Introduction

Digital Transformations in Public International Law: An Introduction

Angelo Jr Golia, Matthias C. Kettemann, and Raffaela Kunz[*]

In the digital age and in the midst of a global pandemic, in which digital technologies have played a greater role than ever in all aspects of human interaction, editing a volume about the regulatory challenges the internet poses to public international law is almost a non-starter. Of course, there already exists an extremely rich body of scholarship in all sub-fields of the legal discipline and writing about the interface between international law and the internet is by no means a novel endeavour.

What prompted us to, nonetheless, start this project was that even more than ten years after the popularization of the term 'Internetvölkerrecht' ('international internet law' or 'international law of the internet'),[1] the myth of the internet as an unregulated space persists. In this sense, although the field is abundantly researched and much discussed, many fundamental questions remain open – and much disputed – from both an analytical and normative perspective. In this context, our aim was not (only) to analyse the application of public international law to the new regulatory fields that have emerged with the internet. Rather, our purpose is to bring out, explore, and critically assess the *impact* of the internet and digital technologies – that is, what we understand as the *digital transformations* – on the structures of public international law itself.

Indeed, processes of digital transformation have had a profound impact on the actors and instruments of international relations. The mode and the tools of stabiliszing the international normative order have changed significantly. Private actors have emerged and created important communication spaces with flanking normative orders in which processes of social self-determination take place.[2] The role and power relations of states have also changed in the digital constellation. From the initially unipolar post-

---

* The indicated order of authors is alphabetic.

1 See Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law,' Max Planck UNYB 10 (2006), 191–272 (192).

2 On the concept of normative order (of the internet), see Matthias C. Kettemann, *The Normative Order of the Internet. A Theory of Online Rule and Regulation* (Oxford:

Cold War world order, centred around the US hegemony, a system of global multi-polar power relations has emerged. Technological change is leading to structural reconfiguration in international political processes, which are particularly evident in global internet governance. From the cybersecurity challenges of the Internet of (Connected) Things to the algorithmic governance of opinion power for private profit maximization to the use of digital spying tools against journalists and civil rights activists, the protection of fundamental and human rights as a central benchmark of international politics, both internally and externally, is coming under pressure.

Democratic participation in these communication spaces requires access. The UN aimed to provide universal and affordable access to the internet in the least developed countries by 2020.[3] The German Government also committed itself to nationwide broadband expansion in the last coalition agreement.[4] Both goals were clearly missed. The pressure to act arising from human rights obligations continues unabated. In the light of increasing centrality – especially in times of COVID-19 – of online com-

---

Oxford University Press, 2020); and Matthias C. Kettemann (ed.), *Navigating Normative Orders. Interdisciplinary Perspectives* (Frankfurt/New York: Campus, 2020).

3 See UNGA Res 70/01 of 25 September 2015, Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1, Goal 9.c. Already in 2015, one of us (Kettemann) wrote a study on the international law of the web (Matthias C. Kettemann, *Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht* (Bonn: Friedrich-Ebert-Stiftung, 2015)). Among other things, that study found that states have agreed that building a people-centered, development-oriented information society can only work if the goals and principles of the United Nations Charter and respect for international law and human rights are taken into account. Even then, the study found that an international law of the internet already existed (in the sense that international law is to be applied to the internet and significant obligations can already be found in existing international law that states have to observe when shaping their digital policy).

4 The fact that the new 2021–2025 coalition agreement once again contains the phrase 'We strive for an international law of the Internet' ('Coalition agreement 2021–2025 between SPD, Bündnis 90/Die Grünen and FPD,' available at: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf, 144) without specifying what is meant by this and how it is to be achieved is surprising, especially since the global process of negotiating cyber norms, which is also being pursued significantly by Germany, is well advanced – as shown by the contributions to this book. See also Matthias C. Kettemann and Alexandra Paulus, 'An Update for the Internet. Reforming Global Digital Cooperation in 2021,' Global Governance Spotlight 4/2020, available at: https://www.sef-bonn.org/publikationen/global-governance-spotlight/42020.

munication for processes of social self-determination, the description of the European Court of Human Rights (ECtHR) has to be agreed with: 'the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest.'[5]

A further example of the many ways in which digital technologies affect the structures of public international law concerns the standards of evidence. Do tweets count as state conduct for the purpose of attribution under State responsibility?[6] In 2020 a WTO panel gave a positive answer for 'the tweets [that] are in fact governmental tweets.'[7] Similarly, in a request for the indication of provisional measures, the International Court of Justice (ICJ) has recently been presented with tweets ultimately tied to the Government of Armenia to probe an alleged disinformation campaign to spread ethnic hatred.[8] While it did not address the evidentiary value of the tweets as such, in its subsequent order, the ICJ granted the sought measures, noting that acts prohibited under Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (CERD) – such as propaganda promoting racial hatred and incitement to racial discrimination – can generate a pervasive racially charged environment within society, 'particularly (…) when rhetoric espousing racial discrimination is employed by high-ranking officials of the State.'[9]

But such transformations do not only concern disputes before international courts. In 2021, Germany and Italy were only the latest European countries issuing position papers on the application of international law

---

5 ECtHR, *Cengiz and Others v. Turkey*, judgment of 1 December 2015, nos. 48226/10 and 14027/11, para. 49.

6 For this issue, see Annalisa Ciampi, 'The Role of the Internet in International Law-Making, Implementation and Global Governance,' HJIL 81 (2021), 677–700 (690–694); as well as, in the specific field of international criminal law, the chapter by Rossella Pulvirenti in this volume.

7 WTO Panel, *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, report of 16 June 2020, WT/DS567/R, para. 7.161.

8 *Interpretation and Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Republic of Azerbaijan v. Republic of Armenia)*, Request for the Indication of Provisional Measures of Protection, 23 September 2021, paras 19–22, available at: https://www.icj-cij.org/public/files/case-related/181/181-20210923-REQ-01-00-EN.pdf.

9 ICJ, *Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Republic of Azerbaijan v. Republic of Armenia)*, Provisional measures, Order of 7 December 2021, para. 83, available at: https://www.icj-cij.org/public/files/case-related/180/180-20211207-ORD-01-00-EN.pdf.

in cyberspace,[10] following the example of other states. The coming decade will most likely see further attempts by states to develop their own 'internets,' controlled to different degrees by national governments. It would mean that the states will prioritisze protecting their interest and their citizens to prevent real or supposed dangers emanating from the use of the internet through censorship, mass surveillance, geo-blocking, etc. One of the results is that the potential of the internet as a truly global and borderless space is being put into question. Chien-Huei Wu has recently used the phrase 'sovereignty fever' to describe this territorial turn in the global cyber order.[11]

What does this mean for the global internet, and can (or should) international law be used to stop its fragmentation? Another related question concerns how such ongoing and accelerating politiciszation/territorialiszation of the internet contributes to transforming (the self-perception of) the main subjects of international law: not anymore – or not only – the self-contained units of the Westphalian/Vattelian order – based on stark internal/external divides – but rather macro-geopolitical units which increasingly act 'imperially,' that is, in terms of center/periphery.

Further, it remains very much an open question how the public interest and the common good on the internet can be protected and defended in times of 'platform capitalism' and mass surveillance. Indeed, private actors seem to hold as much power as never before, pushing the public-private distinction to its boundaries. It is a well-known fact that today it is big tech companies such as Facebook, Twitter, and YouTube who control the respect of freedom of expression and the prohibition of hate crimes on their channels. The result is a de-facto delegation of the protection of human rights to these private bodies with little public oversight, participation, and accountability.

These few examples show how, even after many years into debates about the relationship between international law and the internet, it is still necessary to measure the commitments made by states in 2003 in

---

10 See the position paper of the German Government 'On the Application of International Law in Cyberspace,' 5 March 2021, available at: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; and the position paper of the Italian Government 'International Law and Cyberspace,' 4 November 2021, available at: https://www.esteri.it/MAE/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

11 Chien-Huei Wu, 'Sovereignty Fever: The Territorial Turn of Global Cyber Order,' HJIL 81 (2021), 651–676.

the framework of the World Summit on the Information Society, to achieve 'people-centered, inclusive and development-oriented Information Society […] premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.'[12]

Indeed, one of the main questions is how the internet changes the ways in which human rights are mobiliszed and/or implemented globally. In this context, ensuring human rights is a key aspect of legitimiszing normative orders. At least since 2006, the protection of human rights on the internet has been closely studied,[13] with freedom of expression identified as the key 'enabling' right.[14] The importance of ensuring human rights on the internet globally has been recognized on the UN level, where states confirmed their obligation to respect rights offline just as online.[15] This is an important precedent for procedures to establish internet-related duties of states based on existing international law. Indeed, the international monitoring of human rights violations online, through filtering and blocking, gave rise to early analyses of the international legal duties of states regarding the internet.[16] Questions of internet access and the bridging of

12 World Summit on the Information Society, 'Declaration of Principles. Building the Information Society: a global challenge in the new Millennium,' WSIS-03/GENEVA/DOC/4-E, 12 December 2003, Principle A.1. See also Nula Frei, 'Equality as a Principle of the Networked World? An Exploratory Search for 'Cyber-Equality' in the Field of Internet Governance,' HJIL 81 (2021), 627–650 (640–643).

13 Rikke F. Jørgensen (ed.), *Human Rights in the Global Information Society* (Cambridge: MIT Press 2006).

14 Dragos Cuceranu, *Aspects of Regulating Freedom of Expression on the Internet* (Antwerp: Intersentia 2012); Wolfgang Benedek and Matthias C. Kettemann, *Freedom of Expression on the Internet* (Strasbourg: Council of Europe 2014). See also, Molly Land, 'Toward an International Law of the Internet,' HILJ 54 (2013), 393–458.

15 See the Human Rights Council Resolution 'The promotion, protection and enjoyment of human rights on the Internet,' UN Doc. A/HRC/RES/20/8 of 5 July 2012; and, more recently, the Human Rights Council Resolution 'The promotion, protection and enjoyment of human rights on the Internet,' A/HRC/RES/32/13 of 18 July 2016. For an introduction, see Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books 2012) and Rikke F. Jørgensen, *Framing the Net. The Internet and Human Rights* (Cheltenham: Edward Elgar Publishing 2013).

16 Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge: MIT Press 2008); Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge: MIT Press 2010); Ronald Deibert, John Palfrey, Rafal Rohozinski

the digital divide have also led to research on the international duties of states regarding infrastructure development.[17]

Against this backdrop, in spring 2020, we started a collective project at the Max Planck Institute for Comparative Public Law and International Law in Heidelberg and subsequently issued a call for papers in which we identified three macro-questions that in our opinion still warrant further research:

1) What influence does 'the internet' (information and communication technologies and the socio-legal changes they have brought) have on international law and international legal scholarship?
2) Conversely: What impact does international law – treaties, custom, principles, procedures, actors, legitimacy conceptions – have on the development (the fragmentation or integrity) of the internet? How does the geographical and geopolitical dimension of international law affect the unity and/or fragmentation of international internet law?
3) Finally: How does the interface between international law and the internet affect the relationships and the power balance between the Global South and Global North, in terms of positive law, participation in processes of norm development, hegemonic structures in scholarship, and participation in the epistemic communities of international internet law?

The response to the call was extremely generous, both in quantitative and qualitative terms, and we decided to organize the submissions addressing different aspects of these questions in two distinct publications. This book is the second scientific output of our project, after a special issue of the *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* (the Heidelberg Journal of International Law) published in Autumn 2021.[18] Importantly, we thought and shaped these two publications as complementing parts of a single, coherent research project which should be read accordingly, that

---

and Jonathan Zittrain (eds), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge: MIT Press 2011).

17 Nivien Saleh, *Third World Citizens and the Information Technology Revolution* (London: Palgrave Macmillan 2010); Gaëlle Krikorian and Amy Kapczynski (eds), *Access to Knowledge in the Age of Intellectual Property* (Cambridge: MIT Press 2010).

18 Angelo Jr Golia, Matthias C. Kettemann, and Raffaela Kunz (eds), 'Special Issue: International Law and the Internet,' HJIL 81 (2021), 597–866, available at: https://www.nomos-elibrary.de/10.17104/0044-2348-2021-3/zeitschrift-fuer-auslaendisches-oeffentliches-recht-und-voelkerrecht-heidelberg-journal-of-international-law-volume-81-2021-issue-3.

is, in dialogue with each other. This book, in particular, focuses on aspects that can be grouped under the four guiding ideas of sovereignty, security, rights, and participation.

Part I explores the impact of digital technologies on (the conceptualization of) sovereignty as one of the *topoi* of international legal thinking.[19] To be sure, even this topic can be addressed through many different lenses, for example (the preservation of) the open cyberspace as a global public good[20] or broader geopolitical analyses.[21] Here, *Pia Hüsch* discusses the application of state sovereignty in cyberspace and analyzes the usefulness – and limits – of analogies in this area. At a time when reflections on the real-world impacts of legal metaphors and fictions are becoming increasingly relevant,[22] she comes to the conclusion that analogies and metaphors often lead to more confusion rather than clarification and recommends that, at times, a straightforward analysis of sovereignty in cyberspace is preferable.

Yet another perspective focuses on the traditional link between sovereign entities and constitutions. How and to what extent does the digitalization of social relations contribute to putting further into question the genetic link between states and constitutionalization? What lessons can global constitutionalism scholarship give to the *digital* constitutionalism field? While other approaches focus on phenomena of self-organization and self-regulation in the digital sphere,[23] in the second chapter of this book *Edoardo Celeste* notes that international law theory already projected the notion of constitution beyond the state dimension, helping explain how the emergence of globalized problems in the digital ecosystem necessarily engenders the materialization of a plurality of constitutional responses. The sense of this Gordian knot – he argues – can be deciphered only if these emerging constitutional fragments are interpreted as complementary tesserae of a single mosaic.

---

19 See, in most recent literature, Neil Walker, 'The Sovereignty Surplus,' ICON 18 (2020), 370–428; and Fleur Johns, 'The Sovereignty Deficit: Afterword to the Foreword by Neil Walker,' ICON 19 (2021), 6–12.

20 Cf. Rolf H. Weber, 'Integrity in the 'Infinite Space'– New Frontiers for International Law,' HJIL 81 (2021), 601–626.

21 Cf. Wu (n. 11).

22 Cf. Alessandro Morelli and Oreste Pollicino, 'Metaphors, Judicial Frames and Fundamental Rights in Cyberspace,' AJCL 68 (2020), 616–646.

23 Cäcilia Hermes, 'Cyberspace as an Example of Self-Organisation from a Network Perspective,' HJIL 81 (2021), 817–839. See also Michael A. Cusumano, Annabelle Gawer, David B. Yoffie, 'Can Self-Regulation Save Digital Platforms?,' Industrial & Corporate Change, Special Issue 'Regulating Platforms and Ecosystems' (2021).

Part II turns to security issues. Indeed, as use of force, sanctions, non-interference in domestic affairs lie at the very core of traditional public international law – as inter-*state* law – the internet and digital technologies have also radically changed the way international law deals – has to deal – with security, at both regional and global levels. Although the legal treatment of cybersecurity goes well beyond the traditional issues of collective security,[24] how international law conceptualizes and regulates sanctions in the digital sphere remains an open question, especially when it comes to regional regimes. In the third chapter, *Uchenna Jerome Orji* offers an original analysis of the 2005 African Union Non-Aggression and Common Defense Pact,[25] exploring the potential of this instrument to govern the behavior of Member States with respect to activities that can constitute aggression in cyberspace. In particular, he makes a case for the application of the Pact's principles to promote responsible State behavior in cyberspace, based especially on the need for legal certainty.

Moving to a more global perspective, in the fourth chapter *Alena Douhan* starts from the analysis of UN Security Council resolutions 2419(2018), 2462(2019), and 2490(2019) in order to develop her reflections on the legal qualification of cyber attacks and the application of cyber measures. In particular, she provides an overview of different scenarios where the application of sanctions is affected by the emergence of cyber technologies. She also focuses on the changes in and legal qualifications for the grounds, subjects, targets, means, and methods of introduction and implementation of sanctions regimes in the digital age.

Part III explores the implications of the internet for the protection of rights at the international level. Especially in the early years of the internet, there was great enthusiasm about the potential of the internet, which provided unseen global spaces for communication and exchange for the protection and improvement of human rights. However, the darker sides also accompanying this development soon came to light.[26] While the so-called Arab Spring was seen by many as witnessing the liberating potential of the internet, at the latest, the atrocities and possibly genocidal acts committed against the Rohingya in Myanmar showed that the development could

24 Cf. Antonio Segura-Serrano, 'Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development,' HJIL 81 (2021), 701–731.

25 AU Non-Aggression and Common Defense Pact (Addis Ababa, 2005), opened for signature 31 January 2005 (entered into force 18 December 2009).

26 In most recent literature, see only Tiberiu Dragu and Yonatan Lupu, 'Digital Authoritarianism and the Future of Human Rights,' International Organization 75 (2021), 991–1017.

very well also go in the opposite direction. More recently, the dispute between Armenia and Azerbaijan before the ICJ recalled above[27] shows how digital technologies might offer governments new and more sophisticated possibilities for disseminating hatred and possibly pave the way to genocidal acts.

In the fifth chapter, *Stefanie Schmahl* examines from the general perspective the opportunities and challenges that digitaliszation offers to human rights law. In an impressive *tour de force*, she provides an overview of the main issues in this context, ranging from the question of whether there is a right to access the internet to new challenges arising for the protection against discrimination through the use of algorithms and discussions about cyborgs and robots as new rights holders or duty bearers. Her contribution, in particular, assesses to what extent the digital environment *critically* challenges the functioning of the international human rights regime.

In the sixth chapter, *Rossella Pulvirenti* examines these questions from the specific perspective of international criminal law. She argues that while the internet has changed international armed conflicts and thus brought new challenges, at the same time, it has become an invaluable tool in the fight against crimes committed. She concludes that, overall, the internet and digital tools have had a positive influence on International Criminal Law and the gathering of evidence before International Criminal Courts and Tribunals, as it gives individuals the power to gain control over the information and evidence that are then forwarded to the international criminal courts and tribunals; and strengthens the outreach programmes enhancing the quality and the quantity of data released via the internet by the tribunals to local communities.

In the seventh chapter, *Adam Krzywoń* addresses what has long become a classic in the field of 'international internet law,' that is, the (limits to the) freedom of expression online and the related obligations of states, an issue that unavoidably touches upon the role of private (business) actors.[28] At a time of ever-growing attempts to regulate (and exploit) the systemic position reached by private actors in the field of online content moderati-

27 ICJ, *Azerbaijan v. Armenia* (n. 9).

28 On the international law framework concerning online business actors, see Christine Kaufmann, 'Responsible Business in a Digital World – What's International Law Got to Do With It?,' HJIL 81 (2021), 781–815; as well as Hans-W. Micklitz and Aurelie Anne Villanueva, 'Responsibilities of Companies in the Algorithmic Society' in: Hans-W. Micklitz et al. (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge: Cambridge University Press 2022), 263–280.

on – especially at the European level –[29] his analysis focuses on states' obligations under the specific framework of the ECHR. In particular, he argues that a strict distinction between negative and positive obligations is anachronistic and that the negative understanding of the freedom of expression and protection of privacy does not provide the conceptual apparatus to deal with many current problems.

Finally, part IV sheds further light on questions of participation via digital tools. This is a central issue that goes well beyond debates on the right to access the internet and the dynamics of individual inclusion/exclusion triggered by the digital revolution; or the principle of equality within the digital sphere.[30] Again, the internet, in unprecedented ways, provides global spaces for communication, mobilization, conflict, and deliberation. The digital sphere radically changes the codes and dynamics, sustaining the generation of (political) consensus. Put differently, the digital revolution requires broader legal reflections – involving *also* public international law – on the conditions through which consensus to the purposes of collective decision-making in modern interconnected societies may be generated, especially when it comes to issues (e.g., climate) with an intrinsic global reach. There is, of course, the vast literature on the impact of digital technologies and algorithms on political processes and participation, with several and sometimes contrasting views on whether such new technologies contribute to positive or negative developments.[31] However, the present volume aims to contribute to the debate with a perspective that at least in part transcends well-established analyses on (de-)democratization processes at the national level. Indeed, we have decided to conclude the volume with two contributions that, in different ways, offer a more global perspective, linking issues related to participation/democratization, digital technologies, and climate.

In particular, the chapter by *Katharina Luckner* offers an analysis of how in certain cases, the internet may sustain bottom-up processes and

29 See the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.

30 See again Frei (n. 12).

31 For different perspectives, see among many Oren Perez, 'Electronic Democracy as a Multi-Dimensional Praxis,' North Carolina J. Law & Technology 4 (2003), 275–306; Dragu and Lupu (n. 26); Ngozi Okidegbe, 'The Democratizing Potential of Algorithms?,' Conn. L. Rev. 53 (2021), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835370.

their relevance to public international law. She starts from the observation that through the internet, most inhabited places in the world are a mere click away, which greatly facilitates the constitution of social movements with relevance way beyond their local context. She then uses the 'Fridays for Future' movement as a case study and, drawing from legal, political science, and media studies, shows how social media enables the impact of civil society movements on the development of international law.

Relatedly, in the same context of democratization and social mobilization, a field that has gained a particularly central standing is the so-called strategic human rights litigation. This has proved increasingly relevant to international legal scholarship, especially when it comes to climate legal activism. In the last chapter of this volume, *Vera Strobel* takes a closer look at a relatively underexplored issue, that is, the interplay between strategic litigation and the internet. She argues that the internet has played a multidimensional role in strategic litigation activities and their influences on society, international legal scholarship, and the development and interpretation of public international law itself.

This is not the end of the debate on how to apply international law to the internet and how the internet impacts international law. But perhaps it is the end of the beginning, as we progress to a more nuanced and mature picture of the challenges to the norms and normative actors, institutions, and institutional practices of international law in the digital age. The rules might be digitalized now, and their enforcement partially problematic, but the underlying questions remain similar: from the first four paragraphs of the Code Hammurabi onwards, the rules on how rules are developed and what may be said play a central role in the earliest codifications of the law; and in modern times, citizens' participation in these rules can be seen as a central demand and great achievement of many democratic revolutions. But what about our participation in communication-related decisions on digital platforms today, where significant parts of our public discourse have shifted? Well-established democratic principles do not easily translate to allow users' participation in shaping private selection algorithms and moderation practices. The platforms themselves have become rule-makers, rule-enforcers, and judges of their own decisions. The separation of powers looks different. Communication power or democratic power control (i.e., neither checks nor balances) leads to tensions in the inner fabric of public discourse. International law can alleviate some of this tension, as the contributions to this book show.

They have also shown that online, just as offline, (international) law applies. *Ubi societas, ibi ius* was true in ancient Greece, China, Africa, and South America. It is true today 'online.' Or as Malcolm N. Shaw put it

in the first lines of his introduction into international law: 'in the long march of mankind from the cave to the computer a central role has always been played by the idea of law – the idea that order is necessary and chaos inimical to a just and stable existence.'[32] What we are seeing, and struggling with, therefore, is not the fact that international law applies to the internet and is changed by it, but rather the speed of change.

It took 200 years, Niklas Luhmann recalled, until the disruptive potential of the printing press started to influence all segments of society, eventually leading to a fundamental change in the structure of Western European societies.[33] With the internet having started some fifty years ago (and commercialized social media landscapes emerged in essence only twenty years ago), we will have to wait and see whether the internet has a disruptive potential similar to that of the printing press. We believe it will, and the contributions to this book set the tone and can help steer the debate on the relationship of this development with international law.

32 Malcolm N. Shaw, *International Law* (8th edn, Oxford: Oxford University Press 2017), 1.

33 Niklas Luhmann, *Die Wissenschaft der Gesellschaft* (Frankfurt am Main: Suhrkamp 1990), 600; See also Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Cheltenham: Edward Elgar 2015) 159 ff. (distinct characteristics of modern law were triggered by the printing press).