Dealing with Uncertainty

2019 Conference on Cyber Norms

Leiden University, Institute of Security and Global Affairs | The Hague, the Netherlands | 5-6 November 2019

One way of looking at cyber norms for responsible behaviour is to see them as tools to deal with the uncertainties engrained in the fact that the internet now underpins our societies, economies, vital infrastructures and vital state processes such as elections. This uncertainty can result from the unpredictability of state behaviour – hence the focus on norms for responsible state behaviour – but it can also be traced to the impact of technological developments and/or (new) business models, un- and under-prepared organizations and individuals and a persistent lack of reliable data on the threats and risks to our digital societies. If uncertainty is a central characteristic of (digital) life, then how can states, companies and citizens deal with that uncertainty? How can public instruments such as (international) law, norms and confidence building measures (CBMs) but also private instruments such as insurance, liabilities and (technical) standards contribute to reducing and/or dealing with uncertainty? Also, if the frame of uncertainty and risk applies to international cyber security, then there should be room for categories of acceptable and residual risk in some categories of uncertainty, although we often lack a sense of what that might be. If the frame of (national) security applies, often triggering zero-sum thinking, there is arguably less tolerance for unaddressed uncertainties.

In 2019, we hope to widen the conversation about cyber norms by taking 'uncertainty' 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 in light of the uncertainties that characterize cyberspace lies in bringing together the various disciplines that it relates to. This call for papers is therefore open to extended abstracts from a wide range of academic disciplines.

More specifically, we welcome papers under the following headers, but the call is open for abstracts outside the scope of these clusters:

- **Sources of uncertainty.** Uncertainty can derive from many sources. Geopolitical developments and their translation to the cyber domain may increase uncertainty, technological innovations may be game changers for state-to-state conflict,

economic models and for the way societies function (disinformation, for example). Adding to the uncertainty is an unusual degree of obfuscation about threats and risks in cyberspace. There are many forms of secrecy in play because of the actors involved (such as intelligence agencies) and fear of tarnished reputations (for companies and other actors) contributing to a lack of reliable data and analysis.

- **Ways of dealing with uncertainty.** There are many ways to deal with uncertainty and not all of them have been tried and tested in the cyber domain. At the global and regional level international law and norms have been key strategies to seek to increase predictable state behaviour. At the (inter)national level resilience and capacity building are key, as are strategies of regulating emerging technologies by trying to strike a balance between safeguarding and promoting innovation, responsible use of technology and avoiding international escalation. Various risk management strategies should play a role in mitigating uncertainty at various levels (company, industry, national) and insurance schemes should – eventually – be able to take some low-level risks off the table. There is however much uncertainty about the usefulness of various strategies.

- **Goals of reducing uncertainty.** To what end do we aim to reduce or 'eradicate' uncertainty and to what extent is that possible or even desirable, given the inevitable trade-offs with other goals and values? Does uncertainty also serve a productive function?

The conference is the second 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 an impression of the 2018 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 5 and 6 November 2019. Authors of accepted extended abstracts should prepare their final paper by 16 October 2019. A best paper award will be awarded.

Accepted contributors are eligible for funding for travel and lodging.

THE HAGUE PROGRAM for Cyber Norms

Universiteit Leiden

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	20 May 2019
Notification of acceptance	12 June 2019
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 August 2019
Feedback by review committee	17 September 2019
Submission of final paper	16 October 2019