CRITIS 2026

The 21st International Conference on Critical Information Infrastructures Security

28 - 30 September 2026

Radisson Beach Hotel, Larnaca, Cyprus

critis2026.com

Call for Papers

The **21st International Conference on Critical Information Infrastructure Security (CRITIS 2026)** invites researchers, practitioners, policymakers, and industry experts to submit original contributions on the security, resilience, and protection of critical information infrastructures (C(I)IP) and essential services.

Building on twenty successful editions, **CRITIS** has established itself as a leading international forum for cutting-edge research, emerging challenges, and practical solutions at the intersection of technology, operations, and policy. **CRITIS 2026** will take place on **28 - 30 September 2026** in Cyprus, hosted by the Cybersecurity & Telecommunications Research Lab (CTRL) of the Open University of Cyprus (OUC). As critical infrastructures become increasingly interconnected and exposed to evolving cyber, physical, human, and environmental threats, **CRITIS 2026** aims to foster interdisciplinary dialogue and innovative approaches that strengthen security, resilience, and mission continuity across sectors.

Young CRITIS Award

Continuing the tradition of previous editions, **CRITIS 2026** will present the Young CRITIS Award to recognize and reward outstanding contributions by early-career researchers in the field of Critical Infrastructure Protection (CIP).

Paper Submission & Guidelines

All contributions must be submitted via EasyChair. Accepted papers will be published in the conference proceedings in **Springer Lecture Notes in Computer Science** (LNCS).

The following two paper categories are welcome. Any submission must be explicitly marked as "full paper" or "short paper".

Full Papers

Scientific research papers, surveying works and industrial experiences describing significant C(I)IP advances. Papers should be no longer than 20 pages, including bibliography and well-marked appendices.These submissions correspond to what was previously indicated as "regular papers" in the call for papers.

Short Papers

Early results or work in progress with initial findings. Papers should be 4 to 6 pages long, including bibliography and well-marked appendices. These submissions correspond to what was previously indicated as "ongoing research" in the call for papers. Short papers will be presented as posters and they will NOT be included in the post-proceedings published in Springer Lecture Notesin Computer Science (LNCS).

Key Dates

20 May 2026
Paper submission deadline

11 July 2026
Camera - ready papers

20 June 2026
Notification of acceptance

28 - 30 September 2026
CRITIS 2026 conference dates

Topics

CRITIS 2026 welcomes high-quality submissions including, but not limited to, the following topics:

- **Resilience & Continuity**
  - Cyber resilience
  - Incident response and recovery
  - Continuity planning and preparedness
  - Crisis management for CI
- **Risk, Dependencies & Impact**
  - Risk and vulnerability analysis
  - Cascade and dependency analysis
  - Systemic risk modelling
- **Environmental, Physical Threats**
  - Climate change impacts on CI and services
  - Natural threats to critical infrastructures
  - Sustainable critical infrastructures
- **Governance, Strategy, Legal and Ethical Dimensions**
  - Critical infrastructure governance and regulation
  - Strategic management and policy for C(I)IP
  - Compliance and assurance mechanisms
  - Privacy and data protection in C(I)IP
  - Legal and ethical aspects of critical infrastructures
- **Situational Awareness & Decision Support**
  - Cyber situational awareness
  - Decision support for cyber incident management
  - Threat detection and correlation
  - Threat intelligence and information sharing
  - Intelligence analysis for C(I)IP
- **Platforms, Testbeds & Experimental Environments**
  - Cyber ranges and testbeds for CI
  - Experimental security platforms and labs Largescale CI simulations
  - Digital twins for critical infrastructures and services
  - Evaluation methodologies
- **Human Aspects**
  - Security awareness
  - Cybersecurity capacity building and workforce development
  - Human factors and usable security
  - Training, education, and serious games for C(I)IP
  - Immersive training
- **Cyber-Physical & Industrial Systems**
  - Cyber-physical systems security
  - Human-centric cyber-physical systems
  - Industrial Control Systems (ICS) & Operational Technology (OT) security
  - Critical Services
  - Service-oriented approaches for CI
- **Emerging Technologies & Future Threats**
  - Technology forecasting and TechWatch for C(I)IP
  - Emerging technologies for C(I)IP
  - Explainable AI for critical infrastructures
  - Quantum intelligence and post-quantum security for C(I)IP

Organising Committees

General Chairs:
Stavros Stavrou, CY
Eliana Stavrou, CY
Adamantini Peratikou, CY

Steering Committee Chairs:
Bernhard M. Hämmerli, Switzerland
Simin Nadjm-Tehrani, Sweden
Stefan Pickl, Germany
Javier Lopez, Spain
Stephen D. Wolthusen, UK

Hosted by:
OPEN UNIVERSITY OF CYPRUS
CTRL

Coordinator:
easy CONFERENCES

info@easyconferences.eu
t. +357 22 591900

For any enquiries please contact:
adamantini.peratikou@ouc.ac.cy
t.: +357 22411892