The Rule of Law in Cyberspace

In April 2019 the European Society of International Law [ESIL] Interest Group on Peace and Security organised a workshop as a side event to the ESIL Research Forum at the Georg-August-University Göttingen. The Research Forum addressed the topic of "The Rule of Law in International and Domestic Contexts: Synergies and Challenges" and for *Paulina Starski* and *Nicholas Tsagourias*, the Interest Group conveners, it appeared to be more than timely to focus on the concept of the "rule of law" in the context of cyberspace. The contributions to this Special Issue of the Heidelberg Journal of International Law are the product of the challenging papers presented at the workshop and reflect the interesting debates that took place in the course of the workshop as well as the comments and feedback that the organisers provided to the authors.

The contributions cover different aspects of the "rule of law" in cyberspace but all gravitate towards a common theme: the necessity to constrain the exercise of power (public or private) and to prevent the infringement of rights through regulation within the aterritorial sphere of cyberspace in which a plurality of actors interact.

Nicholas Tsagourias opens the stage by addressing the different challenges posed by cyberspace to traditional "rule of law"-ideas and sketches out how the concept of the "rule of law" could be operationalised in cyberspace to constrain the exercise of power – particularly by private actors – effectively. He puts forward a "*hybrid and networked rule of law*" concept which exhibits some of the traditional attributes of the "rule of law" but is also open and interactive regarding its participants and its properties.[1] *Henning Lahmann* presents a thorough analysis of "active cyber defense" policies implemented by states and the challenges which these pose in the legal respect.[2] Since the attribution of cyberattacks to specific entities is in many instances nearly impossible, states will – as *Lahmann* predicts – increasingly invoke necessity[3] as a circumstance precluding wrongfulness in order to establish the legality of their counteractions directed at neutralising cyberattacks. The "state of exception" which the invocation of necessity connotes – as *Lahmann's* core argument goes – will in the end undermine the "rule of law".[4] One means to uphold it would be the implementation of a "specific

[1] In this issue *N. Tsagourias*, 433 (445).
[2] In this issue *H. Lahmann*, 453 (454 et seq.).
[3] Art. 25 ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts (with commentaries) (UN Doc. A/56/10), YBILC II (2001).
[4] In this issue *H. Lahmann*, 453 (468 et seq., 476 et seq.).

emergency regime for cyber security incidents".[5] *Irene Couzigou* focusses on hacking-back measures employed by private companies. In that regard, *Couzigou* argues for enhanced state action: States should set up common criteria establishing which companies should be entitled to hack-back and supervise companies entitled to do so closely.[6] *Stephan Kolo*ß*a* views Facebook, one of the most powerful actors in the digital world, as the creator of "a new form of transnational legal order" governed by its own rules. This "order" could – in *Kolo*ß*a's* view – depart from normative stipulations integral to the "classical rule of law". In defining the substance of the "rule of law" *Kolo*ß*a* draws largely on *Lon Fuller*[7] by emphasising the aspects of clarity and publicity of rules and non-arbitrariness of decision-making.[8] The implementation of a more "rule-of-law-compliant structure" would necessitate – *Kolo*ß*a* suggests – a "democratic and human-rights-centred approach".[9] And, here again, the state comes into play: the regulative challenge posed should be addressed by states whose human rights obligations require them to take action in order to constrain the power exerted by platforms like Facebook. *Themis Tzimas* focusses in his contribution on Artificial Intelligence [AI] from the perspective of human rights. He argues for the activation of human rights "in order to impose checks and balances" regarding the development as well as the application of AI, the ultimate goal being the preservation of "the human-focus of [our] legal systems".[10]

Finally, *Andreas Kulick*'s contribution proposes a matrix which could assist in understanding the regulative challenges cyberspace poses.[11] He identifies four key questions: "Which Actor?"; "Who Governs How?"; "Which Legal Regime?"; and "Which Regulatory Paradigm?"[12] Indeed these questions and – most importantly – the answers given to them form variables of a (possible) regulative architecture of cyberspace. Which shape it will take requires a deeper inter- and transdisciplinary reflection.

Although the contributions to this Special Issue do not offer "cyber rule of law"-blueprints nor do they aspire to do so, they raise important questions and add layers of thoughtfulness to ongoing debates about the "rule of law in cyberspace".

PD Dr. iur. *Paulina Starski*

---

5 In this issue *H. Lahmann*, 453 (476).
6 In this issue *I. Couzigou*, 479 et seq.
7 *L. Fuller*, The Morality of Law, 1969.
8 In this issue *S. Kolo*ß*a*, 509 et seq.
9 In this issue *S. Kolo*ß*a*, 509 (529).
10 In this issue *T. Tzimas*, 533 (557).
11 In this issue *A. Kulick*, 559 et seq.
12 In this issue *A. Kulick*, 559 (561, 562, 564, 565).