IEEE CSR 2026
Cyber Security and Resilience

Lisboa, Portugal | August 3–5, 2026

https://www.ieee-csr.org

2026 IEEE CSR Workshop on CYber-Physical REsilience and Security Against Digital Breakdowns (CYPRES)

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 4, 2026 (TBC)

Workshop Chairs

Mathaios Panteli (CY)
Juerg Luterbacher (DE)
Antonios Lalas (GR)

Program Chairs

Christos Laoudias (CY)
Elena Xoplaki (IT)
Dimitrios Vamvatsikos (GR)

Organizing Committee

Georg Aumayr (AT)
Jiri Bouchal (CZ)
Steve Gadsdon (UK)
Eva Jaho(GR)
Christina Michailidou (CY)
Bamba Niang (FR)
Nikos Papadakis (GR)
Martina Surynkova (CZ)
Balaji Venkateswaran (CY)
Monique Kuglitsch (DE)
Nikolaos Bartsotas (GR)
Enrico Scoccimarro (IT)

Publicity chairs

Marios Stavrou (CY)
Christiana Koutsoulli (CY)

Contact us

csrcypres@gmail.com

Critical infrastructures, including energy, communications, banking, transportation, and public government services, have become indispensable pillars supporting industrialised economies. The seamless functioning of these infrastructures is crucial for citizens, businesses, and governments, as they rely on a complex network of interconnected physical and information systems to meet their needs and carry out daily operations. Simultaneously, these infrastructures are experiencing a growing level of *interdependence*, where the failure of one component can lead to *cascading effects*, resembling a domino effect. Noteworthy instances include the recent major power blackout across the Iberian Peninsula on 28 April 2025 affecting more than 50M people in Portugal and Spain. In parallel, the diverse and extensive causes of these events have prompted the adoption of all-hazard approaches to policy in many countries aiming to encompass both natural disasters and man-made attacks when formulating prevention and remediation measures against the risk of infrastructure failure. Recognizing the need for coordinated action, EU member states are not only encouraging R&D activities but also implementing policies for critical cyber-physical infrastructure protection.

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 Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Emergency communication systems for first responders and citizens
- Interdependencies modelling and cascading effects analysis
- Cybersecurity anomaly and intrusion detection and mitigation
- Applications for citizen preparedness
- Use cases, pilot trials, and living labs for crisis and disaster management
- Policy recommendations for enhanced civil protection planning
- Crisis and disaster management across different critical sectors
- Frameworks for threat modelling and vulnerability assessment
- Methodologies for critical asset management during digital breakdowns
- Digital Twins, simulation engines, and scenario creation tools
- Risk estimation and impact assessment
- Ethical, Legal and Societal Aspects (ELSA) for resilience

The CSR CYPRES 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/cypres**.

Supported by

SPARROW
MedEWSa
NATWORK
Funded by the European Union

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