HARVARD INTERNATIONAL LAW JOURNAL FRONTIERS
VOLUME 61 / 2020

CYBER SOVEREIGNTY: A SNAPSHOT FROM A FIELD IN MOTION

*Andrea Leiter**

This Post is the second in a new Frontiers series that critically explores the connection between international law and emerging technology, featuring the writing of scholars from a variety of disciplines affiliated with the Institute for Global Law and Policy (IGLP) at Harvard Law School.

This short article offers an overview of the most commonly held understandings of the notion of cyber sovereignty and attempts to push the research agenda with further questions. First, it outlines the regularly offered distinction between state sovereignty and platform sovereignty in cyberspace. However, instead of holding with this distinction, it presents cyber sovereignty as a techno-legal sphere characterised by claims to governance by states, companies, and individuals. With this angle, cyberspace appears as one of the most significant sites of our contemporary political and economic life. Second, while this contribution suggests that we should work with an analytic frame that embraces the intertwined character of cyberspace as techno-legal space governed by a multitude of different actors, the article argues that on a normative level, we still lack an in-depth understanding of the contradictory interests of the actors involved. We have not sufficiently grasped the power structures in cyberspace on either the economic or the political plane. The article suggests drawing on the tradition of critical legal scholarship to first map the field along a set of fundamental questions and then define legal strategies for redistribution and inclusion in cyberspace.

* Andrea Leiter is a Fellow in the Berlin Potsdam Research Group "International Rule of Law - Rise or Decline?"

I. JURISDICTION IN CYBERSPACE

The term cyber sovereignty stems from internet governance and usually means the ability to create and implement rules in cyberspace through state governance. One of the leading voices in internet governance, Bruce Schneier, has coined the term as the attempt of governments to take control over sections of the internet within their borders.[1] The 2017 *Tallinn Manual 2.0* constitutes one of the most important attempts to outline how existing international legal norms apply to cyberspace.[2] Governments discuss the question of cyber sovereignty through the lens of international law with concepts such as intervention, use of force, due diligence, and state responsibility. However, the relationship between data and territoriality challenges some of the most basic assumptions of the international legal order. As Fleur Johns puts it, these are "changes that amount, actually and prospectively, to a reconfiguration of territoriality in international law."[3] Rather than territorial boundaries and physical property, the new concerns relate to data access and technical proficiency.[4]

Yet, cyber sovereignty does not necessarily have to mean governance by a state. It first and foremost refers to the ability to create and implement rules in cyberspace. Alternatively, one could say it refers to the authority to speak the law, i.e., having *juris-diction,* in cyberspace. For the purposes of this article, I would like to challenge the assumption that sovereignty and jurisdiction are concepts exclusively reserved for states. I suggest understanding jurisdiction as a practice

---

[1] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 134 (2015).

[2] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017).

[3] Fleur Johns, *Data Territories: Changing Architectures of Association in International Law*, *in* NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 109 (2016).

[4] *See id.* at 115.

of claiming and engaging with law.[5] In cyberspace this means that protocols and codes in general are as much tools of law-making as is the regulatory apparatus of the state. This approach allows us to consider private legal arrangements, such as contracts (especially terms and conditions of large corporations), as exercises of jurisdiction. This idea is by no means new. As early as 1999, Lawrence Lessig published the book *Code and Other Laws of Cyberspace* in which he argues, by examples of copyright law, that a single dot is governed by the competing frameworks of law, norms, market, and architecture.[6] A more recent iteration of this idea can be found in Primavera De Filippi's and Aaron Wright's book *Blockchain and Law: The Rule of Code*, in which they suggest that "both public and private actors could potentially use blockchain technology to establish their own system of rules and regulations."[7] Thus, on an analytic basis, we should understand cyberspace as hybrid techno-legal governance. According to Goldenfein, "the idea of 'law' and 'technology' on alternate sides of a regulatory schematic needs replacing with an intertwined image of co-coordinating and co-constituting techno-legal regulation."[8]

Where it is clear that we need an analytic approach that understands and embraces the intertwined nature of techno-legal governance, the normative and political sides are not as straightforward. Cyberspace has long been a place for libertarian-minded technologists dreaming of a world without government interference. A strong example is John Barlows's *A Declaration of the Independence of Cyberspace*, published at the occasion of the World Economic Forum in Davos in 1996.

---

[5] *See generally* SHAUNNAGH DORSETT & SHAUN MCVEIGH, JURISDICTION (2012).
[6] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 123 (1999).
[7] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 193 (2018).
[8] JAKE GOLDENFEIN, MONITORING LAWS: PROFILING AND IDENTITY IN THE WORLD STATE 180 (2019).

He proclaims, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[9] A version of this idea with less pathos can be found in the Bitcoin Whitepaper of 2008 that first introduced cryptocurrency. The author, under the pseudonym Satoshi Nakamoto, pins the desire for autonomy on the notion of trust: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[10] Both of these prominent statements about cyberspace draw a picture of "us" versus "them"; "us" being the revolutionary technologists, versus "them" being the establishment usually represented through government institutions and often legacy systems.

In a similar manner, regulatory authorities view their task as regulation *of* technology and not regulation *through* technology. One of the best examples for this understanding is the reaction of governments towards blockchain technology. Attempts at prohibition were followed by attempts to apply old tools to new developments, such as the legal treatment of crypto currencies as either financial assets, property, or securities in different jurisdictions. The perception in both communities was one of threat, rather than opportunity. This mutual suspicion of the technology developers on the one side and governments on the other leads to a competition over jurisdiction or competition of sovereignties, which is often framed as a struggle between platform sovereignty and state

---

[9] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (1996), https://www.eff.org/cyberspace-independence.
[10] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008) https://bitcoin.org/bitcoin.pdf.

sovereignty.[11] The fundamental question is, who can claim to be the rulemaking authority?

II. LINES OF STRUGGLE IN CYBERSPACE

Thinking about rulemaking along the lines of "them" and "us" and overlooking the co-constitutive potential might seem banal and simplified. But this lens is nevertheless important because it points to the political questions involved. We should ask about the relationship between consumers and big companies that has emerged around big data. Through the collection of data, companies are producing ever more comprehensive profiles of consumers and thereby not only sell products but profoundly shape choices and affect lives.[12] Despite these changes, the relationship is legally conceptualised through terms and conditions agreements that understand consumers and companies as on par with private citizens. Building on the liberal mantra of choice, companies argue that their customers can choose not to participate or can choose a different provider. This approach hides the power asymmetry and the sheer impossibility for any individual not to participate in digital life. Thus, one direction for further research will inquire into the conceptualisation of the relationship between big companies and consumers and how consumers can be empowered towards meaningful choices and contributions.[13] Since nation states and local political organisations seem to operate on a mismatching scale vis-à-vis the corporate entities, this question would also involve the technical component and ask how new political communities could be organized to take advantage of new technologies.

---

[11] *See* ZI XIANG TAN, PLATFORMS AND STATES, GOVERNANCE AND SOVEREIGNTY, https://legaltechcenter.openum.ca/files/sites/159/2018/04/9.-Platforms-and-States-Governance-and-Sovereignty.pdf.

[12] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

[13] *See, e.g.*, ANNELISE RILES, FINANCIAL CITIZENSHIP: EXPERTS, PUBLICS, AND THE POLITICS OF CENTRAL BANKING (2018).

In a similar vein, we should analyse the relationships established in cyberspace through the lens of political economy.[14] What would the lines of class struggle look like, if considered through the data economy? Access to knowledge, meaning an understanding of how algorithms work and how they can be changed, has become the privileged knowledge of very few. Yet, precisely this information determines the value production and wealth extraction. Who benefits at which stage of the value chains in cyberspace? How does the data economy map into the North-South divide? How does data extraction differ from resource extraction and which legal forms enable the production of wealth, and for whom?

III. CONCLUSION

Legal scholars and practitioners often find themselves as representatives of clearly defined interests, usually either on the side of the regulatory institutions or in the role of a compliance officer, trying to fit technology into the regulatory schemes. However, since the current moment seems to be marked by a struggle for understanding, rather than clear negotiations of interests, it is also a particularly fruitful moment for intervention. If we understand how legal knowledge is used for the concentration of wealth and power,[15] this knowledge can be used towards redistribution and subversion. Legal scholars and legal practitioners should therefore not only be concerned with the question of who the sovereign in cyberspace is and what rules govern it but also try to design cyberspace as a space of participation and access.

---

[14] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2018).

[15] *See generally* KATHARINA PISTOR, THE CODE OF CAPITAL: HOW THE LAW CREATES WEALTH AND INEQUALITY (2019).