Call for Papers
Committees
Venue
Post Conference

The Fourth International Conference on Cyber-Technologies and Cyber-Systems
CYBER 2019
September 22, 2019 to September 26, 2019 - Porto, Portugal

ACYBER 2019: The Ninth International Conference on Ambient Computing, Applications, Services and Technologies

Submission: Jun 13, 2019
Notification: Jul 14, 2019
Registration: Jul 27, 2019
Camera ready: Aug 07, 2019

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

Cyber Security
Security management [overall information security management in the sense of 27000 series applied to cyber systems]; Compliance management [verify/validate 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-defending and self-defending cyber systems; Trust management, trust-based information processing [using possibly trustworthy 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 traceback; 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 MobNets; 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/steaganalysis, etc.

Nature-inspired and Bio-Inspired Cyber-defense
Bio-inspired anomaly & Intrusion detection: Autonomic 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 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: Jun 13, 2019
Notification: Jul 14, 2019
Registration: Jul 27, 2019
Camera ready: Aug 07, 2019

Call for Papers
Committees
Venue
Post Conference

Conference tracks:

Special tracks:
CSIRW: The Challenges of Implementing Cyber Security in the Real World
Chair and Coordinator: Steve Chan, Decision Engineering Analysis Laboratory, USA
schan@dengineering.org

ACYBER: The Nexus of Cognitive Computing, Artificial Intelligence and Cyber Security – Anomaly Detection at Scale
Chair and Coordinator: Anne Coull, University of New South Wales, Information and Engineering, Australia
www.objectiveinsight@gmail.com

CYBER 2019 is colocated with the following events as part of NexTech 2019 Congress:
- GLOBAL HEALTH 2019: The Eighth International Conference on Global Health Challenges
- ADVCOMP 2019: The Thirteenth International Conference on Advances in Sciences
- SEMAPPRO 2019: The Thirteenth International Conference on Advances in Semantic Processing
- AUSTRALIA 2019: The Eighth International Conference on Data Analytics
- UBICOMM 2019: The Thirteenth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies
- EMERGING 2019: The Eleventh International Conference on Emerging Networks and Systems Intelligence
- DATA ANALYTICS 2019: The Eighth International Conference on Data Analytics
- GLOBAL HEALTH 2019: The Eighth International Conference on Global Health Challenges
- CYBER 2019: The Fourth International Conference on Cyber-Technologies and Cyber-Systems

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

Published by IARIA XPS Press
Archived in the IARIA Digital Library
Prints available at Curran Associates, Inc.

In affiliation with the following journals:

Copyright © 2006-2020, IARIA