
# Call for Papers

## Important dates

Paper submission deadline:
**April 13, 2026**
Authors' notification:
**May 4, 2026**
Camera-ready submission:
**May 25, 2026**
Registration deadline (authors):
**May 25, 2026**
Workshop dates:
**August 3–5, 2026**

## Workshop chairs

Alfredo Nascita (Italy)
Francesco Cerasuolo (Italy)
Giampaolo Bovenzi (Italy)
Antonio Pescapè (Italy)

## Technical program committee

Tran Anh Quang Pham (France)
Danilo Giordano (Italy)
Jonatan Krolikowski (France)
Jan Luxemburk (Czech Republic)
Claudio Fiandrino (Spain)
Tomáš Čejka (Czech Republic)
Haiming Chen (China)
Flavio Esposito (USA)
Marilia Curado (Portugal)
Walter Cerroni (Italy)
Maria Solange Pires Ferreira Rito Lima (Portugal)
Giancarlo Sperlì (Italy)
Catalin Meirosu (USA)
Carlos Becker Westphall (France)
Anat Bremler-Barr (Israel)
Abbas Bradai (France)

## Contact us

alfredo.nascita@unina.it
francesco.cerasuolo@unina.it
giamapolo.bovenzi@unina.it
antonio.pescape@unina.it

Recent advances in Generative Artificial Intelligence (GenAI), particularly Large Language Models (LLMs), are opening new opportunities to enhance the security, resilience, and trustworthiness of modern networks. While GenAI has shown significant impact across multiple domains, its adoption in cybersecurity and resilient network operations is still largely exploratory. Modern networks face increasingly sophisticated cyber threats, including intrusions, large-scale distributed attacks, and zero-day exploits, which traditional security mechanisms and AI approaches often struggle to address. In this context, GenAI enables advanced modeling of benign and malicious network behavior, the generation of realistic attack and traffic patterns, and the automation of security analysis and response, supporting proactive and adaptive cyber defense strategies. However, the growing reliance on AI-based security solutions raises critical challenges related to robustness, reliability, transparency, and resilience to adversarial manipulation. Many models function as black boxes, limiting their use in mission-critical and regulated environments where trust, accountability, and explainability are essential. Explainable Artificial Intelligence (XAI) plays a key role in addressing these challenges by making AI-driven security decisions interpretable, supporting human analysts in threat understanding and response, and facilitating compliance with regulatory and ethical requirements. XAI also contributes to assessing and improving the resilience of AI-enabled security mechanisms by helping identify failure modes and vulnerabilities under dynamic network conditions. The proposed workshop complements the scope of IEEE CSR by focusing on the intersection of GenAI, XAI, and network security and resilience. While IEEE CSR addresses cybersecurity and resilience broadly, this workshop provides a focused forum on generative and explainable AI as enablers of trustworthy, resilient networks, fostering cross-disciplinary discussion and showcasing practical AI-driven solutions.

The workshop will be held in conjunction with the IEEE CSR 2026 conference as a physical event, during August 3–5, 2026. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Generative AI for Network Traffic Modeling and Threat Simulation
- GenAI-based network traffic analysis for intrusion and anomaly detection
- Explainable GenAI for real-time network traffic monitoring and decision support
- Generative approaches for traffic-based attack detection and prediction
- XAI techniques for interpretable network traffic classification and security
- GenAI for automated network security
- Trust, accountability, and transparency in AI-driven network traffic security
- Generative AI for security log and flow data correlation in networked systems
- Robustness of GenAI models under adversarial conditions
- Explainable AI for cyber resilience, fault diagnosis, and incident response
- Explainable AI for cyber resilience, fault diagnosis, and incident response
- GenAI-Driven Automation for Resilient Network Security Management

The CSR GenXSec workshop will accept high-quality research papers presenting strong theoretical contributions, applied research, and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website https://www.ieee-csr.org/genxsec (Tbd)

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
SMC Homeland Security Technical Committee
LOGOS RI RESEARCH&INNOVATION