoretical Foundations of Informatics and Computational Engineering and the Coordinator of the Master studies of Security, Cryptography and Coding. Also, she is the local coordinator of Erasmus Mundus project titled CyberMACS, which stands for a Master's Program in Applied Cybersecurity. She participated/managed more than 30 international/national projects. She was a chair of three International Conference and a member of program/scientific committee at more than 40 conferences. She has published over 80 scientific papers. She participated in more than 100 conferences/workshops in the country and abroad. She is the editor of several books/proceedings and appears as an expert reviewer of two books in the field of Cryptography. She was vice-dean of Finance at the Faculty of Computer Science and Engineering, vice-president of the ICT-ACT Association, head of the FCSE Career Center, a member of the Management Committee of seven international projects and a member of several other committees. The main areas of scientific interest are information security, cryptography, cryptanalysis, application of ML/DL in cybersecurity, human factor in cybersecurity.

Social-psychologist, and criminologist, **Isabella Corradini** is the director of Themis Research Center (Rome, Italy), a nonprofit organization specialized in psychology and criminology, and co-founder of Link & Think Research Lab, focused on socio-technical analysis of information technologies and informatics education. Research activity is focused on the role of the human factor in safety and security, by considering its different dimensions (social, cognitive, emotional and behavioral) as well as organizational factors. She was a lecturer in social psychology at University of L'Aquila for about ten years. Currently, she lectures in industrial training programs and academic masters. She is member of several technical committee (e.g. Master in Homeland Security, University of Campus Bio-Medico, Rome; Women4Cyber Italy Chapter) and editorial advisory board (e.g. In Science Press, Editorial Advisory Board, Construction of Social Psychology; Psychology Applications and Development In Science Press) She is in charge of "Digital Citizenship" area for the national project "Programma il Futuro", an initiative realized by the "Informatics and School Laboratory" of CINI (National Interuniversity Consortium for Informatics), and promoted by the Italian Ministry of Education. She is co-leader of the WG4 "Human factors in wireless security" in the COST Action "Behavioral Next Generation in Wireless Networks for Cyber Security" (BEiNG-WISE) CA22104. She is the research coordinator of the initiative "The role of women for the harmonious, integral and sustainable development of Mediterranean countries", promoted by the University & Research Department of Oikos Mediterraneo, in collaboration with several universities. She has written many papers and books on the expertise areas. For more details https://themiscrime.com/en/isabella-corradini

Pınar Uğurlar is an Assistant Professor of Social Psychology at Özyeğin University. Her research centers on the interplay between the self and social decision-making. She examines how people cognitively represent themselves and others, and how these representations influence decisions in interpersonal and intergroup contexts. A major focus of her work is on trust and cooperation—both their determinants and consequences. This includes investigating the psychological processes underlying trust decisions, as well as how being trusted or distrusted affects behavior. Dr. Uğurlar completed her PhD at Middle East Technical University, conducting much of her doctoral research at the Social Cognition Center Cologne (University of Cologne). She later worked as a postdoctoral researcher at the University of Cologne. Her research has been supported by several funding bodies, including TÜBİTAK and the Center for Social and Economic Behavior (University of Cologne).

Prof. Dr. Hartmut Aden is a distinguished professor specializing in German and European Public Law, Public Policy, and Public Administration at the Berlin School of Economics and Law (HWR Berlin). Since joining HWR Berlin in 2009, Prof. Aden has held several key roles. He was a founding member of the Berlin Institute for Safety and Security Research (FOPS Berlin) in 2013, where he served as Deputy Director from 2016 to 2020. From 2020 to 2024, he also held the position of Vice President for Research at HWR Berlin. His expertise covers a broad range of topics, including internal security, human rights, data protection, and environmental law, often with a comparative and European perspective.