Call for Papers for Special Session

RESEARCH AND APPLICATION OF MCDM METHODS AND DECISION SYSTEMS IN CYBERSECURITY

at the 18th International Symposium on Operations Research in Slovenia (SOR '25)
which will be held in Bled, Slovenia, September 22 – 24, 2025.

Organized and chaired by: Dr. Andrej Bregar

This special session invites researchers with expertise in the broad Operations Research (OR) and Information Security (INFOSEC) fields. It particularly focuses on the use of Multi-Criteria Decision-Making (MCDM) methods, Decision Support Systems (DSS), and Artificial Intelligence (AI) to facilitate cybersecurity. It encourages researchers and practitioners to present novel MCDM methods and decision technology for cybersecurity, demonstrate applications and use cases, empirically evaluate the efficiency of approaches, review state-of-the-art on the topic, study current trends and technologies, and elaborate on various cybersecurity problems that can be solved with the help of MCDM methods, decision support technology, and AI.

Our society is becoming increasingly exposed to cyberattacks due to the geopolitical situation and a strong reliance on Information Technology (IT) and Operational Technology (OT). We can observe that cyberattacks have been occurring more frequently in recent years. Moreover, attackers utilize advanced techniques and tactics that exploit numerous vulnerabilities, posing serious threats to critical infrastructures and corporate systems. This significantly increases the costs and resources required to establish and maintain a sufficient level of cyber resilience. Organizations must select and implement efficient mitigation actions, encourage collaboration between different organizational levels and stakeholders, and facilitate the exchange of Cyber Threat Intelligence (CTI) information. Current trends prioritize cyber risk management through systematic decision-making on cost-effective investments, continuous management of threats and vulnerabilities targeted at achieving high availability of corporate assets, and situational awareness that provides necessary information to make well-informed decisions on protecting the assets. In addition, cybersecurity technology is becoming increasingly complex as it must be able to process an extensive amount of network traffic. Therefore, it should be enhanced with AI and supported with decision modules to optimize and ease incident detection, analysis, and response.

The 18th International Symposium on Operations Research in Slovenia - SOR'25

Bled, Slovenia, September 24-26, 2025

https://sor.fov.um.si/

MCDM methods and decision technologies are gaining relevance in cybersecurity to cope with the above challenges. MCDM methods have been traditionally applied for risk and vulnerability assessment. However, they also have potential for various other tasks and problems, including incident detection and severity assessment, prioritization of incident response procedures and actions, selection of cybersecurity controls and mitigation measures, cost-benefit analysis, CTI analysis, infrastructure and application security analysis, stochastic analysis of time-dependent threats, prioritization of cybersecurity strategies and policies, capability maturity assessment, regulatory compliance assessment, etc. A variety of methods can be used for these purposes, such as AHP (Analytic Hierarchy Process), TOPSIS, ELECTRE, PROMETHEE, additive value/utility models, fuzzy and stochastic models, time series and Markov analyses, attack trees, regression methods, risk and threat simulations, qualitative models, CVSS (Common Vulnerability Scoring System), Delphi processes, and others.

This special session aims to review, analyse, and advance the state of MCDM methodologies and decision support technologies in cybersecurity. We welcome contributions that introduce original new methods and approaches, as well as work that applies and empirically evaluates MCDM and DSS solutions in the context of cybersecurity. You are warmly invited to submit your work that contributes to the body of knowledge, addressing the topics, but not limited to:

- Novel MCDM methods, processes, and approaches for cybersecurity
- Group decision-making and collaborative processes for cybersecurity
- Overview, state-of-the-art, and utilization of MCDM methods for cybersecurity
- Specific problems, areas, and tasks in cybersecurity and information security addressed by MCDM methods
- MCDM as part of cybersecurity and information security policies, strategies, standards, and frameworks
- Predictive and network methods for time series and dependent cyber threats
- Design, development, integration, and use of DSS technology in cybersecurity
- Utilization of AI and ML (Machine Learning) to facilitate decision-making, autonomous incident detection and response, and risk management in cybersecurity
- Use cases and applications in real-life settings, environments, and infrastructures
- Practical and empirical evaluations of MCDM and DSS solutions in cybersecurity settings
- Opportunities for new developments to increase the cyber resilience of ecosystems

DEADLINES:

- Submission of contributed papers: June 1, 2025
- Referee's reports: July 1, 2025
- Submission of revised papers and copies of bank transfer: August 25, 2025

Note: When submitting the paper, please select "Special Session – Research and Application of MCDM Methods and Decision Systems in Cybersecurity".