Moving Forward: Fragmentation, Polarization and Hybridity in Cyberspace

2020 Conference on Cyber Norms

Leiden University, Institute of Security and Global Affairs | The Hague, the Netherlands | 10-11 November 2020

Fragmentation, polarization and hybridity and are setting the scene for the debate about responsible state behaviour in cyberspace. These developments are neither new, nor fully understood, but they are set to play an important role on how to move forward in the diplomatic processes on international security and cyberspace. Fragmentation can cover a lot of different developments in cyberspace ranging from interference with core protocols and processes of the internet itself, to ideas of digital sovereignty that are aimed at 'national infospheres'. Polarization has increasingly become part of national and international politics. Domestic political tensions provide fertile soil for information operations. Geopolitical power play has become an integrated part of international politics in the past decade. Tensions between western countries and Russia and the fierce competition between the US and China extend into, and are reinforced, by the digital domain. These can make or break diplomatic agreement on norms of responsible behaviour in cyberspace. Hybridity, even though the term is often over inclusive, refers to the blurring of categories that were traditionally separate, such as those between civilian and military, overt and covert. It may also refer to a blurring of lines between interfaces, or online and offline worlds. The internet has proven to be an ideal 'space' to blur boundaries of a wide variety, for instance through the contested boundaries between the national and the international, and between technology and politics.

How will these developments play out as states and other stakeholders try to move forward on devising norms of responsible (state) behaviour in cyberspace? At the UN level, the debate itself has been fragmented and polarized, resulting in both a new UN GGE and an Open Ended Working Group (OEWG) with largely the same mandate. At the same time, it seems difficult to deal with (state sponsored) cyber and/or information operations that are neither peace nor war. If the debate can't be moved forward at the UN, it will likely move elsewhere, as it did after the 2017 round of the GGE failed. Will the world divide in different normative enclaves? Will other stakeholders step up to the plate? Will geopolitical tensions, state behaviour and power play in cyberspace become the main source of norms? Will there be a forum in which (state sponsored) attacks like NotPetya and WannaCry can be addressed?

In 2020, we hope to take the conversation about cyber norms further by taking these three macro-level developments – fragmentation, polarization and hybridity- and linking them to the

need to move forward in this debate, as the general theme for the annual academic conference of The Hague Program for Cyber Norms. As before, 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 the development of norms in cyberspace 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.

We welcome papers dealing with different aspects of fragmentation, hybridity and polarization (or combinations thereof) in relation to the question of how the debate on norms and (responsible) state behaviour in cyberspace develops and will develop.

The conference is the third in an annual series organised by The Hague Program for Cyber Norms and aspires to 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 for an impression of the 2018 and the 2019 edition of the conference.

We welcome extended abstracts of maximum 800 words on questions related to international cyber security and cyber norms. We explicitly welcome contributions from early career scholars. The conference will take place in The Hague on 10 and 11 November 2020. Authors of accepted extended abstracts should prepare their final paper by 14 September 2020. A best paper award will be granted.

Accepted contributors are eligible for funding for travel and lodging.

HOW TO SUBMIT YOUR ABSTRACT

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

Please make sure your abstract submission meets the following requirements*:
- Maximum 800 words
- Please mention: name and current affiliation
- Format: .doc or .pdf

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

Important dates	
Submission of extended abstracts	31 May 2020
Notification of acceptance	15 June 2020
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)	14 September 2020
Feedback by review committee	16 October 2020