Governing through crisis.

Conflict, crises and the politics of cyberspace.

2021 Conference on Cyber Norms

Leiden University, Institute of Security and Global Affairs | The Hague, the Netherlands | 9-11 November 2021

The Covid-19 pandemic has both stopped the world in its tracks as well as accelerated its pace digitally. As the world moved its daily life and work online to deal with the crisis, it also opened itself up to new cyber crises. The vulnerable health care sector was exposed to criminal and state attacks, vaccine manufacturers became subject to IP theft and espionage, and disinformation about Covid-19 muddied the national and international debate about the nature of the crisis and how to deal with it. The new digital 'normal' kept the world running, but also vastly increased the attack surface for malicious cyber actors. While some were trying to govern themselves through the crisis, others were using the crisis as a governance mechanism. 'Never waste a good crisis', comes in benign and in malicious shapes.

In cyberspace, crisis comes in many shapes and forms. Mis- and disinformation has created a crisis of trust in information and authority in many societies. For some states this is a governance problem, while for others it is an instrument of governance. New cyber operations keep shifting the goal posts on what is and is not acceptable behavior in cyberspace. Recent operations such as SolarWinds and the Microsoft Exchange hacks put pressure on the demarcation between cyber espionage and (military) cyber operations. Conceptual clarity is still very much subject to debate, with some analytical categories facing a crisis of their own. The field of UN cyber diplomacy has been governing itself through the crisis of the failure to reach consensus in the 2017 UN GGE by multiplying its processes. There is now an ongoing UN GGE, an OEWG process that reached consensus, a new OEWG round 2021-2025, a committee of experts to review the possibility of a UN cybercrime treaty and a proposal for a cyber Programme of Action (PoA) that is gaining support. All against a background of mounting geopolitical tensions and increased state cyber activity.

The relation between crisis and governance is inherently double faced. Crisis management is about preparedness, capacity and capacity building, resilience and more generally combining accurate threat and risk assessment with strategy, policy and resources. But crisis is also a method of governance: escalation can be a conscious political strategic choice, disinformation a policy tool and political and diplomatic fragmentation can be a positive

outcome depending on where you stand and what your interests are. Crisis can fragment and can unite, can be a centrifugal or a centripetal force.

In 2021, we want to place the conversation about cyber norms in the perspective of crises. How well equipped are the governance mechanisms and diplomatic processes that have been put into place to deal with crisis? What are the effects of a global crisis like Covid-19 on state behaviour(s), diplomatic behaviour and international cooperation in cyberspace? What strategies do states – and other actors – develop to deal with crises? How do states use crisis, or the opportunities shaped by crises, to further their own interests? Why do some states escalate and other de-escalate?

The current global health crisis inspired this theme, but this Call for Papers is not limited to that crisis alone. For the annual academic conference of The Hague Program for Cyber Norms we are interested in all papers that have an interesting take on the theme of international crisis, conflict, and the politics of cyberspace. 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.

The conference is the fourth in an annual series organised by The Hague Program for Cyber Norms which 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.

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 9 to 11 November 2021. Authors of accepted extended abstracts should prepare their final paper by 1 November 2021. A best paper award will be awarded.

Accepted contributors are eligible for funding for travel and lodging.

We are planning to organize a hybrid conference this year and we hope to be able to welcome accepted contributors who are able and willing to travel in The Hague this November. If this is not the case for whatever reason, online participation will also be possible.

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*:

- *600-800 words*
- *Please mention: name and current affiliation (if applicable)*
- *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 2021
Notification of acceptance	16 June 2021
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)	13 September 2021
Feedback by review committee	19 October 2021
Submission of final paper	1 November 2021
Conference	9-11 November 2021