Call for Papers: Democracy and Cyberspace

2024 Conference on International Cyber Security

Leiden University, Institute of Security and Global Affairs | The Hague, the Netherlands | 12-13 November 2024

In 2024, an estimated 2 billion people will go to the polls in elections around the world, in what has been called the 'biggest elections megacycle so far this century'. This serves as a reminder that democracy is globally still one of the most prominent political systems, but also one that is under pressure: from undemocratic forces, domestic and foreign. The internet is a vital conduit for democracy: never have people had more direct access to political information and never has it been harder to ascertain the veracity and integrity of that information. Online disinformation and information operations have become vital tools for adversarial state actors seeking to discredit democracy as a system and who are happy to throw petrol on any fire that may destabilise elections and undermine trust in government and political institutions.

Given how online information spreads, democratic states need to look to internet platforms and 'Big Tech' companies to help stem the flow of malicious political disinformation and conspiracy theories. This introduces at least two problems for democracies in cyberspace. Firstly, it forces democracies – albeit indirectly – on the path to distinguishing between true and false information of import to their states and societies, which they have traditionally kept away from. In the UN negotiations on responsible state behaviour in cyberspace, likeminded states have always balked against the notion of information security, but are now seeking ways to address the problem of information operations that hit democracies the hardest. Secondly, it creates a dependency on the big internet platforms to act as an arbiter of legitimate information, which is politically awkward and runs up against the way platform algorithms work as well as how that feeds into their business model in which 'virality' is a good thing.

Additionally, as the grey zone of 'below the threshold' cyber conflict heats up through cyber operations varying from disinformation, subversion, espionage to sabotage, democracies find themselves on the backfoot again. Democracies governed by the rule of law do not enjoy unrestricted liberty to strike back at adversarial states below the threshold. While

they, or at least some, do engage in grey zone activities in cyberspace they are comparatively constrained by legal requirements and oversight. The democratic 'noblesse oblige' means that democracies can't, and should not want to, fight fire with fire. This is essential in light of the continued efforts to come to international terms on responsible state behaviour in cyberspace, but leaves democracies restricted in an operational response.

In 2024, we want to discuss democracy and cyberspace. What are the biggest challenges cyberspace poses for democracies and how can they respond? How can democracies further their agenda in international fora through the negotiation of rules and norms, and how does that stack up against state behaviour? What are strategies of adversarial states to destabilise democracies? How can democracies defend against them? What would be democratically and legally sanctioned ways to 'strike back'? How can democratic states work with and/or regulate internet platforms to help defend democracy? These, and many other related questions we hope to see asked and answered at the 2024 annual of The Hague Program on International Cyber Security.

This is the third annual academic conference of The Hague Program on International Cyber Security, which continues the proud tradition of the annual conferences of The Hague Program for Cyber Norms. We welcome all papers that have an interesting take on the theme of Democracy and Cyberspace. As always, we aim to bring together scholars from a diverse range of disciplines including – but not limited to – international relations, international law, economics, political economy, security studies, political sociology, philosophy, political science, science and technology studies and engineering. The key to understanding international cyber security lies in bringing together the various disciplines that relate to the theme in a broad sense. This call for papers is therefore open to extended abstracts from a wide range of academic disciplines.

The annual conferences of the Hague Program on International Cyber Security, and before that The Hague Program for Cyber Norms, has become a key multidisciplinary venue for peer-reviewed research in the study of cyber security and international stability. See our website for the program and impressions of the previous editions of the conference in 2018, 2019, 2020, 2021, 2022 and 2023.

We welcome extended abstracts of **maximum 500 words** on questions related to the theme of Democracy and Cyberspace in a broad sense. We explicitly welcome contributions from early career scholars. The conference will take place in The Hague on 12 and 13 November 2024. Authors of accepted extended abstracts should prepare their final paper by 15 September 2024. A best paper prize will be awarded. **Accepted contributors are eligible for funding for travel and lodging.**

THE HAGUE PROGRAM on International Cyber Security

Universiteit Leiden

HOW TO SUBMIT YOUR ABSTRACT

Abstracts can be submitted via email to conference@thehagueprogram.nl.

Please make sure your abstract submission meets the following requirements:*

- *Length: maximum 500 words!*
- *Format: .doc only!*
- *Blind review/anonymous – please leave out your name and other identifying details in the submission document*
- *Please mention separately in your email: name and current affiliation/position*

**If your abstract does not follow these requirements, it will not be taken into consideration.*

Important dates	
Submission of extended abstracts	15 May 2024
Notification of acceptance	7 June 2024
Submission of full paper (max. 6000 words excl. footnotes and literature – for references, please use Chicago Manual of Style (preferred citation format being author-date)	15 September 2024
Feedback by review committee	18 October 2024
Conference	12-13 November 2024