Call for Papers CyCon 2021

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

25 – 28 May 2021
Tallinn
Estonia

13th International Conference on Cyber Conflict: Going Viral

CYCON

CyCon, the International Conference on Cyber Conflict, is organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). CyCon 2021 will take place from 25 to 28 May 2021 in Tallinn, Estonia.

CyCon 2021's central theme is **Going Viral**. It alludes to the implications of human crises (such as the 2020 pandemic) for cybersecurity and cyberspace. At a more abstract level, it aims to encourage discussions on the impact of fast proliferation and high unpredictability in cyberspace. Whether they concern old threats such as malware or new trends affecting cyberspace such as information campaigns, these phenomena have major real-life implications. We need to acknowledge those, study them and strive to use them for our common benefit.

It often takes only a small change to produce great consequences in and through cyberspace. What are the dangers and what are the advantages of this ease of propagation? What is the role of the human element in advancing or thwarting the process? How do we maintain the ability to defend ourselves when the physical world comes to a halt? What can governments do in and through cyberspace to prepare for the next crisis? How can crisis management be helped or hampered by cyber means? Can law serve as a gatekeeper or is it an obstacle to technology development? Is it bound to always lag behind technological evolution? What legal and policy costs are we willing to pay when things go viral?

We invite original research that will offer technical, legal, policy or military perspectives on the above questions. We particularly welcome papers focusing on, but not limited to, the following substantive areas:

- The role of international organisations, states and non-state actors in cyber security
- The changing role of states in cyberspace
- Norms and standards to enhance security in cyberspace
- Frameworks for collaboration and information-sharing
- Cross-border dependencies, trans-border access to data
- Military doctrine development, cyberspace as a domain of warfare
- Critical information infrastructure and supply chain security
- Cyber security aspects of 5G technologies and military use of 5G technology
- Crisis management and military-civilian cooperation in cyberspace
- State-led cyber operations, offensive/defensive aspects
- Use of AI technology in state-led cyber operations and/or in crisis management
- Malign information campaigns in and through cyberspace
- Online education and new technologies for cyber exercises and cyber ranges
- Remote work and its cyber security implications
- International law responses to crisis situations
- Electronic surveillance in crisis management (national security/privacy implications)

- Due diligence and state responsibility for prevention of harm to other states
- Emergence of new norms in international law
- Internet of Things
- Vulnerability disclosure
- Cyber-physical systems security
- Critical infrastructure protection (incl. data diodes, IDS, industrial protocols and smart grids, 4G and 5G networks, traffic and transportation)
- 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: 4 October 2020
Notification of abstract acceptance: 19 October 2020
Full paper: 6 January 2021
Author notification: 10 February 2021
Final paper: 9 March 2021
Contact address: cfp2021@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. The papers should be up to 6000 words including footnotes and references and must comply with the CyCon style guidance issued together with this call for papers. The authors are strongly advised not to exceed the required word count by more than 10%. 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/2020/cycon-2021-call-for-papers/

The abstracts and manuscripts must be uploaded electronically to https://easychair.org/my/conference?conf=cycon2021

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