Call for Papers CyCon 2020

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

26 – 29 May
2020
Tallinn
Estonia

12th International Conference on Cyber Conflict: 20/20 Vision: The Next Decade

CYCON

CyCon, the International Conference on Cyber Conflict, is organised annually by the NATO Cooperative Cyber Defence Centre of Excellence. CyCon 2020 will take place from 26 to 29 May 2020, in Tallinn, Estonia.

CyCon 2020, entitled **20/20 Vision: The Next Decade**, will ask questions about how cyberspace and cyber conflict will continue to evolve in the 2020s. Can we see the future of the cyber domain? And if so, how precisely can we predict it? What are the new emerging technologies, policies and legal frameworks that will shape the future at societal and personal levels? New, often unpredictable, technological advances have been characteristic of the cyber domain from its very beginning; recent years have shown that unexpected side-effects have posed challenges to the way cyberspace has been developing so far. How can we ensure that the next decade's cyberspace, continuously open to technical innovation, will be more transparent, predictable, safe and secure, and still reflect our values? Is our vision clear and deep enough to understand and influence the way cyberspace might, or even must, evolve?

The theme of the CyCon 2020 conference should be considered as inspiring, not restricting. Original research papers are invited to address topical issues related to cyberspace and its security from technical, legal, policy, strategy and military perspectives. The submissions can address topics such as:

- Cyberspace governance
- Norms and standards to enhance security in cyberspace
- The role of international organisations, states and non-state actors in cyber security
- The new generation of national cyber security strategies
- The changing role of states in cyberspace
- Frameworks for collaboration and information-sharing
- Cross-border dependencies, trans-border access to data
- The nature of current and future cyber attacks
- Cyber capabilities, forces and weapons
- State-sponsored operations in cyberspace (incl. APTs and proxy actors)
- Military doctrine development, cyberspace as a domain of warfare
- Offence, defence and deterrence in cyberspace; active/responsive cyber defence
- Attack and defence of military systems
- Autonomous cyber weapon systems
- Cyber terrorism
- The evolution of the Internet of Things and its implications
- Vulnerability disclosure
- Cyber-physical systems security
- Critical infrastructure protection (incl. data diodes, IDS, industrial protocols and smart grids, 4G and 5G networks)

- Malware and botnets
- Hardware and software vulnerability mitigation
- Attacks on blockchain, smart contracts and DApps
- Artificial intelligence and cognitive cyber security (incl. data mining and machine learning, and AI supported cyber attacks)
- Cyber threat intelligence
- Cyber threats to space-based services
- Situational awareness and security metrics (incl. security visualisation)
- Attribution and digital forensics
- Digital trust and authentication
- New technologies for cyber exercises and cyber ranges
- Quantum computing and other emerging technologies

Legal aspects of cyber operations and other cyber activities relating to:

- international humanitarian law
- sovereignty
- principle of non-intervention
- espionage
- attribution
- international responsibility of states
- due diligence
- human rights (in particular the right to privacy, the right to freedom of expression, the right to protection of personal data)
- emergence of legal norms
- grey zones in international, national and EU law.

Important Dates

Abstract submission: 14 October 2019
Notification of abstract acceptance: 1 November 2019
Full paper: 6 January 2020
Author notification: 10 February 2020
Final paper: 9 March 2020
Contact address: cfp2020@ccdcoe.org

Publication

Authors are asked to submit a 200-300 word abstract of the planned paper, which should describe the topic and set out the main aspects and structure of the study. After a preliminary review, the authors of accepted abstracts will be requested to submit their full papers, which should be original and unpublished and should meet high academic research standards. Papers should be up to 6000 words, including footnotes and references. Submitted papers will be subject to a double-blind peer review.

Submission details, author guidance and other practical information are available at
https://ccdcoe.org/news/2019/cycon-2020-call-for-papers/
The abstracts and manuscripts must be uploaded electronically to
https://www.easychair.org/my/conference?conf=cycon2020 after creating an account. If you already have an existing EasyChair account, please log into your existing account before clicking on the link.

Authors of papers accepted for publishing in the conference proceedings are requested to make a corresponding presentation at the conference. Speakers will be offered travel (booked by NATO CCDCOE) and accommodation for the duration of the conference, as well as social events in Tallinn.
Proceedings and recordings of the previous CyCon conferences are available at https://ccdcoe.org/cycon/

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. This international military organisation based in Estonia is a community of currently 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law.