Call for Papers
CyCon 2023

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

30 May –
2 June 2023
Tallinn
Estonia

15th International Conference on Cyber Conflict: Meeting Reality

CYCON

CyCon, the International Conference on Cyber Conflict, is organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). In 2023, CyCon will take place from 30 May to 2 June 2023 in Tallinn, Estonia.

In 2022, a full-scale war returned to Europe, causing a paradigm shift in geopolitics, the scope of which is still being shaped. We see a convergence of traditional warfare with cyber operations and diplomatic efforts in the Ukrainian theatre. Its implications for cyberspace and cyber effects, as the components of a modern-day armed conflict, need to be analysed, evaluated and acted upon. At the same time, strategic competition in cyberspace grows and the use of cyber capabilities outside of armed conflict continues to expand.

The fifteenth iteration of the conference calls for stock-taking and perhaps re-assessment of the many assumptions, conclusions, and forecasts made in respect of and about cyberspace, technologies, and people using them. The theme of CyCon 2023 is “Meeting Reality”.

CyCon 2023 will challenge our assumptions about cyber conflict and associated technologies in general, in addition to their role in peacetime as well as crisis and conflict. Do our policies and legal frameworks stand the test of time? What technologies have turned out to be game changers and which have been overrated? CyCon 2023 encourages the discussion of concepts of cyber conflict as tested by real world events, addressing questions that might have appeared niche and theoretical just a few years ago, but now have proven to be of real life significance.

We call for original research papers offering technical, legal, strategical, and operational insight in the above context. Comparative analysis will be of particular interest this year. While a focus on the Russo-Ukrainian conflict will be an added value, we await papers on all uses of cyberspace relevant for the current scholarly debates.

We especially welcome papers addressing topics such as:

- Cyber effects in multi-domain operations and in conflict (concepts/tactics/characteristics/legal implications)
- National cyber strategies and policies in/for armed conflict
- Private companies as the providers of cyber infrastructure and protection
- Non-state actors - volunteers, hacktivists and cyber partisans
- Legal aspects of cyber recruitment
- Biometric data processing for identification or targeting purposes
- Use of drones (for combat or surveillance)
- Technical, strategic and/or legal questions related to the deployment of autonomous capabilities
- Cyber training needs before and during armed conflict
- Military (cyber) exercises

- Narrative control in/through cyberspace
- Information and intelligence sharing
- International law aspects of propaganda and influence operations
- (Cyber) neutrality in a globalized world
- (Cyber) cooperation vs competition between Russia and China
- Critical infrastructure security
    - Cybersecurity of industrial control systems
    - Secured 5G and next generation networks
    - Cybersecurity aspects of transport industry (maritime, aviation, railroad)
    - Satellite communication security
- AI use-cases in cybersecurity
    - AI-based intrusion detection systems
    - Secured AI military applications
    - AI-based malware detection and analysis
- Novel cyber-attacks and malware analysis in the context of Russo-Ukrainian conflict

Important Dates:

Abstract submission: 15 October 2022
Notification of abstract acceptance: 24 October 2022
Full paper submission: 8 January 2023
Author notification: 8 February 2023
Final paper submission: 8 March 2023

Contact address:

cycon2023@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/2022/cycon-2023-call-for-papers/

The abstracts and manuscripts must be uploaded electronically to
https://easychair.org/my/conference?conf=cycon2023

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