Important deadlines:

- Submission (full paper): June 25, 2017
- Notification: August 25, 2017
- Registration: September 10, 2017
- Camera ready: September 30, 2017

Tracks:

**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/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 MobiNets; 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; 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 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