IEEE CSR 2025
Cyber Security and Resilience

Chania, Crete, Greece | August 4–6, 2025

https://www.ieee-csr.org

2025 IEEE International Conference on Cyber Security and Resilience

Call for Papers

Important dates

Paper submission deadline:
February 10, 2025
Authors' notification:
March 10, 2025
Camera-ready submission:
March 31, 2025
Registration deadline (authors):
March 31, 2025
Conference dates:
August 4–6, 2025

Conference chairs

Nicholas Kolokotronis (GR)
Stavros Shiaeles (UK)
Emanuele Bellini (IT)

Steering committee

Emanuele Bellini (IT)
Ernesto Damiani (AE)
Francesco Flammini (CH)
Giancarlo Fortino (IT)
Bogdan Ghita (UK)
Vasilis Katos (UK)
Nicholas Kolokotronis (GR)
Stefano Marrone (IT)
Stavros Shiaeles (UK)
Costas Vassilakis (GR)

Technical program chairs

Kim-Kwang Raymond Choo (US)
Konstantinos Markantonakis (UK)

Track chairs

Nicholas J. Multari (US)
Rosalie McQuaid (US)

Publication chairs

Costas Vassilakis (GR)
Nathan Clarke (UK)

Workshops chairs

Sokratis Katsikas (NO)
Konstantinos Limniotis (GR)

Local operations

Alexios Lekidis (GR)
Kyriakos Fytrakis (GR)

Contact us

info@ieee-csr.org

The IEEE International Conference on Cyber Security and Resilience (IEEE CSR) is an annual event sponsored by the IEEE Systems, Man, and Cybernetics (SMC) Society. It focuses on theoretical and practical aspects of security, privacy, trust, and resilience of networks, systems (including complex cyber-physical systems), applications, and services, as well as, novel ways for mitigating sophisticated cyber-attacks. The IEEE CSR 2025 conference will be held as a **physical event**, during August 4–6, 2025.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

Cyber security

- 5G and B5G cyber-security
- Big data security
- DLT/smart contract security
- Cloud-edge security
- Cyber-security and AI
- Cyber-threat intelligence
- Distributed systems security
- Game-theoretic security
- Forensics
- Identity management and access control
- Insider threats
- Lightweight cryptography
- Malicious cryptography
- Malware detection
- Moving target defense
- Network intrusion detection
- Post-quantum security
- Privacy and data protection
- Trust management systems
- Trusted execution environments
- Web services security

Cyber resilience

- AI for resilience management
- Formal methods in resilience
- Self-adaptive cyber resilience
- Attack resilient architectures
- Cyber-range platforms
- Cyber-resilience assessment
- Cyber-resilience foundations
- Cyber-risk forecasting
- Cyber-security training
- Cyber-threat adaptive capacity in IoT
- DLT resilient architectures
- Dynamic risk management
- Fault tolerant architectures
- Gamification in security
- Human factor in resilience
- Operational recovery and continuity
- Preparation and adaptation strategies
- Safety-critical applications
- Zero-trust architectures
- Zero-trust security

Complex CPS security

- Automotive cyber security
- Autonomous systems security
- Critical infrastructure security
- Cyber-physical attacks
- Digital twins and cyber-security
- eHealth security
- Embedded systems security
- Hardware security
- Internet of body security
- ICS security
- IIoT security and privacy
- ITS security
- IoT and cloud forensics
- Mobile applications security
- SCADA cyber-security
- Security-as-a-service
- Sensor network security
- Side-channel attacks
- Smart cities security
- Smart grid security
- Virtualization security

The IEEE CSR 2025 conference will accept high-quality regular research papers, Systematization of Knowledge (SoK) papers providing insights in the above areas, and industrial papers promoting contributions on technology development, innovations and implementations. The IEEE CSR 2025 also hosts workshops that specialize into the conference's areas or focus on high-quality applied research and innovation results obtained from cyber-security and resilience projects.

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 have been posted at IEEE CSR 2025 conference website https://www.ieee-csr.org.

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