

# The Sixth International Conference on Cyber-Technologies and Cyber-Systems

## CYBER 2021

October 03, 2021 to October 07, 2021 - Barcelona, Spain

Submit a Contribution

Registration

Camera Ready

### Deadlines

Submission	Jul 27, 2021
Notification	Aug 19, 2021
Registration	Sep 02, 2021
Camera ready	Sep 04, 2021

Deadlines differ for special tracks. Please consult the conference home page for special tracks Call for Papers (if any).

Past Events

Sponsors



### Publication

Published by IARIA Press (operated by Xpart Publishing Services)



Archived in the Open Access IARIA ThinkMind Digital Library.



Prints available at Curran Associates, Inc.

Authors of selected papers will be invited to submit extended versions to a IARIA Journal Indexing Procedure

### Affiliated Journals



### CYBER 2021

Onsite and Online Options: In order to accommodate a large number of situations, we are offering the option for either physical presence or virtual participation (pdf slides or pre-recorded videos).

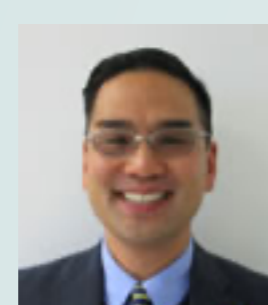
ISSN: 2519-8599  
ISBN: 978-1-61208-893-8

- Registered: with the Library of Congress of the United States of America (ISSN)
- Free Access: in [ThinkMind Digital Library](#).

### CYBER 2021 is colocated with the following events as part of NexTech 2021 Congress:

- [UBICOMM 2021](#), The Fifteenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies
- [ADVCOMP 2021](#), The Fifteenth International Conference on Advanced Engineering Computing and Applications in Sciences
- [SEMAMPRO 2021](#), The Fifteenth International Conference on Advances in Semantic Processing
- [AMBIENT 2021](#), The Eleventh International Conference on Ambient Computing, Applications, Services and Technologies
- [EMERGING 2021](#), The Thirteenth International Conference on Emerging Networks and Systems Intelligence
- [DATA ANALYTICS 2021](#), The Tenth International Conference on Data Analytics
- [GLOBAL HEALTH 2021](#), The Tenth International Conference on Global Health Challenges
- [CYBER 2021](#), The Sixth International Conference on Cyber-Technologies and Cyber-Systems

### CYBER 2021 General Chair



**Steve Chan**  
Decision Engineering Analysis  
Laboratory  
USA

### CYBER 2021 Steering Committee



**Carla Merkle Westphall**  
UFSC  
Brazil



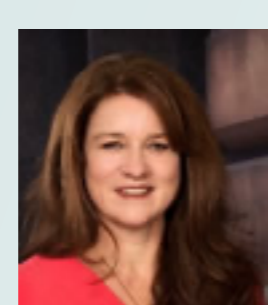
**Barbara Re**  
University of Camerino  
Italy



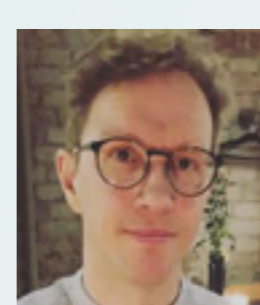
**Rainer Falk**  
Siemens AG, Corporate  
Technology  
Germany



**Soultana Ellinidou**  
Cybersecurity Research Center |  
University Libre de Bruxelles  
(ULB)  
Belgium



**Anne Coull**  
University of New South Wales  
Australia



**Patrik Österberg**  
Mid Sweden University, Sundsvall  
Sweden



**Daniel Kästner**  
AbsInt GmbH  
Germany



**Steffen Fries**  
Siemens  
Germany

### Special tracks:

#### SAFAR: Information Security Awareness at the Forefront of Achieving Organisational Resiliency

Chair: Dr. Alina Andronache, University of the West of Scotland - London, UK [alina.andronache@partner.uws.ac.uk](mailto:alina.andronache@partner.uws.ac.uk)

#### AMCPS: Autonomous Mobile Cyber-Physical Systems

Chair: Professor Peter Schneider-Kamp, University of Southern Denmark, Denmark [petersk@imada.sdu.dk](mailto:petersk@imada.sdu.dk)

Coordinator: PhD Candidate Golizheh Mehrooz, University of Southern Denmark, Denmark [mehrooz@imada.sdu.dk](mailto:mehrooz@imada.sdu.dk)

### CYBER 2021 conference tracks:

#### Trends in Cybersecurity

Blockchain and machine learning for cybersecurity; Behavioral biometrics authentication; Privacy by design; Anonymity of blockchain and cryptocurrencies; Threat categorization and threat detection; Threats on critical national infrastructures; Gift card hacking techniques; Medical IoT Device-to-Device communication; Blockchain in supporting critical infrastructures; Vulnerability on social media spaces; Internet of Medical Things (IOMT); Cybersecurity for digital vehicles; Potential radicalization on social media; Blockchain and healthcare systems; Risk-based human behavior profiling; Forensic recovery of cloud evidence; Hacking pacemakers; Prediction of cyber attacks; Ransomware cyberweapon; Liability attribution in smart workplaces; Cybersecurity, laws and regulations; Information from browsers by online advertising platforms; Predicting social engineering victims; Cybercrime awareness

#### Cyber Resilience

Cyber security assessment; Data analytics for Cyber resilience; Organizational security (government, commercial); Resilient smart cities; Resilient Internet of Things (RIOT); Cyber-cities and Cyber-environments; Critical infrastructure security; Back up and recovery for systems of systems; Disaster planning and management from Cyber perspective; Integrated and smarter sensors

#### Resiliency and risks

Resiliency in smart cities; Reliability and resiliency in wireless networks; Detecting anomalous activity; Resources constrained systems/devices; Disruption-tolerant systems; Resiliency and access in restricted areas; Monitoring maritime critical disasters; Critical supply networks; Risk assessment

#### Technologies for resiliency

Self-organized disaster management systems; Technological catastrophes and crises management; Deep-learning & Big Data and disaster recovery; Disaster management in 5G uRLLC-based systems; 5G and IoT in disaster management; Aerial Systems for Disaster Management; IoT sensing platforms for public safety

#### Cyber Security

Security management [overall information security management in the sense of 27000 series applied to cyber systems]; Compliance management [verify/check compliance with defined policies, provide corresponding management reports]; Security administration of cyber systems [technical security management of security services]; Security and privacy regulations and laws; Securely interconnected cyber systems [firewalls, cross-domain security solutions]; Self-securing and self-defending cyber systems; Trust management, trust-based information processing [using possibly untrustworthy data sources in a controlled way]; Security technologies for protecting cyber systems and devices; Identity and access management in cyber systems; Anti-counterfeiting; Secure production and supply chain; Cloud computing security; Big-data security; Advanced persistent threats; Network traffic analysis and trace-back; Cyberspace operations; Incident response, investigation, and evidence handling; Intrusion detection and prevention; Cyberspace protection and anti-malware; Cooperation and sharing for Cyber-defense

#### Cyber Infrastructure

Cyber-Cities and Cyber-environments; Information technology infrastructure; Telecommunications and networks; Cyber-space and data centers; Cyber-enabled control systems; Cyber-enabled critical infrastructure systems; Cyber-physical systems and Internet of Things; Special application domains (smart grid, traffic management systems, autonomous driving, etc.); Embedded processors and controllers; Mobility in Cyber-space; Virtualization in Cyber-space

#### Cyber Forensics

Computer and networks forensics; Social networking forensics; Digital forensics tools and applications; Applications of information hiding; Identification, authentication, and collection of digital evidence; Anti-forensic techniques and methods; Watermarking and intellectual property theft; Privacy issues in network forensics; Tools, applications, case studies, best practices

#### Cyber Crime

Cyber-crimes: Challenges in detection/prevention; Anomalies detection; Advanced Persistent Threats and Cyber-resilience; BotNets and MoliNets; Cyber crime-related investigations; Challenges and detection of Cyber-crimes; Network traffic analysis, traceback; Security information and event management (SIEM); Stealthiness improving techniques: information hiding, steganography/steganalysis, etc.

#### Nature-inspired and Bio-inspired Cyber-defense

Bio-inspired anomaly & intrusion detection; Autonomous and Adaptive Cyber-Defense; Adaptive and Evolvable Systems; Cooperative defense systems; Network artificial immune systems; Adaptation algorithms for cyber security; Biometrics related to cyber defense; Bio-inspired security and networking algorithms and technologies; Biomimetics related to cyber security; Bio-inspired cyber threat intelligence methods and systems; Bio-inspired algorithms for dependable networks; Correlations in moving-target techniques; Neural networks, evolutionary algorithms, and genetic algorithms for cyber security Prediction techniques for cyber defense; Information hiding solutions (steganography, watermarking) and detection

#### Social-inspired opportunistic mobile Cyber-systems

Design of cyber-physical applications for opportunistic mobile systems based on behavioral models; Social metrics for networks and systems operations; Application of mixed physical and online social network sensing; Social-aware modeling, design and development of routing algorithms in cyber-physical; Incentive mechanisms, reputation systems and key management algorithms in cyber-physical opportunistic mobile systems; Participatory mobile sensing for mining integration in cyber-physical opportunistic mobile systems; Experiments with cyber-physical opportunistic mobile systems

### Deadlines:

Submission	Jul 27, 2021
Notification	Aug 19, 2021
Registration	Sep 02, 2021
Camera ready	Sep 04, 2021

Deadlines differ for special tracks. Please consult the conference home page for special tracks Call for Papers (if any).

### Technical Co-Sponsors and Logistic Supporters



CYBERSECURITY  
RESEARCH CENTER



DECISION engineering  
Analysis Laboratory