National School of Cybersecurity (NSCS)

Information System Security Agency (ASSI)

Conference on Cybersecurity and Applications (CCA'2026)
25-26 November, 2026

Description

The National School of Cybersecurity (NSCS) and the Information System Security Agency (ASSI) are pleased to announce the organization of the 1st edition of the "***Conference on Cybersecurity and Applications (CCA'2026)***", which will take place on November 25th–26th, 2026 at The "National School of Cybersecurity", located within the "Scientific and Technological Hub Chahid "Abdelhafid Ihaddadene", Sidi Abdallah, Algiers".

Currently, cybersecurity has become a cornerstone of trust, resilience, and sovereignty. With the rapid evolution of digital technologies, industrial and critical infrastructures, financial systems, healthcare services, and national security are increasingly exposed to cyber-attacks. Research in cybersecurity is therefore of paramount importance to develop new approaches, tools, and strategies for protecting data, systems, and users against malicious activities.

The ***CCA'2026*** conference will focus on shaping the future of cybersecurity in Algeria. The event will offer academics, researchers, engineers, professionals and policymakers the opportunity to interact and exchange ideas, and present recent advances of their research results, projects, investigative works, industrial experiences and innovations, and build collaborative solutions that address both current and future challenges in such a rapidly changing fields. It aims to bring together researchers, academics, practitioners, students and professionals to discuss recent advances, challenges, and applications in the field of cybersecurity.

Tracks and topics

The ***CCA'2026*** conference is organized into four main tracks. Academics, researchers, practitioners, students, and professionals are warmly invited to contribute and to submit their original research articles, surveys, technical reports, and case studies on, but not limited to, the following topics:

- **Track 1: Cryptography, Privacy, and Trusted Digital Systems**
  - Cryptography and secure communications
  - Information-theoretic security in quantum systems
  - Quantum computing
  - Quantum-safe infrastructure
  - Quantum and post-quantum cryptography
  - Quantum hardware and implementation security
  - Blockchain algorithms, security and privacy
  - Secure, trusted and privacy-preserving architectures and protocols
  - Privacy and data protection
  - Trust frameworks and management models
  - Smart card security and authentication

- **Track 2: Artificial Intelligence and Cybersecurity**
  - Machine learning for cybersecurity and privacy
  - Adversarial machine learning
  - Privacy-preserving machine learning
  - Deep learning for security
  - Attack against federated learning
  - Threat and attack models
  - Intrusion and malware detection

- **Track 3: Systems, Networks, Industrial and Critical Infrastructures Security**
  - Network security and intrusion detection
  - Routing and quality of service
  - Cloud, fog and edge computing and security
  - Cybersecurity in IoT
  - Cybersecurity of 5G/6G networks and data protection
  - Data centers security
  - Cybersecurity in robotics and autonomous systems
  - Drone and drone networks security
  - Swarm-UAV security
  - Security of smart grid and smart city
  - Cybersecurity for cyber-physical systems
  - Cybersecurity for embedded systems
  - Industrial and critical infrastructures protection
  - Identity and access security management

- **Track 4: Cybersecurity Governance, Policies and Applications**
  - Cybersecurity fundamentals, frameworks and models
  - Cyber-defense strategies and policies
  - Cybersecurity education and training
  - Languages, awareness, and human factors in cybersecurity
  - Cyber-risk management and compliance
  - Digital forensics and incident response
  - Security and privacy in social networks
  - Applications of cybersecurity in industry, healthcare and finance

Important Dates
- **Submission opening:** 15 March 2026
- **Submission deadline:** 15 August 2026
- **Acceptance notification:** 30 September 2026
- **Camera-ready:** 20 October 2026
- **Registration deadline:** 02 November 2026
- **Conference date:** 25-26 November 2026

Paper submission guidelines

Papers must be original, not submitted or under consideration, unpublished, and must be written in English. Each paper should not exceed eight (08) pages, including figures and references, and must follow the IEEE conference template (PDF format).

All submissions will undergo a rigorous double-blind peer review process. Authors names and affiliations must be removed from the submitted manuscript. Acceptance will be based on quality, relevance, originality, and clarity of presentation.

Authors are invited to submit their contributions electronically in PDF format via the following link: https://cmt3.research.microsoft.com/CCA2026/

Registration fee
- **Academic staff/Researcher:** 10.000 DA
- **Industry professional:** 15.000 DA
- **Student participant:** 5.000 DA

A reduction of 50% will be applied for students and academic staff of the “Scientific and Technological Hub Chahid “Abdelhafid Ihaddadene”, Sidi Abdallah, Algiers”. Reduction is also applied to startup and self-employed professionals.

The registration fee covers:

- Participation in the technical program.
- Conference bag.
- Conference proceedings.
- 02 lunches.
- 03 coffee breaks.
- Participation certificate.

Contact

- **Host**: National School of Cybersecurity
- **Address**: Scientific and Technological Hub Chahid Abdelhafid Ihaddadene, Sidi Abdallah, Algiers, Algeria
- **Website:** https://www.enscs.edu.dz/?page_id=8994
- **Submission:** https://cmt3.research.microsoft.com/CCA2026/
- **Email:** cca@enscs.edu.dz