CYBERWARFARE AGAINST CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII): ADVANCES AND CHALLENGES

SESSION ORGANIZER:

Professor Ts Dr Madihah Mohd Saudi,
Cyber Security and Systems (CSS) Research Unit,
Information Security and Assurance (ISA) Programme,
Faculty of Science and Technology (FST),
Universiti Sains Islam Malaysia (USIM), Malaysia.
madihah@usim.edu.my.

SESSION DESCRIPTION:

The session's focus is to systematically cover all essential aspects, state-of-the-art solutions, the latest research results, and the real-world deployment of cyberwarfare, with a focus on Critical National Information Infrastructure (CNII).

Cyberwarfare against CNII is a concerning issue and has rapidly taken an important position in our technological and information society to achieve strategic and financial advantages. It involves manipulating, disrupting, damaging, or compromising the vital CNII systems and services a nation relies on for its functioning and security. These attacks include, but are not limited to, government networks, power grids, communications, financial systems, and military command and control systems.

RECOMMENDED TOPICS:

This track will accept papers on research articles and reviews in the areas including, but not limited to:

- Cryptography and its applications
- Network and critical infrastructure security
- Software and system security
- Ontology and data analytics
- Data-driven security and measurement studies
- Malware analysis
- Privacy-enhancing technologies and anonymity
- IoT/IoMT Security
- Banking and Financial Security
- Information Security & Data Protection
- Cyber Crime and Digital Terrorism

SUBMISSION PROCESS

Authors are invited to submit papers for this special theme session through the website. All submissions must be original and may not be under review by another publication. Interested authors should consult the conference's guidelines for manuscript submissions. All submitted papers will be reviewed on a double-blind, peer-review basis. Please select the track 'Cyberwarfare Against Critical National Information Infrastructure (CNII): Advances and Challenges'.

SUBMISSION GUIDELINES

Papers reporting original* and unpublished research results on the related topics are solicited. *(papers with plagiarism more than 30% will be outrightly rejected). To know more about paper format and other submission guidelines please visit the following link of SN LNNS: https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines
Submissions should include the author(s), affiliation(s), e-mail address(es), and postal address(es) in the manuscripts. Papers will be selected based on their originality, significance, relevance, and clarity of presentation. Paper submission implies the intent of at least one of the authors to register and present the paper, if accepted.