IEEE CSR 2022
Cyber Security and Resilience
Virtual Conference | July 27–29, 2022
https://www.ieee-csr.org

2022 IEEE CSR Workshop on Maritime Cyber Security (MCS)

Call for Papers

Important dates

Workshop papers' deadline:
~~April 22~~ May 20, 2022
Workshop authors' notification:
~~May 13~~ June 10, 2022
Camera-ready submission:
~~May 27~~ June 24, 2022
Early registration deadline:
June 24, 2022
Workshop's date:
July 27–29, 2022

Workshop chairs

Leandros Maglaras
Christos Douligeris
Despina Polemi
Vasileios Vlachos
Ying He
Ioanna Kantzavelou

Publicity chairs

Kyriaki Chantzi

Contact us

mcs@uniwa.gr

Critical infrastructures are vital assets for public safety, economic welfare, and the national security. Vulnerabilities of critical infrastructures have increased with the widespread use of information technologies. As Critical National Infrastructures are becoming more vulnerable to cyberattacks, their protection becomes a significant issue for any organization as well as nation. The risks to continued operations from failing to upgrade aging infrastructure or not meeting mandated regulatory regimes are considered higher given the demonstrable impact of such circumstances. Critical infrastructure in the maritime sector sustains essential services and the movement of vital goods. Maritime activities are so crucial that their unavailability or delays in their supply chain may adversely affect the well-being of a country.

Due to the rapid increase of sophisticated cyber threats targeting the maritime sector with significant destructive effects, the cyber security of critical infrastructures has become an agenda item for academics, practitioners, and policy makers. A holistic view that covers technical, policy, human, and behavioral aspects is essential to handle cyber security of critical infrastructures effectively. Moreover, the ability to attribute crimes to criminals is a vital element of avoiding impunity in cyberspace.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following: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 of complex and distributed critical infrastructures;
- Situational Awareness towards Maritime Cyber Incidents;
- Prevention, resilience and preparedness;
- Maritime security management methodologies (MSMM);
- Safety-security interactions;
- Protection of Ports' Information and Telecommunication (PIT) systems;
- Maritime security policies, standards and regulations;
- Vulnerability and risk assessment methodologies for maritime systems;
- Detection and response mechanisms for maritime systems;
- On-vessel architectures and services;
- On-ship and in-port cyber-attacks;
- Attack surfaces in IoT devices in ships and ports;
- Digitalisation of maritime industry;
- Emerging technologies in maritime security and privacy;

In this workshop, both research and practical aspects of cyber security considerations in critical infrastructures in the maritime sector are of interest. Aligned with the interdisciplinary nature of cyber security, authors from academia, government, and industry are welcome to contribute.

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. The workshop's proceedings will be published by IEEE and will be included in IEEE Xplore. Detailed information about the paper submission and guidelines to authors can be found at the workshop's website https://www.ieee-csr.org/mcs.