Call for Papers CyCon 2022

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

31 May – 3 June 2022
Tallinn
Estonia

14th International Conference on Cyber Conflict: Keep Moving!

CYCON

The International Conference on Cyber Conflict, CyCon, is organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). CyCon 2022 will take place from 31 May to 3 June 2022 in Tallinn, Estonia.

Coming out of the pandemic, it is time to stand up to new challenges while making sure issues that have remained or intensified during the global crisis do not paralyse us. We observe a constant evolution of technologies and threats, the next generation surely sooner or later becomes the current generation.

CyCon 2022's central theme **Keep Moving!** is to be understood literally and figuratively. Cybersecurity in transportation and in the supply chain is moving into the spotlight of the security community and is likely to define future battlegrounds. In an increasingly adversarial environment, the ability to deliver on military mobility, in spite of technical, infrastructural and legal obstacles, becomes evermore relevant. Autonomous technologies are not on the horizon anymore but move rapidly into our lives. How much autonomy and automation is acceptable though, before the technology becomes a threat? How to ensure that regulation at the national and international levels keeps pace with the fast moving reality? In a broader sense, how do we avoid being immobilized by the next crisis? How do we move in a coordinated manner?

We invite original unclassified research looking at the above topics and questions from the technical, legal, policy or military perspective. We particularly welcome papers focusing on, but not limited to, the following substantive areas:

- cyber security in transportation sector
- autonomous vehicles
- autonomous weapons systems
- supply chain security
- military mobility
- cyber security aspects of 5G and next generation technologies
- military use of 5G and next generation technology
- automated operations
- privacy and human rights in autonomous systems
- collaboration and information sharing frameworks
- international organisations cooperation
- public-private partnership in cyber defence
- artificial intelligence in military operations
- critical infrastructure protection (incl. data diodes, IDS, industrial protocols and smart grids, 4G and 5G networks, traffic and transportation)
- strategic approaches to emerging and disruptive technologies

- ripple effect of nation-specific approaches to sovereignty and international law
- crisis management and military-civilian cooperation in cyberspace
- cross-border dependencies, trans-border access to data
- the changing role of states in cyberspace
- state-led cyber operations, offensive/defensive aspects
- use of AI technology in state-led cyber operations and/or in crisis management
- emergence of new norms in international law
- NATO deterrence and defence posture
- developments in education and training for cyber operations
- vulnerability disclosure
- cyber-physical systems security
- malwares 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)
- artificial intelligence training
- cyber threats against and in the space domain – cross-domain dependencies
- NATO's cyber defence – emerging and disruptive threats; use of AI technology

Important Dates:

Abstract submission: 24 October 2021
Notification of abstract acceptance: 2 November 2021
Full paper: 9 January 2022
Author notification: 9 February 2022
Final paper: 9 March 2022
Contact address: cycon2022@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 invited to submit full papers. Only original research papers that have not been previously published will be admitted for review. Authors must specify CyCon conference track they are submitting their paper to: legal, strategy/policy, or technology. In case of doubt, consult CCDCOE in advance. The full submissions should have between 4000 and 6000 words, including abstract, footnotes, captions and references. Exceptions exceeding the maximum word count by more than 10% require prior consent by CCDCOE. Submitted papers will be subject to a double-blind review.

Submission details, author guidance and other practical information are available at https://ccdcoe.org/news/2021/cycon-2022-call-for-papers-now-open/.

The abstracts and manuscripts must be uploaded electronically to https://easychair.org/my/conference?conf=cycon2022.

Authors of papers accepted for publication in the conference proceedings will be requested to make a corresponding presentation at the conference. Speakers will be exempted from the conference fee and offered travel (booked by NATO CCDCOE) and accommodation for the duration of the conference.

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 34 nations, with expertise in the areas of technology, strategy, operations and law.