



## CSNet 2023 – CALL FOR PAPERS

After the first successful edition of CSNet 2017 in Rio de Janeiro (Brazil), the second edition CSNet 2018 in Paris (France), the third edition CSNet 2019 in Quito (Ecuador), CSNet 2020 in Lausanne (Switzerland) (Online), CSNet 2021 in Abu Dhabi (UAE) (Hybrid), CSNet 2022 in Brazil, the seventh edition of Cyber Security in Networking (CSNet) conference will be held in Montreal (Canada) next October 16 – 18, 2023.

We are seeking full papers, short papers, and demos papers in cyber security for the networking domain. The driving theme at CSNet 2023 is **“the resilient networked systems and services”**.

The technological disruption is generating an impact on society and leading to a new industrial revolution. This social and industrial change presents new technological environments constituted by ubiquitous systems and large amounts of information, which requires a change in the way how cyber security is designed and developed. The use of artificial intelligence, machine learning, data mining, and data analytics provides additional tools for security analysts to face new forms of cybersecurity threats.

In today's highly connected world, networks and systems are expected to support a wide range of critical and vital services. Resiliency of such services, which includes cyber security, adaptability, and autonomy, will be a key driving factor for future networked systems.

### TOPICS OF INTEREST

The industry and academia research community will be invited to contribute with manuscripts describing novel, work-in-progress research on the design of solutions to relevant security issues on a wide variety of network security technologies. The topics of interest of the workshop include, but are not limited to

AI Technologies Applied to Cyber Security	Malware Attacks
Attacks on Virtualized Systems	Network and Operating System Administration for Security Purposes
Blockchain	Network Attached Storage
Cloud Security	Privacy and Responsibility in Digital Age
Cognitive Cyber Security	Resilient Networks and Systems
Cyber-attacks & defense	Secure Protocol Design and Key Management
Cyber-Physical System (CPS) Security	Secure Architecture Design
Cybersecurity and Human Rights	Secure Network Design
Data Center Network Control, Security, and Optimization	Security Policies Design
Decentralized Security	Security for the Internet of Things
Demilitarization Zone (DMZ)	Security in Fog/edge Computing
Disaster Recovery Plan	Security, Trust, and Privacy Challenges
Enterprise Network Security	Security for Vehicular Networks
Hardware-Based Attacks	Smart City Security
Intrusion Detection and Prevention Systems	Smart Grid Security
Industrial Control System Information Security	Smart Phones Privacy and Security
Integrated Network Security Hardware	Social Networks Security
Internet Content Filters	System Security for Wired and Wireless Networks
Internet Security Issues	Usable Security

### AUTHOR INSTRUCTIONS

Submitted papers must represent original material that is not currently under review in any other conference or journal, and has not been previously published. Papers accepted and presented at CSNet 2023 will be indexed in the IEEE Xplore Digital Library. Best papers will be invited to submit an improved version for publication in journal's special issue in the fields of the conference.

Papers must be submitted through EDAS: <https://edas.info/N30575>

### IMPORTANT DATES

#### Paper Submission Deadline

May 22nd, 2023

#### Notification of Acceptance

June 30th, 2023

#### Camera-ready papers

July 19th, 2023

### ORGANIZING COMMITTEE

#### General Co-chairs:

Carol Fung  
Concordia University, Canada

Augusto Neto  
Federal University of Rio Grande do Norte, Brazil

#### TPC co-chairs:

Nur Zincir-Heywood  
Dalhousie University, Canada

Changqing Luo  
Virginia Commonwealth University, USA

For more information, please visit  
<https://csnet-conference.org/2023>