German Law Journal (2023), **24**, pp. 438–460
doi:10.1017/glj.2023.31

ARTICLE

Special Issue: International Law and Digitalization

Does Digitalization Change International Law Structurally?

Dana Burchardt

Free University of Berlin, Germany
Email: dana.burchardt@fu-berlin.de

(Received 11 April 2023; accepted 11 April 2023)

Abstract

The article provides a meta-analysis of the structural impact of digitalization on international law. It synthesizes the contributions of this special issue, showing how their findings are interrelated and which cross-cutting trends we can observe. It uses an analytical framework designed to assess structural changes in international law by analyzing the impact that digitalization has on key reference points: Actors, norms, and values. From this assessment, it draws the conclusion that digitalization is changing, and will continue to change structural features of international law.

Keywords: Digitalization; international law; change; actors; norms; values

A. Introduction

Digitalization has the potential to change law, including international law, in a fundamental manner. We are only gradually realizing the extent to which it could alter norm-application and even norm-creating processes as well as the functions of law. This article aims to dig deeper into the structural impacts that digitalization has on international law, and thus contributing, with this meta-analysis, to the emerging body of literature on digitalization and international law.[1] Rather than assessing this impact for a specific field of international law, the article takes a bird's eye perspective, looking at the overarching developments that can be discerned. To provide this perspective, the article synthesizes the contributions of this special issue and shows how their findings are interrelated. It uses an analytical framework designed to assess structural changes in international law by analyzing the impact that digitalization has on key reference points: Actors, norms and values. From this it is possible to draw general conclusions about the structural impact of digitalization on international law as a legal space.

[1]Examples of the scholarship that assesses more generally the relationship between digitalization and international law include: Nicholas Tsagourias & Russell Buchan, Research Handbook on International Law and Cyberspace (2d ed. 2021); Matthijs M. Maas, *International Law Does Not Compute: Artificial Intelligence and The Development, Displacement or Destruction of the Global Legal Order*, 20 Melbourne J. Int'l. L. 29 (2019); Thomas Burri, International Law and Artificial Intelligence, 60 Ger. Y.B. Int'l L. 91 (2017). For a discussion of international law and technology in general, see Colin B Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 Cardozo L. Rev. 149 (2001). Regarding the impact of digitalization on key features of global policy, Fleur Johns, #Help: Digital Humanitarianism and the Remaking of International Order (forthcoming 2023).

First, the framework used to assess the structural impact of digitalization on international law is outlined, defining the key terms that shape the relationship of digitalization and law, and describing the reference points used in this contribution to assess structural change. Second, based on this framework, the main part of the article traces and categorizes the structural impacts that digitalization has on international law.

B. Assessing the Structural Impact of Digitalization

I. Digitalization and the Law

Digitalization and related notions are not defined in a uniform manner throughout disciplines, contexts, and authors.[2] At the same time, these notions are often presupposed as a given, without authors defining them explicitly for their purposes. Taking these practices into account, digitalization is understood broadly in the present contribution. It refers to the impact of digital technologies on international law. Technologies are qualified as digital here when they are based on binary coding. This makes it possible to include various aspects of digitalization that can be grouped into two subsets: an interactive space created by digitalization, and tools for the automatization of tasks.

First, *cyberspace* refers to the space created by computer networks.[3] It is a space that has been created by digital technology and digital means are used to communicate and act within this space.[4] While being based on a physical infrastructure of computer networks, cyberspace is (also) non-physical in nature and thus relates to the notions, "virtual" and "virtual reality," which for some are characteristic for digitalization. As a space, cyberspace is a framework in which actors interact.[5] Cyberspace is often equated with the Internet, although other computer networks can create a cyberspace as well. Given its societal and economic, as well as growing political, importance, the Internet provides the bulk of phenomena considered under this aspect of digitalization. This includes the manner in which actors use the Internet as well as its regulation. Cyberspace as an environment or *room of interaction* that potentially differs from the analogous sphere of interaction is addressed here.

A second aspect of digitalization looks more closely at the *tools* that can be created by digital technology. This includes the *automatization* of decision-making and of actions, in particular by using artificial intelligence based on (self-learning) algorithms. Specifically, the latter term distinguishes between natural intelligence that is characteristic for (some) living beings, including humans, as compared to artificial intelligence that is constructed and does not stem from the natural environment.[6] Automatization is thus characterized by an "independence of systems in relation to direct human control."[7] Digital tools in the context of automatization are connotated as being opposite to human decision-making and actions. A relevant notion in this context is also Big Data, a term that refers to a big volume and variety of data which is created with great velocity and assessed by digital tools such as machine learning.

[2]Authors stress different aspects of digitalization, e.g., digital as opposed to analogous and including hardware, software and infrastructure, Deborah Lupton, Digit. Socio. 7 (2015); the "system" dimension of digitalization and digital technologies, Hin-Yan Liu, *The Digital Disruption of Human Rights Foundations*, *in* Human Rights, Digital Society and Law 75, 76 (Mart Susi ed., 2019); the juxtaposition of digital and physical word, Miloon Kothari, *The Sameness of Human Rights Online and Offline*, Human Rts, Digit. Soc'y & L. 15 (Mart Susi ed., 2019).

[3]On the notion of cyberspace as space, Julie E. Cohen, *Cyberspace as/and Space*, 107 Colum. L. Rev. 210 (2007).

[4]*See* Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in* Research Handbook on International Law and Cyberspace 55 (Nicholas Tsagourias & Russell Buchan, eds., 2015).

[5]On the "social layer of cyberspace," Nicholas Tsagourias, *The Legal Status of Cyberspace Sovereignty Redux*, *in* Research Handbook on International Law and Cyberspace 9, 12 (Nicholas Tsagourias & Russell Buchan eds., 2d ed., 2021).

[6]On the difficulties of defining artificial intelligence, Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 Harv. J. L. & Tech. 353, 359 (2016).

[7]Stefan A. Kaiser, *Legal Challenges of Automated and Autonomous Systems*, 60 Ger. Y.B. Int'l L. 173, 175 (2017).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

The abovementioned dimensions of digitalization can relate to law in two ways. First, cyberspace and automatization can be the *object of regulation*. The range of possible regulation is broad. For example, law can determine the situations and extent to which automatization can be used to replace or complement human action and what the consequences of such automatization are, including in terms of accountability and liability. Law can further regulate how actors can use the cyberspace or parts of it, how they can interact among each other, and which tools they can use within this space. Second, in addition to being the object of regulation, digitalization can provide the *means*, or even the agents, for norm-setting and law application, including monitoring of legal obligations. Automatized decision-making and artificial intelligence (AI) as an agent with (quasi) legislative, administrative, or judicial functions are key aspects of such a way in which law and digitalization can interrelate.[8] The way in which the interrelation between digitalization and law is approached has for some time centered on the first aspect. However, due to ongoing technological advancements, the second aspect is coming into more prominent focus. In the present contribution, both aspects are included in the assessment.

1. Structural Changes in International Law

In this article, I narrow down the interrelation between digitalization and law in a twofold manner. I focus on international law as specific legal space rather than assessing the impact of digitalization on law in general. The specificities of international law in the digital context are analyzed, while nevertheless keeping the comparison with other areas of law in mind to highlight where developments are indeed specific to international law.

Moreover, when assessing the impact of digitalization on international law, this article concentrates on a certain kind of impact: *Structural changes* to international law that are caused, fostered, or enabled by digitalization. While law has both a static and dynamic dimension so that change is one of its inherent characteristics, changes can be of different intensity and extensity, and they can concern fundamental or rather peripheral elements of a legal space. Here, the focus is on the structural impact, that is, on changes that concern features of international law that are relevant for international law as a whole, rather than being specific to some areas of international law. These features embody meta-aspects that determine the legal space. Further, structural change is approached as a gradual notion. Each structural feature can change to different degrees. In addition, it is possible that only one structural element changes or, alternatively, that several elements change at the same time. Finally, structural features can also develop into diverging directions.

The framework used in this article to analyze structural shifts is three-fold. It includes the impact of digitalization on three structural features of international law: The legal actors involved, changes regarding foundational characteristics of the legal norms, and changes regarding underlying values.[9]

When assessing the *actors* dimension, various issues are relevant. Aspects to assess include whether certain (groups of) actors are able to participate in regulatory processes and adjudication. It also includes whether and to what extent they can exercise influence as compared to other actors involved, that is, whether they can shape the law when setting legal standards and applying them.

[8]For examples of the domestic legal debate, see, e.g., John Morison and Adam Harkens, *Re-Engineering Justice? Robot Judges, Computerised Courts and (Semi) Automated Legal Decision-Making*, 39 Legal Stud. 618 (2019); Joshua P. Davis, *Law Without Mind: AI, Ethics, and Jurisprudence* 55 Cal. W. L. Rev. 165 (2018); Anthony J. Casey & Anthony Niblett, *Self-Driving Laws*, 66 Univ. Toronto L. J. 429 (2016); contributions in 68 Univ. Toronto L. J., Supplement 1: Artificial Intelligence, Technology, and the Law (2018). On the role of AI as such means in the sense of an "automatization of international law," see Maas, *supra* note 1, at 43.

[9]For a three-fold framework for addressing change in international law that also includes "actors" and "values," see The International Rule of Law: Rise or Decline? (Heike Krieger, Georg Nolte & Andreas Zimmermann eds., 2019). On the value element, see also Tracing Value Change in the International Legal Order – Perspectives from Legal and Political Science (Heike Krieger & Andrea Liese eds., forthcoming 2023).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

When examining potential changes, one can in particular ask whether certain actors are empowered or disempowered by digitalization. This can include differences among groups of actors such as states, public actors beyond the state such as international and regional organizations, and private actors including corporate entities and individuals. On this basis, one can determine how the digitalization-related impact on international law relates to other ongoing developments, for example, regarding the role of private actors in the international realm. And actor-related shifts can take place within groups, for example, when the power-dynamics among states change. Digitalization might cause changing power relationships or act as a catalyst for such shifts. Finally, actor-related changes occur—in a more drastic manner—when novel actors enter the scene, be it as subjects of international law or even as norm-creating entities. For the traditional actors in international law, this can mean being replaced, at least in part, in their various legal roles.

The second reference point for assessing the impact of digitalization on international law are the legal norms that constitute international law. Aspects to be analyzed relate to whether existing and novel regulation engages with digitalization and the effect that such regulation has on the overall body of international law. At the outset, it is asked whether the existing norms already capture digital issues or whether it is necessary for international law to adapt. If so, the forms of adaptation, as well as the results, are examined as to their structural impact on international law. This includes issues such as informalization, bilateralization, and fragmentation—aspects that take up existing scholarly debates about the development of international law. Do actors use binding or non-binding forms of norm-setting and are there divergent and/or conflicting norms addressing digital issues from the perspective of different international law regimes? Does digitalization contribute to a trend to use bilateral rather than multilateral forms of treaty making? And do we even witness the development of parallel regimes for the digital and non-digital context? A further impact to be assessed are potential ambiguities and legal gaps that, because of their extent or persistence, might undermine the guiding function of international law. In addition, analyzing the impact on norms also means analyzing their interrelations. A structural impact can be observed when there are novel interrelations among norms of different international law regimes or of different private/public, national/international origin, creating different forms of hybridization of law. Conceptually, one can ask whether, and if so how, international law is affected when it is integrated in such hybrid regulatory spaces.

The underlying values of international law constitute the third reference point for the impact of digitalization. Digitalization can challenge certain values while reinforcing or establishing others. For example, several issues should be considered: Do the relevant actors change their normative preferences? What are the contexts in which actors change their normative preferences? Which actors focus on which values? Further, the analysis includes questions relating to the values reflected in digitalization-related regulation. Which values are reflected in, or challenged by, this regulation? What is more, engaging with the underlying values of international law also means reassessing the purpose that international law is expected to fulfill in various contexts. Digitalization might alter this purpose and thus alter the direction in which norms develop. Values are thus addressed both as to their role in shaping legal norms and as to their role in legal discourse more broadly. It should be noted that the notion of value is understood here as aspects that relevant actors consider normatively as important and that provide guidelines for legal regulation. While other understandings of these notions exist, including conceptions that are more closely linked to ethical or moral considerations, the notion of value adopted here is broader. Further, the values relevant for international law are not necessarily reflected in each norm of this body of law but are, or can be, underlying in various international law fields in a cross-cutting manner.

When using this threefold analytical framework, one can not only trace observable changes but also situate causal claims as to the extent to which the respective changes are generated by digitalization. Here, it is crucial to consider that international law is exposed to various social, political,

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

and geopolitical transformations which might also affect the actors, norms and/or values in a structural manner. It thus is necessary to consider potential interactions between these developments and those observed in the digital context. Digitalization might contribute to structural developments that are also induced by other factors. In this case, digitalization fosters rather than triggers certain shifts. When considering whether digitalization might be only one factor among others, it becomes possible to critically assess the extent of (multiple) causalities. But it also makes it possible to connect developments in the digital and non-digital context, highlighting overarching tendencies. In addition, comparing the impact of digitalization on the actors, norms, and values of international law to ongoing digitalization-related challenges and changes to law on the domestic level and elsewhere shows to what extent changes are inherent to the digital context, and thus a general phenomenon in law; and in contrast, where the particularities of international law play out.

Finally, it bears mentioning that the reference points suggested here are not the only possible lens that one can take to analyzing whether a legal space such as international law is changing in a structural manner. But the analytical framework suggested here provides various benefits. To start with, the three reference points reflected in the framework speak to various accounts of international law, including a range of actor-centered ones such as realist or interactional accounts of international law, norm-centered positivist approaches, or value-centered idealist approaches. It can relate not only to debates in legal scholarship but also to political science research on change regarding norms, discourses, and power-relationships.[10] The present analytical framework is thus inclusive and compatible with other assessments of similar matters. Moreover, by including actors, norms, and values, the framework provides a bird's eye's perspective, making it possible to compare the developments in different fields of international law, connecting them, and integrating them into one overarching picture of the digitalization-related developments of the international legal space. At the same time, the framework is not limited to the digital context. It can be used to assess structural changes in other contexts as well. This also provides an additional digital/non-digital comparability, as well as a comparability of the impact of digitalization on international law, on domestic law, or on other legal spaces. Finally, the framework is well-suited to observe structural developments through a lens that it is not as normatively connotated as other analytical yardsticks that have been used to assess certain aspects of the interrelation between digitalization and international law—such as a possible "disruption" of international law by digital technologies.[11] For these reasons, the framework can be fruitfully used to highlight the various dimensions in which digitalization influences international law.

II. The Dimensions of Digitalization's Impact on International Law

Various developments emerge from the assessments of the impact of digitalization on international law that have been undertaken for this special issue. Although not all developments are visible (yet) in each field of international law studied here, several patterns become apparent that are cross-cutting in nature and can be traced in more than one field of international law. In this section, such patterns are outlined. Using the analytical framework suggested above, these developments are grouped according to whether (1) they concern the actors involved in international legal practice, (2) the norms that constitute the content of international law, and (3) the values that underlie international law.

[10]Especially as to norm change, *see, e.g.*, Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 Int'l Org. 887–917 (1998); Antje Wiener, Contestation and Constitution of Norms in Global International Relations (2018); Lisbeth Zimmerann, *Norms Under Challenge: Unpacking the Dynamics of Norm Robustness*, 4 J. Glob. Sec. Stud. 2–17 (2019); Krieger & Liese, *supra* note 9.

[11]For such an approach, see e.g., Maas, *supra* note 1.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

1. Impact on Actors

Regarding the impact that digitalization has on the actors involved, three main patterns emerge. We observe the empowerment of non-state actors, shifting power-dynamics among state actors, and the (possible) emergence of novel actors. These three aspects are addressed in turn.

1.1 Empowerment of Private and Public Actors Beyond the State

The first actor-related development concerns actors other than states. This involves both private actors and public actors such as international and regional organizations. For these groups of actors, digitalization has influenced and continues to influence their role in international legal practice.

To start with, *private actors* are empowered in the context of digitalization. In this regard, digitalization seems to foster, or at the least contribute to, an ongoing development that is taking place in international law more generally.[12]

In the context of digitalization, a first set of empowered private actors are *corporate entities*. First, these entities assume novel roles as to the creation of legal norms and institutions. This is particularly apparent in the human rights context. Tech companies that shape the interactions, platforms and tools used in the digital sphere create (part of) the rules that govern these interactions from a human rights perspective. This includes, for example, the community standards or guidelines used by platforms such as Facebook and Twitter. These standards are a set of private norms that constitute the core—although not the exclusive content—of what has come to be termed Platform Law.[13] What is more, with the creation of the Meta Oversight Board, private corporate entities also have started to construct institutions that fulfill traditionally public functions such as adjudication. And, as Gulati observes in his contribution to this special issue, these privately created institutions in turn influence the content of platform law and potentially human rights law more generally.[14] In this regard, tech companies have become "key players"[15] in a field that was initially left unregulated by states, and which they have only gradually tried to penetrate. This has created a de facto regulatory competition that empowers corporate actors while "replacing" states as regulatory agents to some extent.[16] As a further result, "digital human rights law" is, as outlined by Shany, considerably dependent on private actors. As he observes, "the enjoyment of digital rights is heavily dependent on the conduct of private companies" such as digital platforms and service providers.[17] Moreover, beyond the human rights context, private actors play an increasing role in international institutional settings as well as the application of law. Villarreal has noted this development in the context of international health law, commenting that the ongoing "private turn" in this field of law as to financing of institutions and normative standard setting has been corroborated for law application where novel digital health tools are involved, including when disease surveillance is delegated to private actors.[18]

Normatively, authors evaluate this development in divergent manners. For Tsagourias, it bears the risk that "states and individuals may transfer their allegiance from international law and institutions responsible for its creation, interpretation, and application to private companies and their

[12]For an overview, see, e.g., Non-State Actors and Int'l Obligations (James Summers & Alex Gough eds., 2018).

[13]On platform law, see Molly K. Land, *The Problem of Platform Law: Pluralistic Legal Ordering on Social Media*, *in* Oxford Handbook Global Legal Pluralism 975–94 (Paul Schiff Berman ed., 2020); Orly Lobel, *The Law of the Platform*, 101 Minn. L. Rev. 87 (2016).

[14]Rishi Gulati, *Meta's Oversight Board and Transnational Hybrid Adjudication—What Consequences for International Law?*, in this issue.

[15]*Id.* at 491.

[16]Nicholas Tsagourias, *Digitalisation and its Systemic Impact on the Use of Force Regime: Legal Uncertainty and the Replacement of International Law,* in this issue.

[17]Yuval Shany, *Digital Rights and the Outer Limits of International Human Rights Law*, in this issue.

[18]Pedro A. Villareal, *International Law and Digital Disease Surveillance in Pandemics: On the Margins of Regulation,* in this issue. *See also* Owain David Williams & Simon Rushton, *Private Actors in Global Health Governance*, *in* Partnerships And Foundations in Global Health Governance 1–25 (Owain David Williams & Simon Rushton eds., 2011).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

regulatory frameworks."[19] In contrast, for Gulati, the empowerment of private actors comes with chances for international law and institutions, for example, as to innovative ways of guaranteeing access to justice.[20] These innovative institutional forms and regulatory approaches adopted by the actors that dominate the digital sphere today also make it likely, according to Gulati, that other tech companies adopt a similar strategy.

An additional development empowers corporate actors without replacing states in their regulatory function: Digitalization can trigger a broadened international legal protection of corporate entities. For international investment law, Polanco points out that corporate entities benefit from the fact that new fields of their activities, especially in relation to the use of data, are protected.[21] And in enforcement law, as highlighted by Ryngaert, corporate entities can obtain a practical role in state activities such as the exercise of extraterritorial enforcement jurisdiction.[22] In such situations, tech companies become necessary intermediaries for states to exercise their authority in the transnational context.

In addition to corporate entities, a broad range of *other private actors* can benefit from certain digitalization-driven shifts.[23] In international investment law, it is not only companies whose international law protection is broadened in the digital context. Even for individuals it seems at least conceivable, according to Polanco, that investment law norms expand to them as well in novel ways.[24] This includes in particular the users of platforms and other digital services that involve giving access to the users' data. If the user as investor of data were to be legally recognized, the personal reach of investment law among individuals would expand in a yet unseen manner. Moreover, there are also other forms of empowerment. For example, digitalization has provided tools to empower private actors in the international legal discourse. These actors have more opportunities to participate in this discourse because international legal documents, as well as related policy and academic texts, are available in a digital and more accessible manner.

The second set of empowered actors is public rather than private in nature: *International and regional organizations*. As to the former, the United Nations (UN) has been very active in shaping issues regarding the applicability of international law norms in cyberspace. This includes, *inter alia*, the establishment of Groups of Governmental Experts issuing reports regarding cooperative needs and applicable norms in cyberspace as well as the UN Open-Ended Working Group (OEWG) issuing a report in 2021 on the applicability of international law, especially concerning Information and Communications Technologies (ICTs).[25] Although such activities are of course

[19]Tsagourias, *supra* note 16.

[20]Gulati, *supra* note 14.

[21]Rodrigo Polanco, *The Impact of Digitalisation on International Investment Law Are Investment Treaties Analogue or Digital?*, in this issue.

[22]Cedric Ryngaert, *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, in this issue.

[23]On the international norm-setting for artificial intelligence, Thomas Burri argues that traditional international law fora are bypassed by an "amorphous and leaderless legislature" involving "interested individuals, professional associations, social and natural scientists, companies, and civil society organisations." Burri, *supra* note 1, at 106. On the range of actors participating in "Internet governance", see Pauline C. Reich, Pravin Anand, Vaishali Mittal, Ayushi Kiran, Anna Maria Osula & Stuart Weinstein, *Internet Governance: International Law and Global Order in Cyberspace*, *in* SAGE Handbook Globalization 592–620 (Manfred B. Steger, Paul Battersby & Joseph M Siracusa eds., 2014).

[24]Polanco, *supra* note 21.

[25]U.N. General Assembly, *Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/65/201 (July 30, 2010); U.N. General Assembly, *Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98 (June 24, 2013); U.N. General Assembly, *Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security,* U.N. Doc. A/70/174 (July 22, 2015); U.N. General Assembly, *Report of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/76/135 (July 14, 2021); U.N. General Assembly, Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021). On the potential role of the UN Security Council, see Eneken Tikk & Niels Nagelhus Schia, *The Role of the UN Security Council in Cybersecurity—*

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

part of the general UN mandate, the potential empowerment lies in the fact that in the digital context, this organization assumes a strong role in legal discourse and regarding norm shaping attempts. In comparison, the role of (individual) states in this regard is (so far) less pronounced, especially considering that states do not agree on whether novel legal regulation should be envisaged or not.[26]

Regarding regional organizations that assume a growing role in various regions of the world,[27] Poli and Sommario discuss this empowerment for the EU.[28] First, in order for existing international norms to be applied to the digital context, such as in the case of the sanctions regimes in reaction to internationally wrongful acts, factual assessments need to be made. This includes, in particular, detecting cyberattacks and determining their origin.[29] As this technical determination requires technical capability and expertise not possessed by all states,[30] regional organizations such as the EU can provide the framework and the resources necessary. The de facto attribution of cyberattacks then would lie in the hands of these actors. Consequently, these actors would be empowered to *operationalize* the international law regime of state responsibility (without becoming the formal holder of such sanction rights). They would thus have an increased role in the application of existing international law.

Second, such actors are also likely to assume a stronger role for legal standard setting in the digital context. This includes harmonized standards not only for transnational commercial activity in cyberspace but also issues regarding digital human rights and, again in the context of state responsibility, novel legal standards for attribution of actions—for example by fully or partially automatized tools. As has been described as the "Brussels effect", such standards have the potential of shaping regulatory activities in other regions of the world as well.[31] For the context of state responsibility, Poli and Sommario thus predict that attribution standards developed by the EU "could provide a model for technical attribution to be adopted or adapted by the international community."[32] The already quite pronounced norm-shaping capacity of the EU is thus likely to be even more enhanced in the ongoing regulation of the cyberspace. This is confirmed by the EU's cybersecurity strategy according to which it sees itself as well-placed to "advance, coordinate and consolidate Member States' positions in international fora."[33]

1.2 Shifting Power Dynamics Among States

A second actor-related development involves shifting power-dynamics among states related to the use of digital tools. On the one hand, digital tools can empower states that use these tools—or enable or condemn the use by private actors in their interest—for international purposes. This has become particularly salient when public opinion and/or elections are being manipulated

International Peace and Security in the Digital Age, Routledge Handbook of Int'l Cybersecurity (Eneken Tikk & Mika Kerttunen eds., 2020).

[26]For the context of the principle of non-intervention, see, e.g., Lukas Willmer, *Does Digitalization Reshape the Principle of Non-Intervention?*, in this issue.

[27]On the role of regional organizations such as ASEAN or the Asia-Pacific Economic Cooperation and the ensuing "Asia-Pacific regionalism" regarding cyberspace, see Hitoshi Nasu & Helen Trezise, *Cyber Security in the Asia-Pacific*, *in* Research Handbook on International Law and Cyberspace 564–581 (Nicholas Tsagourias & Russell Buchan eds., 2d ed., 2021).

[28]Sara Poli & Emanuele Sommario, *The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions*, in this issue.

[29]On the challenges of identifying the origin of cyberattacks, see James Gow, *The Ambiguities of Cyber Security—Offence and the Human Factor*, Routledge Handbook War, Law and Technology 118, 120 (James Gow, Ernst Dijkhoorn, Rachel Kerr & Guglielmo Verdirame eds., 2019).

[30]*See infra* Part B.II.1.1.2.

[31]On the Brussels effect, see Anu Bradford, The Brussels Effect: How the European Union Rules the World (2020).

[32]Poli & Sommario, *supra* note 28.

[33]*Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*, at 11, COM (2020) 18 final (Dec. 16, 2020).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

by automatized tools such as "bots" and the use of Big Data. Such tools are readily available for a broad range of states, providing interference possibilities even for otherwise less powerful states. As Willmer points out, states are aware of this novel vulnerability,[34] quoting a statement by the German Ministry of Foreign Affairs that in "cyberspace, only limited resources are often needed to cause significant harm."[35] According to Willmer, digitalization "at least for now, changes the assumption that a powerful actor has relatively little to fear from weaker adversaries."[36] For international law, this influences the way in which legal arguments are discursively used. For example, the group of states that invoke legal principles such as the principle of non-intervention has changed—it is used more often by conventionally "stronger" rather than "weaker" states.[37] This corroborates perceptions that international law is used as a tool in power relationships that are either balanced or, if they are unequal, by the weaker party. As the power-dynamics are changing in the digital context, states reassess which legal arguments are useful for them in the relationship with different actors.

On the other hand, we witness a disempowerment of certain states when being targeted by such strategically used digital tools. As Poli and Sommario outline even regarding EU member states, only some states have the technical capabilities to determine where cyber-attacks originate.[38] This creates novel power-inequalities among states that are the result of varied technical resources. These factual inequalities translate into legal inequalities when not being able to determine the technical origin, prevent states from legally attributing cyber-attacks to other states, and trigger the sanction regime that would apply based on such attribution. In such situations, states are disempowered as to the application of international law.

Furthermore, states can be disempowered with regard to their regulatory capacities. Regulating certain aspects of the cyberspace requires significant resources and expertise that many smaller states might not necessarily have.[39] This is a phenomenon also addressed as "digital divide" in the development and human rights context.[40] The complexity of the data and cyber-related regulation adopted and envisaged by the EU including the Digital Services Act and Digital Markets Act, the Data Act, the Artificial Intelligence Act, the GDPR and the Cybersecurity Act highlights this aspect.[41] For many states, having a coherent domestic regulation and potentially participating in regional or international regulatory efforts of the digital sphere will be difficult due to lacking resources. Similarly, digital tools as objects of potential international regulation are, due to the digital divide, not available (yet) to the same extent in all states, thus making it less likely that certain states participate in regulation on the matter that might eventually concern them as well. As Villareal points out, this is the case in the global health context, which is characterized by a digital divide regarding digital contract tracing tools.[42] As a consequence, states disadvantaged by this divide have a limited role as potential "norm-shapers" in international law due to technical factors and thus even before political power-dynamics come into play.

In sum, there is thus a tendency of empowerment on the side of the users of digital tools for cyberattacks while the disempowerment happens on the side of the targeted states. Such changing

[34]Willmer, *supra* note 26.

[35]Position Paper: On the Application of International Law in Cyberspace (2021) (Ger.).

[36]Willmer, *supra* note 26.

[37]*Id.* See also *infra* B.II.3.

[38]Poli & Sommario, *supra* note 28.

[39]Also pointing to the issue that not all states have the "technological know-how to understand what regulation is needed, or even to appreciate that it is needed", Maas, *supra* note 1, at 53. On the impact of "unevenly shared technology" on international law, see Picker, *supra* note 1, at 191.

[40]David P. Fidler, *Cyberspace and Human Rights*, *in* Research Handbook on International Law and Cyberspace 94 (Nicholas Tsagourias & Russell Buchan eds., 2015).

[41]Regarding some of the coordination issues among these acts, Federica Casarosa, *Cybersecurity Certification of Artificial Intelligence: A Missed Opportunity to Coordinate Between the Artificial Intelligence Act and the Cybersecurity Act*, 3 Int'l Cybersecurity L. Rev. 115 (2022).

[42]Villareal, *supra* note 18.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

power-dynamics appear as a certain equalization, with power differences being less stark. However, as Willmer notes, it remains to be seen whether further technical advancements will cause for power-dynamics to bounce back to their original divergences.[43]

1.3 Possible Emergence of Novel Actors

In addition to existing state and non-state actors, digitalization and especially its automatization dimension has opened the debate for novel actors in international law. This concerns, in particular, international criminal law and the use of force regime. Here, constructing legal personality for AI seems increasingly within the realm of possibilities. As Swart outlines for international criminal law, attributing legal personality to AI might appear one of the options, or even a necessity, to close accountability gaps.[44] If such a legal personality for AI was to be accepted, this would have implications for various fields of international law. It would raise the question as to whether an AI can be a right holder akin to private actors in contexts such as human rights and investment law and whether they can have international obligations akin to states in some or all contexts in which states do. Structurally, acknowledging AI as a legal person would amount to international law broadening its reach in terms of subjects.

In addition to being (potential) subjects of international law, AI can be attributed a norm-creating function. As Tsagourias outlines for the use of force regime, it is indeed conceivable that the artificial actors can play a role in the creation of international customary law.[45] AI activities can be potentially considered as part of assessing practice and opinio juris.[46] This again would mean a certain disempowerment of traditional actors, especially, states. Yet this disempowerment would be a self-inflicted one given that human actors within states decide, for example in the context of the use of force, to use AI for their purposes. The disempowerment would thus come with the technical advantages that states enjoy when using automatization.

In general, the international law debate mirrors aspects of AI-related discussions on the domestic level. This includes questions such as legal personality for AI, issues of liability and attribution in tort and criminal law, as well as the adjustment of procedural rights when administrative or even judicial decision-making is partially or fully automatized.[47] As the automatization on the domestic level is in various ways (especially regarding automatized decision-making) more advanced than the international level, it is likely that domestic law will shape these questions first. International law is then expected to follow the predominant domestic approach, rather than shaping these questions in an original manner.

In addition to the discussion about the legal personality of AI, a further novel legal actor might be emerging. For the human rights context, Shany points to the construction of a "digital personality" or "online personality" which would be recognized as a legal entity that is separate from the physical person related to it.[48] Such an online personae as right holder or potentially even duty bearer regarding human rights would further extend the range of actors in international law.

In sum, the impact of digitalization on the actors in international law fosters existing tendencies and creates novel trends. So far, this is only the beginning of how digitalization could change the

[43]Willmer, *supra* note 26.

[44]Mia Swart, *Constructing "Electronic Liability" for International Crimes: Transcending the Individual in International Criminal Law*, in this issue.

[45]Tsagourias, *supra* note 16. Skeptical as to whether AI can assume a non-creating function in international law, see Maas *supra* note 1, at 47; Burri, *supra* note 1, at 92.

[46]Automatized decisions that can potentially contribute to state practice also occur beyond the use of force context, e.g., concerning migration decisions.

[47]*See e.g.*, Shawn Bayern, Thomas Burri, Thomas D. Grant, Daniel M. Hausermann & Florian Möslein, *Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators*, 9 Hastings Sci. & Tech. L. J. 135 (2017); on issues of liability and attribution internationally and domestically, Stefan A. Kaiser, *Legal Challenges of Automated and Autonomous Systems*, 60 Ger. Y.B. Int'l Law 173 (2017).

[48]Shany, *supra* note 17.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

international legal actors in the future. It is however certain that the ongoing and emerging shifts already touch upon the very structures of international law.

2. Impact on Norms

The second reference point for assessing structural changes in international law are the legal norms involved. Digitalization contributes to a range of ongoing developments in international law and creates certain novel layers to these developments. This includes: (1) a flexibilization, informalization, and use of novel regulatory fora; (2) new dimensions of the fragmentation of international law; (3) ambiguities as to the content and application of norms as well as legal gaps; and (4) legal hybridity.

2.1 Flexibilization, Informatisation and Different Regulatory Fora

In its reaction to digitalization, international law shows its limited adaptability that characterizes it in other contexts as well.[49] Formal amendments to existing treaty law, or the adoption of novel multilateral instruments is thus judged as unlikely by most contributors to this special issue in their respective fields. Tsagourias summarizes a range of factors that prevent states from regulating digitalization by multilateral treaties:

> [D]igital technologies are "dual-use" without being able to demarcate in advance which aspect of the technology is peaceful and which is not or how it will be used. This affects the scope and content of regulation. Another issue that advocates against treaty based law-making is the fact that digital technology is a buddle of other technologies which are at different levels of development and therefore regulating one technology or its use will be ineffective without regulating all other technologies. Furthermore, questions about the role of the private sector in treaty based law-making will definitely be raised to the extent that digital technologies are developed, produced and distributed by the private sector. Even if states enter into treaty negotiations, they may be delayed or prolonged because of states' divergent interests, resources and capabilities, and thus the concluded treaty may quickly become obsolete in view also of the rapid development and proliferation of digital technology. [50]

As a consequence, international law adapts in different ways. This includes a flexibilization of existing norms, and informalization of norm-creation, and the use of different regulatory fora.

First, we can observe for various fields of international law that existing norms intended for non-digital contexts are expanded to respond to regulatory needs generated by digitalization. In enforcement law, *flexibilization* of existing norms takes place by broadening the scope of application of norms with open or discretionary content to other than the original sub-regime.[51] For human rights law, one can observe a "radical reinterpretation of existing human rights in order to allow them to meet the new conditions of the digital age", as exemplified by freedom of expression and the right to privacy.[52] In investment law, the broad scope of application of existing treaty norms such as the definitions of investment and investor makes it comparatively easy to include digital assets.[53] And in the WTO regime, which so far has not been used as much for the regulation of digital trade, some potential for the flexibilization of existing norms exists as well. This includes technologically neutral rules such as the principles of most-favored nation and national treatment

[49]*See, e.g.*, Joost Pauwelyn, Ramses A. Wessel & Jan Wouters, *When Structures Become Shackles: Stagnation and Dynamics in International Law Making*, 25 EUR. J. INT'L L. 733 (2014).

[50]Tsagourias, *supra* note 16, at 501.

[51]Ryngaert, *supra* note 22.

[52]Shany, *supra* note 17. *See also* Dafna Dror-Shpoliansky & Yuval Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights—A Proposed Typology*, 32 EUR. J. INT'L L. 1249 (2021).

[53]Polanco, *supra* note 21.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

that could be applied to digital trade; and the dispute resolution mechanism which provides a framework for a dynamic interpretation of norms so as to match digital trade requirements.[54] In contrast, a possibility of judicial flexibilization of norms does not exist for fields such as the use of force regime which is generally not the object of judicial decision-making.[55]

Second, the trend towards an *informalization* of international law materializes in the digital context as well.[56] Examples include the Tallinn Manual on cyber warfare which is a non-binding, academic document, or the voluntary Code of Conduct for Information Security proposed by the Shanghai Cooperation Organization, and, as Willmer highlights, the reports of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace, which focuses primarily on non-binding norms.[57] The risk of such informalization for the formal body of international law is twofold. If international legal actors perceive the guiding effect of informal norms as sufficient, the added value of binding legal rules as a regulatory tool for future purposes might become less salient to them. And as regards existing binding law, if informal norms are created that overlap with formal ones, the content of the latter might be "informalized" and thus its bindingness put into question.[58] The structural impact of informalization, including when it is fostered by digitalization, is thus both general and specific in nature.

Third, when formal regulation takes place in the digital context, there is a *shift from multilateral to bilateral, and from global to regional regulation*. The former trend is particularly pronounced in international trade law. While the WTO as multilateral forum would be an appropriate regulatory framework for digital trade, it can "deliver neither swift nor comprehensive solutions."[59] As a result, states have turned to Free Trade Agreements as bilateral or at the most plurilateral instruments in order to regulate international trade. For these instruments, Burri observes that "that the move towards more, more detailed and more binding provisions on digital trade has intensified significantly over course of the past few years and there is also a recent trend of adopting dedicated Digital Economy Agreements."[60] This regulatory trend is thus somewhat opposed to the informalization described above. It seems that in fields of international law, in which bilateral and plurilateral agreements make sense, states opt for formal legal regulation of the digital sphere, while in areas where this is not useful, informalization prevails. What is more, regional approaches to regulating digitalization have become more pronounced. This includes divides between authoritarian and democratic states, for example with regard to cyberattacks and the principles of non-intervention.[61] But there is also a divide between western states such as highlighted by the diverging approaches that the EU and the US take on various digitalization-related issues including data and digital trade, data protection regulation, or the applicability of certain human rights to the digital sphere.[62]

Where international law is adapting to digitalization, it thus does so in ways that contributes to ongoing structural developments in international law, such as informalization and regionalization.[63] As digitalization requires ongoing and large-scale legal adaptation, it is likely to fuel these developments substantively.

[54]Mira Burri, *The Impact of Digitization on Global Trade Law*, in this issue.

[55]Pointing to the lack of an authoritative interpreter in the use of force context, Tsagourias, *supra* note 16.

[56]On this trend in general, Informal International Lawmaking (Joost Pauwelyn, Ramses Wessel & Jan Wouters eds., 2012).

[57]Willmer, *supra* note 26.

[58]On this risk, see also Willmer, *supra* note 26.

[59]Burri, *supra* note 54, at 572.

[60]Burri, *supra* note 54, at 563.

[61]*See also* Willmer, *supra* note 26.

[62]*See, e.g.*, Fidler, *supra* note 40, at 100, 103; Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair (Russell A. Miller ed., 2017).

[63]On informalization, see Pauwelyn et al., *supra* note 56. On regionalization, see, e.g., Select Proceedings of the European Society of International Law: Regionalism and International Law (Mariano J. Aznar & Mary E. Footer eds., 2015).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

2.2 New Dimensions of Fragmentation

A further effect that digitalization has on international legal norms concerns the emergence of regulatory regimes that are fragmented in novel ways. This digital fragmentation has two dimensions.

To start with, fragmentation is created by *parallel regulatory attempts*. This occurs when different fields of international law or different regulatory fora address a single phenomenon created by digitalization and regulate it, or aspects of it. An example of this are cyberattacks. In the international law discussion of how to qualify and confront them legally, cyberattacks are being addressed from the perspective of the use of force regime, the principle of non-intervention, and state responsibility more generally. Further, there is a fragmentation of regulatory processes regarding cyberattacks. As Willmer outlines, different fora (such as UN Governmental Group of Experts, Open-Ended Working Group, and Programme of Action) tackle the same issue in a parallel manner.[64] With regard to cyberattacks, these fragmented discussions and regulatory attempts are still ongoing. In contrast, in international trade law, we already see fragmented treaty norms for digital trade matters. Free Trade Agreements have been used as legal instruments to regulate digital trade instead of the multilateral WTO framework. This form of digital trade regulation has fragmented an area of law that, due to its global scale calls for more uniform standards.[65] Furthermore, for other subject matters, there is a fragmentation of regulatory attempts originating from the international, domestic, and transnational sphere. One can observe this in the regulation of digital corporate entities and in the establishment of human rights standards for the digital realm.

This dimension is fueled by, and contributes to, the already existing and much discussed fragmentation of international law along subject matter lines as well as the multiplication of regulatory fora.[66] The latter includes diverse coexisting international fora as well as the coexistence of international, transnational, domestic, private, and public regulatory activities. However, the digitalization-related dimension of fragmentation is not particular to *public* international law, despite its predisposition for fragmentation. In fact, the insufficient coordination among various *private* international law fora for legal harmonization is seemingly very pronounced with regard to digitalization-related regulation as well.[67] Digitalization is thus challenging in its fragmenting potential also for other areas of law other than public international law.

A second dimension of fragmentation occurs where *different regulatory regimes for the digital and the non-digital context* are created.[68] This seems so far to be an emerging trend in various fields of international law. In investment law, this phenomenon is already quite common. In particular, there are different regimes for traditional types of investments in the digital economy and purely digital assets.[69] While for the former, the prevailing approach seems to be to apply the existing rules, the latter is generally not covered by existing regulation. Some instruments thus include particular rules for digital assets. Further, in international human rights law, a new set

[64]Willmer, *supra* note 26.

[65]Burri, *supra* note 54.

[66]As an example of the discussion about fragmentation, see, e.g., Martti Koskenniemi, *Fragmentation of International Law*, U.N. Doc. A/CN.4/L.682 (Apr. 13, 2006); Regime Interaction in International Law—Facing Fragmentation (M.A. Young ed., 2012); Anne Peters, *Fragmentation and Constitutionalization*, *in* Oxford Handbook Theory International Law 1011 (A. Orford and F. Hoffmann eds., 2016); Andreas Fischer-Lescano & Gunther Teubner, *Regime Collisions: The Vain Search for Legal Unity in the Fragmentation of International Law,* 25 Mich. J. Int'l L. 999 (2004).

[67]*See* Rishi Gulati, *Access to Justice and Multinational Corporations: Promoting Privately Driven Transnational Hybrid Adjudication in Content Moderation Disputes*, *in* Elgar Companion to UNIDROIT (Rishi Gulati, Thomas John & Ben Koehler eds., 2022). Generally, on the insufficient coordination among private international law institutions, Susan Block-Lieb & Terence C. Halliday, Global Lawmakers International Organizations in the Crafting of World Markets 357–388 (2017).

[68]For an early contribution arguing for such parallel digital and non-digital legal regimes, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996).

[69]Polanco, *supra* note 21.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

of digital rights has developed that is specific to the digital sphere, including for example the right not to be subject to automated decisions and the right to be forgotten.[70] In contrast, for other fields of international law, parallel regimes for digital and non-digital contexts are still only part of the discussion rather than the lex lata. For enforcement law, Ryngaert suggests that a "better option may be to accept the principled international lawfulness of 'extraterritorial' enforcement jurisdiction over digital data [. . . which] would leave intact the traditional prohibition of extraterritorial enforcement jurisdiction in the non-cyber domain."[71] This amounts to parallel regimes for enforcement jurisdiction in the digital and the non-digital sphere. Further, concerning sanctions against cyberattacks, Poli and Sommario point to an emerging discussion about whether different regimes for cyber and non-cyber sanctions should be developed.[72] They observe however that the practice of the EU does not seem to move in this direction yet, as the official position still is to (only?) apply existing norms to the cyber context. Finally, an additional and potentially very impactful—so far still potential—development is highlighted by Tsagourias: It seems possible that parallel sets of secondary rules of norm creating in international law might emerge, especially with regard to customary law.[73] Such a development would fully institutionalize a divide in international law between digital and non-digital regulation. Both the process of norm-creation and the content of the norms would diverge, creating autonomous legal spaces for digital and non-digital law. Such fragmentation would reach an entirely new level as compared to the "classical" fragmentation and alter the structures of international law to a yet unseen extent.

2.3 Ambiguities and Legal Gaps

An impact of digitalization on law that comes naturally with any major societal or technical change is a certain amount of ambiguity and even legal gaps when novel phenomena first occur.[74] The more legal regulation addresses these phenomena, the less law will be ambiguous or regulation incomplete. However, such development is not a given for international law in the digital context. To start with, the extent to which digitalization has changed and continues to change societal and technical parameters is considerable, thus necessitating large scale legal adaptation. Further, the ongoing change happens at a speed that requires constant and continued regulatory adaptation. And, due to its structurally limited adaptability, such adaptation is a particular challenge for international law. As a consequence, ambiguities and legal gaps can be expected to be more widespread and long-lasting in formal international law than would be the case in domestic law or with regard to informal norm-setting. The following examples show that ambiguities and legal gaps are indeed very characteristic for international law in the digital context.

The indeterminacy in the scope and content of the rules on the use of force has been analyzed in detail by Tsagourias. He shows that in terms of creating legal ambiguities, digitalization has, as regards the use of force regime, fallen on fertile ground. There is only a small body of rules to begin with, and those norms use "vague and open-ended language."[75] According to Tsagourias, digitalization thus exacerbates the resulting uncertainties. In particular, the definition of what constitutes "digital force", and which kinds of physical, non-physical, direct, and indirect effects are included remains ambiguous.[76] In addition, there is a broad range of fact-related uncertainties that make the applicability of the use of force regime uncertain. This includes difficulties to analyze existing data, to prove causation and to establish intent. As this is the basis for applying the rules on

[70]Shany, *supra* note 17; Dror-Shpoliansky & Shany, *supra* note 52.

[71]Ryngaert, *supra* note 22.

[72]Poli & Sommario, *supra* note 28 (citing Peter Z. Stockburger, *Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents*, 9 Int'l Conf. Cyber Conflict 1–14 (2017)).

[73]Tsagourias, *supra* note 16.

[74]*See also* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep up with Technological Change*, J. L., Tech. & Pol'y 239 (2007).

[75]Tsagourias, *supra* note 16, at 497.

[76]Tsagourias, *supra* note 16, at 499.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

attribution, it remains unclear whether and how to apply these rules when these difficulties occur.[77] Both legal ambiguity as well as legal gaps can ensue with regard to individual norms as well as to the applicability of the regime as such. As to cyberattacks, it is particularly challenging to clearly distinguish between the applicability of the use of force regime and the self-defense rules on the one hand and state responsibility and counter-measures on the other hand.

Similarly, cyberattacks create "regulatory vagueness" with regard to the principle of non-intervention.[78] Although states agree that this principle applies in cyberspace, its content in the digital realm remains ambiguous. In particular, it remains unclear what coercion means when digital tools are being used, for example for election interference. Neither have customary legal standards emerged yet nor are states willing to create treaty law to solve these questions.

Such ambiguity as to the distinction between different legal regimes also occurs beyond the context of cyberattacks. Regarding jurisdictional regimes, Ryngaert points to the fact that the lines between the norms for prescriptive jurisdiction and those for enforcement jurisdiction are blurred by digitalization.[79] Norms from the former regime such as genuine connection and reasonableness are transferred to the latter regime. For Ryngaert, this regime ambiguity is "digitalization's main transformative effect on the law of jurisdiction."[80] What is more, the rules borrowed from prescriptive jurisdiction also carry their own element of ambiguity into the enforcement jurisdiction regime. The more flexible "case by case approach" of the prescriptive jurisdiction regime makes, when transposed to enforcement jurisdiction, legal outcomes more unpredictable than was previously the case.[81]

Another example of regime ambiguity is provided by international trade law. The distinction between goods and services is difficult to maintain for digital trade phenomena. As Burri outlines, digitalization has raised "critical questions of whether previously not existing digital offerings should be classified as goods or services (and thus whether the more binding General Agreement on Tariffs and Trade [GATT] or the GATS apply), and if categorized as services, under the scope of which subsector they would fall."[82] Regime boundaries are thus blurred here as well.

What is more, in particular regarding the use of AI, not only ambiguities as to applicable norms but also explicit legal gaps exist. For example, the specific algorithms on which artificial tools and agents are based have not been assessed by international legal standards yet. Relevant judicial fora in this regard would be the regional human rights courts but also, for the specific case of Facebook, the Meta Oversight Board, for which such a competence has been already discussed.[83] Further, "protection gaps" exist in the human rights context also for other aspects such as exemplified by the discussion about a right to access the Internet.[84]

A last aspect that bears mentioning is that ambiguities and legal gaps in international law are often not accidental. Rather, states seem, for strategic reasons, to prefer to keep international legal rules indeterminate as to digital regulatory issues. As Poli and Sommario observe, "[t]here seems to be a general trend among States to refrain from establishing rigid legal frameworks in the area of cyber operations, also in light of the fast technological development. Many States have chosen to adopt a policy of silence and ambiguity about how international law applies in cyberspace."[85]

The strategic interest of states here lies in broadening their room for—legally not explicitly forbidden—behavior. For example, when it comes to classifying a cyberattack as use of force

[77]On issues of attribution in cyberspace, see also Antonopoulos, *supra* note 4, at 62–65.

[78]Willmer, *supra* note 26.

[79]Ryngaert, *supra* note 22.

[80]Ryngaert, *supra* note 22.

[81]*Id.*

[82]Burri, *supra* note 54, at 562.

[83]*See* Edward L. Pickup, *The Oversight Board's Dormant Power to Review Facebook's Algorithms*, Bulletin 39 YALE J. ON REGUL. (2021).

[84]Shany, *supra* note 17, at 466.

[85]Poli & Sommario, *supra* note 28.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

or not, ambiguous rules give leeway to states to choose self-defense or counter-measures as a reaction to such attacks. At the same time, a strategic consideration against creating unambiguous norms can also be the risk of narrowing the reach of existing legal norms. A new regulatory process may render certain existing norms optional that otherwise might not be perceived as such. States could pick and choose which rules to include into a new treaty,[86] and specific norms could open "the gate for an argumentum e contrario for putting in question the applicability and legally binding character of customary international law, general principles of law and treaty obligations with regard to ICTs."[87]

Despite these strategic benefits that states might see in legal ambiguities, there are risks for the respective legal norms—and for the international rule of law in general. Tsagourias warns that ambiguity might lead to norm decay[88] due to a potential "rejection of particular rules on the use of force for example the rule on self-defence or . . . rejection of the whole regime if states or individuals lose faith because, in their opinion, the regime is not normatively and regulatorily cost effective."[89] Further, a lower scale impact that does not go as far as norm decay would be to diminish the guiding function of the norms. When the content of norms or their applicability is ambiguous, these norms do not, or not as much, guide the behavior of states and other international actors. Ambiguities, when they occur at a large scale and persist over a considerable time, thus have the potential to affect international law severely and structurally. With respect to the ambiguities triggered by digitalization, it is likely that they will be, at least in some fields of international law, long-lasting in nature, thus increasing the risk of affecting international law substantively.

2.4 Hybridity

A final impact of digitalization on international norms is the hybridization of legal norms and spaces. Hybridization occurs when legal elements belong to more than one legal space at once.[90]

A first form of hybridization caused by digitalization is *regime overlaps*. This development can be triggered when existing norms are applied more broadly than initially intended. In such situations, formerly distinct legal regimes such as enforcement jurisdiction and prescriptive jurisdiction can start to share norms that are applied to both. Further, regime overlaps can occur as a result of parallel regulatory attempts. As described above for cyberattacks, different regimes can try to regulate a single phenomenon created by digitalization. In this case, each regime concerned expands to a new regulatory object, thus leading to a multilayered normative framework regarding this object. This multilayered normative body becomes hybrid when its elements interact, thus forming an integrated whole. In contrast, without such interaction, the respective subject matter remains fragmented. For the context of digital human rights law, one can observe both these forms of regime overlaps. As noted by Shany, parallel regulatory attempts of digital rights as well as the broadening of existing norms and discourses beyond regime boundaries foster an ongoing process in which boundaries between international human rights law and other branches of international law are blurred or even "disappearing."[91]

A second form of hybridization is the emergence of *hybrid legal spaces*. This occurs for example when sets of international legal norms such as human rights are interwoven with norms created by private entities such as in the context of platform law. The resulting body of law is hybrid in

[86]*See* Willmer, *supra* note 26, with further references.

[87]Comments by Austria on the Pre-Draft Report of the OEWG (2020), https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf.

[88]On norm decay, see Nicole Deitelhoff & Lisbeth Zimmermann, *Norms Under Challenge: Unpacking the Dynamics of Norm Robustness*, 4 J. Glob. Sec. Stud. 2 (2019).

[89]Tsagourias, *supra* note 16, at 502.

[90]Dana Burchardt, *The Concept of Legal Space: A Topological Approach for Addressing Multiple Legalities*, 11 Global Constitutionalism 518 (2022).

[91]Shany, *supra* note 17, at 470.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

nature. The interaction among the elements of this hybrid space occurs in various forms. The norms as such can refer to other subsets of the space, for example when the Meta standards refer to international human rights law as part of the applicable law by the Oversight Board.[92] Further, the actors who engage with, and apply, the relevant norms —especially judicial actors—can create discursive interactions. In the Platform Law context, a potential judicial dialogue between classical judicial bodies on the international level on the one side and "transnational hybrid courts" on the other side would enhance the hybridization and expand it to the transnational human rights regime more broadly.[93]

In sum, the already existing and further expected impact of digitalization on international legal norms is multilayered and structural in nature. Among the effects addressed above, some are common to legal norms of different origins, including domestic legal norms, while others are specific—or at least particularly pronounced—for international law. For example, what has been discussed as ambiguity and legal gaps seems more prominent on the international level, given the structurally lower adaptability of (formal) international law than of other legal norms which can be more easily replaced, adapted, expanded etc. by regulatory and judicial actors. Further, trends such as hybridization are perceived as especially impactful for international law as it seems to affect its status as "autonomous" legal space.

3. Impact on Values

Digitalization has a two-fold impact on the values that underlie international law. On the one hand, it challenges certain values, fostering existing tendencies to diminish their role in shaping international law (a). On the other hand, digitalization reinforces other values and broadens their reach into the digital sphere (b). Both developments coincide, so far without causing major normative tensions.

3.1 Values Challenged

A value that is prominently challenged is *territoriality* as a reference point for international regulation.[94] In many fields of international law, territoriality is reassessed in the digital context.[95] For investment law, this challenge is very pronounced. As Polanco outlines, it concerns a range of aspects such as the fact that a territorial link for digital investment is difficult to establish; that the role of electronic residency in the context of the investor definition requires the territorial element of residency to be reconsidered; and that for digital assets, their "boundless nature [makes] them seemingly incompatible with geographically based law."[96] For international human rights law, Shany argues that "the territorial focus" of this regime "is eroding" and that the emergence of digital human rights is one of the driving factors behind this development.[97] Digitalization has contributed to various human rights courts and bodies recognizing a form of extra-territorial application of these rights. In addition, the business and human rights approach also fosters the regulation by states of extra-territorial impacts of private commercial

[92]International law is also applied by other private actors in the digital sphere such as by the Independent Objector in the ICANN context. On this aspect, see Fidler, *supra* note 40, at 116.

[93]*See* Gulati, *supra* note 14, at 492.

[94]Territoriality is also challenged by digitalization in other areas of law; see David R. Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996). On territory and digitalization, see also Fleur Johns, *International Law and Digitalization*, *in* CAMBRIDGE HISTORY OF INTERNATIONAL LAW: INTERNATIONAL LAW SINCE THE END OF THE COLD WAR 13 (Eyal Benvenisti & Dino Kritsiotis eds., forthcoming).

[95]In addition to the fields of international law mentioned hereafter, territoriality is also challenged with regard to IHL and the notion of armed conflict when applied to cyberattacks, Kai Ambos, and international criminal responsibility in cyberspace, RSCH. HANDBOOK ON INT'L L. AND CYBERSPACE 118 (Nicholas Tsagourias & Russell Buchan eds., 2015).

[96]Polanco, *supra* note 21.

[97]Shany, *supra* note 17.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

actors.[98] Further, with regard to various areas of law, the territorial dimension of (state and institutional) jurisdiction is challenged. To start with, this is the case for novel legal constructions such as the dispute resolution mechanism created by Meta. As Gulati observes, the jurisdictional framework of the Oversight Board "has deterritorialized the rules on personal jurisdiction, being rules which historically have been primarily based on the connecting factor of territoriality."[99] As to states, both their prescriptive and enforcement jurisdiction are being deterritorialized in the digital context. For prescriptive jurisdiction, territoriality is more and more flexibilized.[100] When regulating the cyberspace, states interpret territoriality broadly and have to find novel approaches when considering "how a genuine (territorial) connection with the regulating State [can] precisely be established."[101] Alternatively, states use the notion of extraterritorial jurisdiction, a normative approach that, although it has always existed in prescriptive jurisdiction, is fostered in the digital context.[102] In contrast, as Ryngaert outlines, the value-shift in enforcement jurisdiction is more radical. Enforcement jurisdiction has traditionally been strongly linked to territoriality. In the cyberspace, territoriality is "fading into irrelevance."[103] To start with, there are numerous factual limits that make a territorially anchored enforcement jurisdiction difficult. This includes the following aspects:

> Digital evidence . . . may be scattered all over the globe, be stored, split, copied, mirrored, and distributed 'in the cloud' on servers chosen algorithmically by Internet service providers, for reasons of ease of user access and cybersecurity. Relevant data may be moved from one jurisdiction to another with the click of a mouse ('data volatility'), and may be stored in different jurisdictions at the same time. The technical features of cloud computing render territorial location a contingent phenomenon. . . . [M]oreover, the exact location of data may even be unknown, which renders reliance on territoriality a non-starter to begin with. Insofar as the 'physical' location of digital data (on a server) may be entirely fortuitous, and may in fact not be known by the territorial State, that State cannot reasonably invoke its territorial sovereignty as a shield against another State's jurisdictional claims over such data.[104]

Due to these factual challenges, states have started to unilaterally adopt a non-territorial approach, creating a de facto extra-territorial enforcement jurisdiction. For example, they directly assess data using remote techniques or source data using intermediaries.[105] As a legal reference point, they replace territoriality "by such flexible notions as effects, connections and interests."[106]

This challenge to territoriality as value in international law is not an entirely new phenomenon that would be only observable in the digital context. Rather, tendencies towards a deterritorialization have been described for international law for some time now.[107] However, here again, it is

[98]Shany, *supra* note 17.

[99]Gulati, *supra* note 14.

[100]*See* Uta Kohl, *Jurisdiction in Cyberspace*, *in* Research Handbook on International Law and Cyberspace 30 (Nicholas Tsagourias & Russell Buchan eds., 2015).

[101]Ryngaert, *supra* note 22.

[102]For the discussion about the extraterritorial application of the right to privacy, see also Fidler, *supra* note 40, at 113–114.

[103]Ryngaert, *supra* note 22.

[104]*Id.*

[105]*Id.*

[106]*Id.*

[107]*See, e.g.*, Catherine Brölmann, *Deterritorialization in International Law: Moving Away from the Divide Between National and International Law*, *in* New Perspectives on Divide Between National and International Law 84 (Janne Nijman & André Nollkaemper eds., 2007); Andreas Paulus, *From Territoriality to Functionality? Towards a Legal Methodology of Globalization*, *in* Governance and International Legal Theory 59 (Ige F. Dekker & Wouter G. Werner eds., 2004). *See also* Martin Kuijer & Wouter Werner, *The Paradoxical Place of Territory in International Law*, 47 Neth. Y.B. Int'l L. 3 (2016); Boaventura de Sousa Santos, *Law: A Map of Misreading—Towards a Postmodern Conception of Law*, 14 J. L. & Soc'y 279 (1987).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

fair to say that the extent of factual deterritorialization that comes with data volatility and unknown or random data location goes beyond previous phenomena. Consequently, territoriality as a value for legal regulation of the cyberspace sits on a weak basis.[108]

A second value that is considerably challenged is the idea of a *human-centered international responsibility*. This is relevant for all fields of international law in which agency is a crucial reference point for regulation and in which autonomous or semi-autonomous agents play a role.[109] This is for example the case in international criminal law for which Swart argues that such autonomous agents "necessitate a rethinking of . . . the insistence on human agency in international criminal law."[110] As she points out, this "will also require a rethinking of the purposes of international criminal law and the extent to which the preoccupation with the individual continues to serve these purposes."[111] In fact, this observation is true for each regulatory area in which automatization is relevant. The regulatory purposes will need to be reassessed to determine whether a human-centered approach is essential for law to fulfill its assigned functions or whether these functions make it possible to incorporate non-human entities into the regulatory subjects. This includes, in particular, considering whether AI should be attributed legal personality. But as the discussions regarding the use of force regime show, legal impacts beyond immediate subjecthood exist as well. A central notion affected by a human or non-human reference point is attribution of AI actions to states. This challenges the human-centered international responsibility per se which traditionally traces back attribution at least indirectly to human actors. Immediate attribution of automatized actions would broaden this approach. What is more, if one considers, as Tsagourias does, that autonomous digital agents could contribute to practice and opinio juris in the context of customary law creation, the human agency for norm creation would also be challenged.[112] This would constitute a shift in foundational values not only of international law but of law in general.

International law shares this challenge for human-centered regulation with other fields of law, such as, on the domestic level, tort law, criminal law, administrative law or procedural law more generally. Here, although an immediate role of AI in legislative processes is so far not discussed, the challenge to human-centricity also includes both AI as potential subject of law as well as automatized legal agency such as in the context of automatized administrative decision-making or the use of AI in judicial decision-making.[113]

In addition, digitalization challenges in a more *indirect* manner the human-centricity of specific fields of international law such as human rights law and international criminal law. It fosters ongoing developments with regard to international legal obligations of corporate entities. In particular, the "business and human rights" approach is reinforced by the de facto human rights relevance of digital tech companies[114] as well as by their active regulatory role when creating "Platform Law."[115] Similarly, the use of AI fosters existing debates on corporate responsibility for international crimes.

3.2 Values Reinforced

While the above values are challenged, others are reinforced in, and expanded to, the digital context. A first set of such values are *procedural values*. For private models of adjudication as the Meta

[108]On territoriality in cyberspace, see, e.g., Stephen J. Kobrin, *Territoriality and the Governance of Cyberspace*, 32 J. INT'L BUS. STUD. 687 (2001).

[109]On the challenges of AI for human agency in human rights law, see Helmut Aust, *"The System Only Dreams in Total Darkness": The Future of Human Rights Law in the Light of Algorithmic Authority*, 60 GER. Y.B. INT'L L. 71 (2017).

[110]Swart, *supra* note 44.

[111]*Id.*

[112]Tsagourias, *supra* note 16.

[113]Morison & Harkens, *supra* note 8; Davis, *supra* note 8; Casey & Niblett, *supra* note 8.

[114]Shany, *supra* note 17, at 469.

[115]*See* Fidler, *supra* note 40, at 98.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

Oversight Board created by digital tech companies, procedural values are center stage. This includes access to justice of the users concerned, and thus accountability of these companies, as well as institutional values such as judicial independence. As Gulati outlines, Meta has indeed gone to great length to explore novel ways of guaranteeing judicial independence of a privately created judicial dispute resolution mechanism.[116] The innovative trust structured used to construct the institutional independence of this body is but one element that indicates that the relevant corporate actors in the digital tech sphere support and emphasize this value. Moreover, the fact that such a mechanism has been created in the first place promotes access to justice as a value in the transnational sphere. At the same time, this emphasis on access to justice has the potential to put a spotlight on existing deficiencies as to dispute resolution mechanisms on the international level such as the deficient access to justice against acts of international organizations.[117] Procedural values could thus be boosted more generally in the international and transnational realm. This could counterbalance the structural differences that contribute to procedural values being implemented to different extents in the transnational and international context. These differences include a higher visibility by, and awareness of, the general public of access to justice deficits against digital tech companies as compared to access to justice deficits against international organizations. And due to this visibility as well as to the sheer number of users concerned as compared to the individuals concerned by detrimental international organizations' activities, the power-dynamics make it more likely that access to justice is optimized in the transnational digital context.

Procedural values are also fostered where international trade law engages with digitalization. For the regulation of digital issues, novel for a are used which reflect procedural values differently than it is the case for traditional trade for a. Participatory rights, accountability and transparency are a more prominent part of regulatory forms such as Free Trade Agreements as compared to the state-only formats characteristic for WTO trade regulation. As Burri highlights, "FTAs may offer suitable venues, with more open and flexible procedural frameworks and participatory and co-regulatory elements."[118]

Moreover, wherever AI is targeted by regulatory attempts, procedural values play a crucial role. This includes for example transparency of automatized decision-making for example as to the algorithms used;[119] and due diligence standards for the users or AI.[120] However, this focus on procedural values might come with a downside. It might, as least in part, replace the legal protection of substantive values. As Tsagourias warns for the context of the use of force regime: "The normative and mandatory regulatory modality of international law" such as the substantive use of force rules might be "replaced by an administrative, managerial and technical regulatory modality" if the focus is shifted to procedural values.[121]

Further, digitalization contributes to fostering, or even introducing, certain *substantive values* in international law. To start with, in the debate about non-intervention and its applicability to

[116]Gulati, *supra* note 14.

[117]Rishi Gulati, Access to Justice and International Organisations (2022).

[118]Burri, *supra* note 54, at 573.

[119]On transparency and accountability as values in the context of automatization in the domestic legal orders, Monika Zalnieriute, Lyria Bennett Moses & George Williams, *The Rule of Law and Automation of Government Decision-Making*, 82 Mod. L. Rev. 425 (2019). Critical on the focus on transparency and suggesting an alternative approach, *see* Lorna McGregor, Daragh Murray & Vivian Ng, *International Human Rights as a Framework for Algorithmic Accountability*, 68 Int'l & Compar. L. Q. 309 (2019).

[120]Tsagourias, *supra* note 16. For the human rights context, Aust considers transparency as one of the "escape routes out of the dilemma of how to preserve 'human sovereignty' over the data-driven processes." Aust, *supra* note 109, at 86. Relatedly, on due diligence as the primary reference point for state responsibility in cyberspace, see Antonopoulos, *supra* note 4, at 66.

[121]Tsagourias, *supra* note 16, at 506.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

cyberattacks targeted at influencing domestic elections, democracy as a value was introduced as a potential reference point for this principle.[122] This would go beyond the so far existing normative neutrality as to the political regime which is the object of the principle of non-intervention. Similarly, introducing (as an alternative to the direct reference to democracy) a protection of transparent deliberative processes, as is suggested in the discussion about non-intervention, would create a novel normative layer for this principle.[123]

In the non-intervention context, a strengthened normative focus on state sovereignty has also become apparent. As Willmer shows, this development has various dimensions.[124] First, some states and scholars suggest making sovereignty the direct legal reference point rather than the principle of non-intervention to address cyberattacks.[125] Second, the group of state actors that invokes sovereignty or the principle of non-intervention which is a correlate of sovereignty has broadened.[126] While, for a long time, it was mostly used by non-western and/or authoritarian states, western and/or democratic states have started to refer to it in the context of cyberattacks. As a further indication of this trend, sovereignty has also been stressed in the UN Group of Governmental Experts (GGE) and OEWG reports. Third, and beyond the context of non-intervention, sovereignty as a value is explicitly transposed to the digital sphere when concepts such as "digital sovereignty" or "cyber sovereignty" are developed,[127] and when the control over the free flow of information on the Internet is integrated into this notion as propagated for example by China and Russia.[128] In relation to the Internet, an emphasis on sovereignty has also been described as relevant for the field of human rights.[129]

This reinforcement of sovereignty somewhat contrasts with the above-mentioned challenges that the value of territoriality is facing. As sovereignty and territoriality of the state have been closely connected notions, challenges to the latter such as in the case of extra-territorial enforcement jurisdiction, which is perceived as highly sovereignty sensitive, affect this value as well.[130] Yet as sovereignty is also reinforced, this value is, through these opposing developments, reshaped in substance. The territorial connotation of sovereignty loses influence while other dimensions such as a potential deliberative and community-related dimension come into focus. If this development solidified, this would amount to an impactful structural shift in international law's normative basis.[131]

A further example of shifting substantive values in the digital context is provided by international trade law. Here, non-economic values are more prominently reflected in novel digital trade regulations. As Burri observes:

[122]On such suggestions, see Willmer, *supra* note 26.

[123]Willmer, *supra* note 26.

[124]Willmer, *supra* note 26.

[125]*See* Alaa Assaf & Daniil Moshnikov, Contesting Sovereignty in Cyberspace, 1 Int'l Cybersecurity L. Rev. 115 (2020). On the position of EU member states on this point, Anna-Maria Osula, Agnes Kasper & Aleksi Kajander, *EU Common Position on International Law and Cyberspace*, 16 Masaryk Univ. J. L. & Tech. 89 (2022).

[126]Willmer, *supra* note 26.

[127]On this notion in the European context, see Theodore Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, Multidisciplinary Inst. on A.I., Grenoble Alpes Data Institute, December 2020.

[128]*See e.g.*, Yi Shen, *Cyber Sovereignty and the Governance of Global Cyberspace*, 1 Chinese Pol. Sci. Rev. 81 (2016); Stanislav Budnitsky & Lianrui Jia, *Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance*, 21 Eur. J. Cultural Stud. 594 (2018).

[129]Fidler, *supra* note 40.

[130]On the link between territoriality and sovereignty, Tsagourias, *supra* note 5, at 13. Specifically on territorial sovereignty in the context of cyberattacks, *see* Luke Chircop, *Territorial Sovereignty in Cyberspace After Tallinn Manual 2.0*, 20 Melbourne J. Int'l L. 349 (2019).

[131]More generally on the controversial debate about sovereignty-related trends in international law, see Don Herzog, Sovereignty, RIP (2020); Heike Krieger, *Of Zombies, Witches and Wizards—Tales of Sovereignty*, 33 Eur. J. Int'l L. 275 (2022) (reviewing Herzog's Sovereignty, RIP).

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

> [T]he DEPA deals with the importance of a rich and accessible public domain and digital inclusion, which can cover enhancing cultural and people-to-people links, including between Indigenous Peoples, and improving access for women, rural populations, and low socio-economic groups. This is indicative of shifting of values when attempting to regulate digitization, which clearly goes beyond the economic domain and affects a great number of broader societal issues.[132]

This example shows that digitalization can *provide an opportunity* for reassessing normative choices made in international regulation, even if a value shift is not a necessary result of digitalization or of changing interests triggered by it. The fact that digitalization requires novel regulation can in itself provide an opportunity to emphasize certain values more than in previous regulations of the same subject matter.

In sum, digitalization touches upon a range of values that are foundational for international law. Value shifts have started to occur and have the potential to intensify as digitalization continues to shape societal, economic, and political practice. It bears mentioning that what we observe is not the emergence of a less value-based international law. Rather, legal actors put a stronger focus on some values than on others. For the most part, this means that these actors "merely" modify their normative preferences, as their interests in the digital contexts change. An exception to this is the value of a human-centered international responsibility, for which factual necessity requires a reassessment. The latter aspect also highlights that some of the value-shifts outlined above are particular to the digital context while for others, digitalization fosters pre-existing trends.

C. Conclusion

This article has illustrated trends in the interrelation between digitalization and international law. It has highlighted that structural shifts as to actors, norms and values in international law are currently taking place and that there is a potential for such shifts to continue, expand, and intensify. It has outlined how these impacts of digitalization are linked to ongoing developments in international law, situating whether and to what extent digitalization triggers or merely contributes to otherwise initiated structural shifts. And it has provided a framework that can be used to link the digitalization-related developments observed here to those in fields of international law that have not been covered by the contributions of this special issue. Finally, the above findings also highlight that the developments regarding actors, norms and values are not isolated from each other. Rather, many of them are interrelated in various ways. For example, with changing power dynamics among actors, it is likely that different sets of values come to the forefront.

How to evaluate the impacts of digitalization on international law normatively, remains a question that eludes a general answer. Some of the impacts can be more easily qualified as normatively desirable or undesirable, while for others, the normative assessment is more demanding. For example, ambiguities and legal gaps might be qualified as risks for the rule of law, and, in contrast, strengthening values such as accountability and access to justice can be seen as promoting it. For other developments, the assessment depends very much on the normative stance on specific issues such as the role of states in international law, as the actor-related impact of digitalization contributes to partially replacing the state as central actor in the international realm. Each impact would thus need to be evaluated individually and thoroughly—a task for future research. Yet, independently of how one qualifies these impacts normatively, what appears clearly from the

[132]Burri, *supra* note 54, at 571.

https://doi.org/10.1017/glj.2023.31 Published online by Cambridge University Press

analysis presented in this article, is that the outlined trends will continue to shape the future of international law in a structural manner.

Competing Interests. The author declares none.

Funding Statement. No specific funding has been declared in relation to this article.

Cite this article: Burchardt D (2023). Does Digitalization Change International Law Structurally?. *German Law Journal* **24**, 438–460. https://doi.org/10.1017/glj.2023.31