

ZaöRV

Zeitschrift für ausländisches
öffentliches Recht und Völkerrecht

3|2021

81. Jahrgang
Seiten 585–884

HJIL

Heidelberg Journal
of International Law

Aus dem Inhalt

Elif Askin

Environmental Injustice: The (Unaddressed)
Case of Toxic Waste Disposal in the Global South

Special Issue:

International Law and the Internet

Edited by Angelo Jr Golia, Matthias Kettemann &
Raffaella Kunz

With Contributions by

Annalisa Ciampi, Stefano Dominelli, Nula Frei,
Cäcilia Maria Hermes, Ralph Janik,
Christine Kaufmann, Antonio Segura-Serrano,
Patricia A. Vargas-León, Rolf H. Weber,
Chien-Huei Wu



MAX-PLANCK-INSTITUT
FÜR AUSLÄNDISCHES ÖFFENTLICHES RECHT
UND VÖLKERRECHT

<https://doi.org/10.17104/0044-2348-2021-3-581>

Generiert durch IP '57.133.22.171', am 10.09.2024, 19:33:02.

Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.





Bezugspreise 2022

ZaöRV + Zeitschrift für ausländisches öffentliches Recht und Völkerrecht

Die Bezugspreise (einschließlich MwSt.) betragen ab 1.1.2022:
Normalpreis jährlich € 219,- jeweils zuzüglich Vertriebsgebühren jährlich € 10,50
Abbestellung bis 6 Wochen vor Jahresende. Einzelheft € 59,50

Bestellen Sie bei Ihrem Buchhändler oder bei:

beck-shop.de oder Verlag C.H.BECK · 80791 München · Fax: 089/38189-358 · www.beck.de



Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV)

The Journal may also be cited as:

Heidelberg Journal of International Law (HJIL)

Editors in Chief/Herausgeber: Armin von Bogdandy, Anne Peters
in Gemeinschaft mit Rudolf Bernhardt, Jochen Abr. Frowein, Rüdiger Wolfrum

Managing Editor/Schriftleitung:
Rainer Grote

Book Reviews Editor/Schriftleitung Rezensionen:
Richard Dören

Academic Advisory Board/
Wissenschaftlicher Beirat:

Elif Askin, Guillaume Futhazar,
Matthias Goldmann, Angelo Golia,
Matthias Hartwig, Laura Hering,
Michael Ioannidis, Jannika Jahn,
Martin Andrew Jarrett, Christoph Krenn,
Raffaella Kunz, Christos Kypraios,
Christian Marxsen, Carolyn Moser,
Davide Paris, Christiane Philipp,
Erin Pobjie, Achilles Skordas,
Mark Somos, Thomas Sparks,
Paulina Starski, Saskia Stucki,
Pedro Villarreal

V.i.S.d.P.: Armin von Bogdandy, Anne Peters

Postanschrift: Redaktion MPI für Völkerrecht,
Andrea Hug, D-69120 Heidelberg,
Im Neuenheimer Feld 535

Mit der Einreichung eines Manuskripts bietet der Autor den Herausgebern die Übertragung der Nutzungsrechte, einschließlich des Rechts zur öffentlichen Zugänglichmachung (§ 19a UrhG), das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form an. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Erscheinungsweise: Vier Ausgaben und ein Registerband jährlich

Bezugspreis 2021: Normalpreis jährlich € 219,00 (inkl. MwSt.)
Einzelheft: € 59,50 (inkl. MwSt.)
Jeweils zuzüglich Versandkosten.

Manuskriptsendungen an die Redaktion werden erbeten unter der Adresse:
<https://www.editorialmanager.com/heidelbergil>
Sie müssen den unter <http://www.zaoerv.de> einsehbaren Manuskriptrichtlinien entsprechen und werden nur unter der Voraussetzung angenommen, dass der Autor/die Autorin nicht denselben Gegenstand in einer anderen Publikation behandelt. Sie geben die wissenschaftliche Auffassung des jeweiligen Autors wieder.

With the submission of a manuscript the author offers to transfer to the editors the rights of use, including the right of communication to the public (§ 19a German Copyright Law), the rights to publicly reproduce or access, the rights to include in any databank, the rights to store on electronic data carriers and the rights to distribute and copy as well as the rights to any other utilisation in electronic form. The mandatory statutory secondary rights of the author after 12 months from the date of publication as set out in § 38 section 4 Copyright Act (UrhG) shall not be affected hereby.

Subscription price for the complete volume (4 issues and index): € 219,00

Single issue: € 59,50

Postage and handling fees will be added.

Cancellation of subscriptions: Publisher must be notified no later than 6 weeks prior to the end of the calendar year.

Verlag: C.H. BECK oHG, Wilhelmstr. 9, D-80801 München. Postanschrift: 4003 10, 80703 München, Tel.: 089/38189-0, Fax 089/38189-398, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX. Der Verlag ist oHG. Gesellschafter sind Dr. Hans Dieter Beck und Dr. h.c. Wolfgang Beck, beide Verleger in München.

Bestellungen über jede Buchhandlung und beim Verlag.

Abo-Service: Tel.: 089/38189-750, Fax 089/38189-358, E-Mail: kundenservice@beck.de.

Abbestellungen müssen 6 Wochen vor Jahrgangsende erfolgen.

Adressenänderungen: Bei Adressenänderungen muss neben dem Titel der Zeitschrift die neue und alte Adresse angegeben werden.

ISSN 0044-2348

<https://doi.org/10.17104/0044-2348-2021-3-581>

Generiert durch IP '57.133.22.171', am 10.09.2024, 19:33:02.

Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.



MAX-PLANCK-INSTITUT
FÜR AUSLÄNDISCHES ÖFFENTLICHES RECHT
UND VÖLKERRECHT

ZaöRV 81 (2021)

Inhaltsverzeichnis

Comment

<i>Elif Askin: Environmental Injustice: The (Unaddressed) Case of Toxic Waste Disposal in the Global South</i>	585
--	-----

Abhandlungen *

<i>Angelo Jr Golia / Matthias C. Kettemann / Raffaela Kunz: International Law and the Internet</i>	597
<i>Rolf H. Weber: Integrity in the 'Infinite Space' – New Frontiers for International Law</i>	601
<i>Nula Frei: Equality as a Principle of the Networked World? An Exploratory Search for 'Cyber-Equality' in the Field of Internet Governance</i>	627
<i>Chien-Huei Wu: Sovereignty Fever: The Territorial Turn of Global Cyber Order</i>	651
<i>Annalisa Ciampi: The Role of the Internet in International Law-Making, Implementation and Global Governance</i>	677
<i>Antonio Segura-Serrano: Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development</i>	701
<i>Stefano Dominelli: Internet and eDiplomacy: 'Traditional' Diplomatic Law in the Digital Era</i>	733
<i>Patricia A. Vargas-León: Microsoft Corp. v. United States and the 'Hot Pursuit': A Case Study Against the Application of the Law of the Sea into the Cyberspace</i>	755
<i>Christine Kaufmann: Responsible Business in a Digital World – What's International Law Got to Do With It?</i>	781
<i>Cäcilia Maria Hermes: Cyberspace as an Example of Self-Organisation from a Network Perspective</i>	817
<i>Ralph Janik: Interpretive Community 2.0: How Blogs and Twitter Change International Law Scholarship</i>	841

* Alle als Abhandlungen veröffentlichten Beiträge haben zuvor ein Begutachtungsverfahren (double-blind peer review) durchlaufen. / All articles published under the heading "Abhandlungen" were subject to double-blind peer review.

Buchbesprechungen

<i>Goeble, Thilo</i> : Freiraum oder Herrschaftsgebiet. Menschenrecht auf Zugang und völkerrechtliche Prinzipien als Schranken staatlichen Handelns im Internet (<i>Clara Rauchegger / Janine Prantl</i>)	867
<i>Amoroso, Daniele</i> : Autonomous Weapons Systems and International Law (<i>Elisabeth Hoffberger-Pippan</i>)	873
<i>Delerue, François</i> : Cyber Operations and International Law (<i>Rachel F. Behring</i>)	879

Abhandlungen

International Law and the Internet

Edited by Angelo Jr Golia, Matthias C. Kettemann and Raffaella Kunz

Introduction

by Matthias C. Kettemann, Raffaella Kunz and Angelo Jr Golia

Fifteen years is not a long time in the evolution of international law. Establishing the crystallisation of a rule into custom, for instance, might take decades. Fifteen years is, however, a substantial time when it comes to technological developments, especially information and communication technologies (ICTs). Probably the most important advancement in the field of ICTs is the evolution of the Internet into the key communication facility of our time. At its core, the Internet remains '[a] global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols'.¹ But the Internet is more than such a technical definition might suggest. It has permeated all aspects of human life and human agency. It has substantially affected how states conduct international affairs, how threats are communicated and carried out, how information is gathered and spread, and, how attacks are prepared and made. International law questions abound, but the Internet also affects scholarly communication about international law and the way international legal scholarship is discussed and disseminated.

This is why we have put together this special issue on international law and the Internet. Ten contributions query into the role of international law for the Internet and the impact of the Internet on international law. Read together, they offer fascinating perspectives on international law as a force of order. International law already forms part of the normative infrastructure of the Internet, be it as a legal basis of the right to access to the internet, as a benchmark for assigning custodial sovereignty to a state with an important Internet Exchange Point (such as Germany's DE-CIX), as a yardstick for qualifying a state-led information operation via cyber channels as lawful (but awful) or unlawful, or for discussing the rights and duties of online platforms to delete hate speech. However, it remains an open question how interna-

¹ Oxford English Dictionary, s. v. 'Internet' (2018), <<https://en.oxforddictionaries.com>>.

tional law can successfully perform its role as the *ius necessarium* of the internet, with, next to, or even against the several forms of transnational private and/or hybrid regulation which continue to emerge.

The contributions in this special issue go a long way towards furthering this understanding. Rolf H. Weber, who has been an influential voice in law of internet governance for the past decades, shows how the notion of Internet integrity can be usefully employed. Nula Frei discusses the role of equality in a world where all can be connected, but inequalities persist (and are exacerbated by differences in access to technology). Chien-Huei Wu focuses on the dark side of the 'cyber order' and identifies an authoritarian turn. Annalisa Ciampi shows how the Internet impacts the formation and evidence of custom and Antonio Segura-Serrano analyses the impact of international law on cybersecurity and describes new dynamics of norm development. Stefano Dominelli investigates the changing nature of diplomacy in times of digitalisation, as shows that foreign policy has to be rethought now that a lot of diplomatic action happens online. Applying concepts from space law and the law of the sea to cyberspace is often useful, as Patricia A. Vargas León, shows by reference to the *Microsoft v. US* case. Microsoft, as a big online company, is an important player in the digital ecosystem. With power also comes responsibility. As Christine Kaufmann shows, ensuring responsible business in a digital world is a case to be made on the basis of international law. Căcilia Hermes then takes a step back and analyses cyberspace from the perspective of network theory. Concluding the special issue, Ralph Janik discusses how online platforms and the communication taking place on them have changed international legal discourse.

International Internet law develops quickly. We are therefore lucky to have among our authors one who has published already in 2006 – 15 years ago – an analysis where he described international law not only as a 'tool for solving regulatory conflicts, but [...] a tool for governance' regarding key aspects of internet regulation, especially privacy, intellectual property, the use of force and human rights online, such as the right to internet access.² He called on international law to 'take a normative stance'.³ Since then, Antonio Segura-Serrano and others have developed international internet law much further – as he shows in his contribution on cybersecurity and norm development. More recently, authors have also analysed the reliance of internet-related normative processes on non-traditional norms⁴ or criticised their

² Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law', Max Planck UNYB 10 (2006), 191-272 (192).

³ Segura-Serrano (n. 2), 271.

⁴ Martha Finnemore and Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', AJIL 110 (2016), 425-479 (477) (emphasis added).

prevalence,⁵ or developed a comprehensive ‘normative order’⁶ of the Internet, in which international law plays a key role as a normative anchor.

As the contributions collected here show, international law can act as an important retaining force in light of the ever quicker technological change. The goal is clear. After all, the international community committed itself to achieving a ‘people-centred, inclusive and development-oriented Information Society [...] premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights(.)’ We hope that this special issue will further stimulate this important debate that even after fifteen year is certainly far from being over.

Last but not least, it is worth mentioning that this special issue has been edited during (and despite) the troubled period that started with the outbreak of the COVID-19 pandemic in 2020. It collects a selection of the papers presented at the authors’ workshop held online on 15-16 October 2020. In the following months, reviewing and editing the papers has been particularly challenging and would not have been possible without the generous contribution of several people. Here, we would like to particularly thank the anonymous reviewers, Andrea Hug from the Redaktion of the ZaöRV, and the student assistants that helped us, especially Elisabeth Alexander, Sarah Gebel, Carolin Eschenfelder, Leon Seidl, Marieke Simons.

⁵ Calling on states to develop a treaty-based international law of cybersecurity: Kubo Mačák, ‘From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers’, LJIL 30 (2017), 877-899.

⁶ Matthias C. Kettemann, *The Normative Order of the Internet* (Oxford: Oxford University Press 2020).

Integrity in the ‘Infinite Space’ – New Frontiers for International Law

Rolf H. Weber*

University of Zurich, Zurich, Switzerland

rolf.weber@rwi.uzh.ch

Abstract	601
Keywords	602
I. Introduction	602
II. Internet Integrity and Cybersecurity Challenges	603
1. From Cybersecurity to Cyber Resilience	603
2. Limited Impact of Existing Cybercrime Instruments	605
III. Searching the Holy Grail: Embedding Internet Integrity into International Legal Concepts	607
1. Moving to Global Cosmopolitan Governance	607
2. Coping with Digital Sovereignty	609
IV. Fructification of Available Legal Concepts	610
1. Concept of Global Public Goods	610
2. Concept of Shared Spaces	612
a) Objective of the Concept	612
b) Examples: Comparable International Legal Instruments	613
c) Starting Point for Cooperation	615
3. Concept of State Responsibility and Due Diligence	616
4. Further Potential Concepts	618
V. Relevance of Soft Law for Internet Integrity	619
1. Self-Regulatory Approaches	619
2. Co-Regulatory Approaches	621
VI. Forward-Looking Perspectives	624
1. Implementation of International Legal Concepts Based on Soft Law	624
2. Search of New Paths Leading to Internet Integrity	624

Abstract

Internet integrity encompassing the security, stability, robustness, and resilience of the most widely used global infrastructure has become a key topic of governance debates. The early emphatic cyberspace pronouncements volatilised; in addition, network security influence interests and national Internet policies increasingly jeopardize the global normative order. Since multilateral treaties are hardly suitable to realize an open space, international

* The Author is Professor at the University of Zurich, Faculty of Law.

legal concepts, particularly the concept of global public goods, of shared spaces, and of State responsibility, merit to be applied on a wider scale. Thereby, a bridge should be built between Internet governance principles and public international law.

Keywords

Concept of Shared Spaces – Concept of State Responsibility – Co-Regulation – Global Public Goods – Internet Integrity – Soft Law

I. Introduction

The Internet as the most important global infrastructure is an environment in which international law, with all its perplexities, should be effectively and coherently applied. The now 25 years old ‘Declaration of Independence of Cyberspace’ (John Perry Barlow) does not suffice. Yet the current approach of politicians, scholars and practitioners shows a pertaining reluctance to embrace the challenges posed by global cyber governance in respect of present and future cross-border electronic networks, notwithstanding the fact that Internet regulations deserve a steady place in the international law dogmatic.

In particular, available international legal concepts are not yet sufficiently debated in the policy-makers’ circles. Internet governance principles should be contextualised within public international law. The classification into different categories must be overcome and replaced by bridge-building efforts. The ‘*Infinite Space*’ (as coined by Star Trek almost ten years ago) may not remain without normative guidelines designing an appropriate social order.

This article attempts at contributing to the building of bridges between the discussed Internet governance principles and public international law. The specific research object of the article is the not yet widely analysed issue of *Internet integrity*. At various existing venues, the practically important Internet integrity is debated but the narratives are often dispersed. In addition, the Internet as the most important global network is still not seen as a stable part of international legal scholarship.¹ Nevertheless, the article does not reflect the decades old argument of ‘the law of the horse’² but rather develops ideas

¹ For a first attempt into this direction see Joanna Kulesza and Rolf H. Weber, ‘Protecting the Internet with International Law’, *Computer Law & Security Review* 40 (2021), 105531, 1 ff.

² See Lawrence Lessig, ‘The Law of the Horse: What Cyberlaw Might Teach’, *Harv. L. Rev.* 113 (1999), 501-549, reacting to Frank H. Easterbrook, ‘Cyberspace and the Law of the Horse’, *University of Chicago Legal Forum* 1 (1996), 207-216.

for a comprehensive and future-oriented assessment of the today prevailing challenges.

At the beginning, the research object, namely Internet integrity being exposed to security challenges, is discussed (chapter II.). Thereafter, the article develops the relevant elements which can embed Internet integrity into the existing pillars of public international law (chapter III.), to be followed by the main part of the article analysing a possible fructification of acknowledged legal concepts in this context (chapter IV.). Subsequently, the relevance of soft law for Internet integrity is laid out (chapter V.). The article closes with the presentation of forward-looking perspectives outlining new paths that are suitable to realise Internet integrity (chapter VI.).

II. Internet Integrity and Cybersecurity Challenges

The integrity of the Internet depends on its proper functioning without technical interference and (unjustified) governmental intervention. The technical setting must ensure that data is real, accurate, and safeguarded from unauthorised modification. The preservation of these qualities is a matter of proper governance of the Internet environment.

The term governance can be traced back to the Greek word *kybernetes*, the steersman, leading though the Latin word *gubernator* to the English notion *governor* addressing aspects of steering and governing behaviour.³ Consequently, cyber governance looks at the measures taken by the concerned actors with the objective to protect information and data as well as the underlying assets and infrastructures.

1. From Cybersecurity to Cyber Resilience

During the last few years, different terms have been coined with the objective of safeguarding the integrity of the Internet. At the beginning, (i) *cybersecurity* was the most commonly used word, followed by other notions such as (ii) *cyber stability* and (iii) *cyber resilience*; these terms can be described in short as follows:

- (i) *Cybersecurity* refers to processes and measures protecting networks and data form cybercrimes. So far, no standard or universally accepted definition of the term cybersecurity exists. As the Internet Society remarked, 'as a catchword,

³ Rolf H. Weber, *Shaping Internet Governance: Regulatory Challenges* (Zurich: Schulthess 2009), 2.

cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges and ‘solutions’ ranging from the technical to the legislative’.⁴ The International Telecommunication Union defines cybersecurity as ‘the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions trainings, best practices, assurance and technologies that can be used to protect the cyber environment and the organisations’ and users’ assets’.⁵ Apart from the unclear definition, cybersecurity encompasses two different relevant phenomena, namely the traditional cybercrime appearances and the increasingly important ‘cyberwar’ phenomena.

(ii) *Cyber stability* means that everyone can be reasonably confident in the ability to use the Internet and – generally – cyber space in a safe and secure manner; this relatively new term having recently gained importance addresses the availability and integrity of services and information to be provided in a secure way.⁶

(iii) *Cyber resilience* is the ability to provide and maintain an acceptable level of service rendering as well as to deliver the offered or envisaged outcome, despite adverse cyber events.⁷ This term was mainly developed in the context of private organisations’ risk management frameworks.

Notwithstanding the above described *cyber notions*, general security objectives including (i) confidentiality, (ii) integrity, and (iii) availability, also known as the CIA triad of the information security industry, always play an important role. Confidentiality means that information is not improperly disclosed to unauthorised individuals, processes, or devices; integrity refers to information being protected against unauthorised modification or destruction; availability pertains to a timely and reliable access to data and information for authorised users.⁸ The International Organisation for Standardisation (ISO) defines information security as the preservation of confidentiality and availability in its ISO/IEC (International Electrotechnical Commission) 27000:2018 standards on Information Security Management Systems.⁹

⁴ Karen O’Donoghue, ‘Some Perspectives on Cybersecurity’, Internet Society 2012, <<https://www.internetsociety.org/>>.

⁵ ITU Definition: <<https://www.itu.int/>>; for a more general overview see Rolf H. Weber and Evelyne Studer, ‘Cybersecurity in the Internet of Things: Legal Aspects’, Computer Law & Security Review 32 (2016), 715-728 (716-717).

⁶ Global Commission on the Stability of Cyberspace (GCSC), Advancing Cyberstability, Final Report (IGF Berlin: November 2019), 13.

⁷ Fredrik Björck, Martin Henkel, Janis Stirna and Jelena Zdravkovic., ‘Cyber Resilience – Fundamentals for a Definition’, <https://doi.org/10.1007/978-3-319-16486-1_31>.

⁸ Rolf H. Weber, ‘Cybersecurity in International Law’ in: Asian Academy of International Law (ed.), 2019 *Colloquium on International Law* (Hong Kong: AAIL 2020), 279-308 (281).

⁹ See <<https://www.iso.org/>>.

This article does not analyse the details of existing legal instruments (or their preparatory documents) combatting cybercrime, but only mentions their existence and some key messages at the beginning. Moreover, the article has the objective to assess in more depth to what extent the established and widely accepted international legal concepts (in particular the concept of global public goods, of shared spaces, and of State responsibility) can contribute to an acceptable cyber governance (chapter IV.). These legal concepts do not coincide with the international legal principles as contained in the Statute of the International Court of Justice (mainly article 38) and often addressed in the traditional discipline of public international law. The herein-after discussed legal concepts could further be supported by the already existing self- and co-regulatory initiatives (chapter V.).

2. Limited Impact of Existing Cybercrime Instruments

For decades, international and regional organisations have tried to develop legal instruments that could harmonise the regulatory standards mainly in the field of cybersecurity prevention.¹⁰ Some efforts have been (partly) successful, particularly if implemented by sector-specific international organisations (e. g. International Telecommunication Union, World Trade Organization).¹¹ However, in the most intensively discussed area, namely cybercrime, the outcomes are rather limited; in addition, cybercrime only covers a part of Internet integrity, for example not a network disruption for political reasons.

On the global level, legal instruments intending to combat cybercrime are discussed for quite some time. Already five United Nations Groups of Governmental Experts (UNGGE) have exchanged ideas and published reports, without, however, being able to agree on binding principles.¹² The most forward-looking statement in respect of the importance of the herein-after addressed international law has been made by the fourth UNGGE:

'1. In the use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.

¹⁰ For an overview see Weber (n. 8), 284 ff.

¹¹ Specific security provisions are contained in the ITU- and WTO-Agreements (for further details Weber [n. 8], 288-290).

¹² For further details see Kulesza and Weber (n. 1), 5-6, and Anders Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace', *Journal of Cybersecurity* 5/1 (2019), 1-9 (4 ff.).

2. Obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.’¹³

Recently, two new groups, namely (i) a further UNGGE and (ii) the United Nations (UN) Cyber Open-ended Working Group (OEWG), have been established (based on not really coherent mandates) with the objective to work out further cybersecurity recommendations in the course of 2021. In March 2021, the OEWG published its Final Substantive Report,¹⁴ but the guidelines remain quite vague. Therefore, the mentioned assessment of the fourth UNGGE that the key principles (or concepts) of international law should play a major role remains valid.

Regional approaches have been more successful: The Council of Europe (CoE) adopted the (Budapest) Convention on Cybercrime in 2001 (being partly outdated in the meantime) encompassing now more than 60 ratifying States (also outside of Europe).¹⁵ The European Union (EU) released the Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union on 6 July 2016¹⁶ with the main objectives/measures of improving (i) national cybersecurity capabilities, (ii) the cooperation on the EU-level and (iii) the security and incident notification requirements as well as the Cybersecurity Act in 2019.¹⁷ As a noteworthy remark it may be added that the term digital infrastructure is mentioned in Annex III of the Network and Information Systems (NIS)-Directive alongside to energy, transport, banking, health sector, and drinking water supply as a critical infrastructure.¹⁸

Reality shows that in particular the efforts on the global level for the implementation of cybercrime regulations have failed to be successful. Even

¹³ UNGGE on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of 26 June 2015, A/70/174.

¹⁴ For the appointment see UNGA Resolution 73/266 of 22 December 2018, A/RES/73/266 and UNGA Resolution 73/27 of 5 December 2018, A/RES/73/27; for the OEWG-Report of 10 March 2021 see UN Doc. A/AC.290/2021/CRP.2; a first critical analysis of the Report can be found in Rolf H. Weber, ‘Cybersecurity Governance – international law as policy driver?’, Jusletter IT, 27 May 2021, no. 12 and nos 67–69.

¹⁵ Council of Europe, Convention on Cybercrime, ETS no. 185, Budapest, November 2001.

¹⁶ OJ 2016 L 194/1 of 19 July 2016.

¹⁷ Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ 2019 L 151/15.

¹⁸ To the discussions in the context of Annex III see Joanna Kulesza und Rolf H. Weber, Protecting the Public Core of the Internet (Delhi: GCSC 2017), 2017, 75–98 (87), <<https://www.researchgate.net>>; see also Weber (n. 14), no. 16.

the CoE Cybercrime Convention did not have remarkable effects.¹⁹ The EU legal instruments are restricted to their regional scope of application. In addition, as mentioned, traditional cybercrimes only are a limited part of the issues influencing the integrity of the Internet, not even covering all aspects of cybersecurity as well as neglecting the elements of cyber stability and cyber resilience.

This assessment justifies a broader analysis of the possibilities to make the international legal concepts fruitful in the Internet integrity context. The objective of this article consists in the attempt of finding a proper foundation for the improvement of Internet integrity. By purpose, not the well-known international legal principles of public international law as stated in Article 38 of the Statute of the International Court of Justice but the widely acknowledged cyberspace concepts will be in the focus of the considerations.

III. Searching the Holy Grail: Embedding Internet Integrity into International Legal Concepts

1. Moving to Global Cosmopolitan Governance

In public international law, it is not contested that new norms and policies should be developed in order to enhance the global security, stability and resilience of the Internet. As Martti Koskeniemi has recently noted, international law contributes to global governance aiming at a 'cosmopolitan future, a united humanity governed by a global law'.²⁰ The concept of cosmopolitanism drives towards a certain decentralization of State power in the interest of a more global appreciation.²¹ An appropriate policy framework encompassing democratic and accountable global governance principles is the most suitable way of implementing cosmopolitan concepts of justice.²²

¹⁹ Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', Mon. L. R. 40 (2014), 698-736 (701 ff.); Weber (n. 8), 283-284.

²⁰ Martti Koskeniemi, 'International Law as "Global Governance"' in: Justin Desautels-Stein and Christopher Tomlins (eds), *Searching for Contemporary Legal Thought* (Cambridge: Cambridge University Press 2017), 199-218 (199); see also Rolf H. Weber, 'New "Cosmopolitically" Founded Concepts for the Cyberworld' in: Giovanni Biaggini, Oliver Diggelmann and Christine Kaufmann (eds), *Polis und Kosmopolis, Festschrift für Daniel Thürer* (Zurich and Baden-Baden: Dike and Nomos 2015), 779-786 (781-782).

²¹ See Francis Fukuyama, *Governance and World Order of the Twenty First Century* (Ithaca NY: Cornell University Press 2004), 98-99.

²² For further details see Rolf H. Weber, *Internet Governance at the Point of No Return* (Zurich: EIZ Publishing 2021), 37-38.

The merits of the international legal concepts to be discussed hereinafter are reflected in the fact that some constitutional norms have already emerged at the global level, even if tensions can exist between different spheres of policy-making and even if the categories that supported universalism from relativism are blurred.²³ In this context, the term societal constitutionalism (Teubner) has been coined to explain developments in civil society and provide for general foundations of rule-making by way of normative standards.²⁴ Similarly, the term digital constitutionalism is used to describe the practice of articulating a set of political rights, governance norms, and limitations on the exercise of powers on the Internet.²⁵

In addition, scholars increasingly acknowledge that based on actual cooperation in networks even treaty compliance might gain better attention in solution-oriented systems of transgovernmentalism.²⁶ Strategies of transnational advocacy networks in digital constitutionalism have been mobilised from a political and a legal angle. Based on a wide variety of theoretically developed and potentially applicable regulatory models²⁷ it is generally acknowledged that global civil society in a transnational sphere must encompass manifold stakeholders that realise shared values, dense exchanges of information, and a common discourse.²⁸

As a concrete translation of general governance principles in the Internet integrity context, the Global Commission on the Stability of Cyberspace (GCSC) has proposed a comprehensive Cyberstability Framework in November 2019, at the occasion of the Internet Governance Forum (IGF) in Berlin, encompassing (1) multistakeholder engagement, (2) cyber stability principles, (3) development and implementation of voluntary norms, (4) adherence to international law, (5) confidence building measures, (6) capacity building objectives, and (7) open promulgation and wide spread use of technical standards ensuring cyber stability.²⁹ This framework has again been presented at the (virtual) Internet Governance Forum in November 2020,

²³ Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalisation* (Oxford: Oxford University Press 2012), 51-52.

²⁴ Teubner (n. 23), passim; Weber (n. 20), 781-782.

²⁵ See Dennis Redeker, Lex Gill and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights', *International Communication Gazette* 80 (2018), 302-319 (302-303).

²⁶ See Kal Raustiala, 'The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law', *Va.J. Int'l L.* 43 (2002), 1-92 (1, 23-24, 55-56, 76).

²⁷ The manifold regulatory models cannot be discussed in the context of this article; for a detailed description, differentiating between first generation and second generation regulatory models see very recently Weber (n. 22), 17 ff. with further references.

²⁸ See Weber (n. 22), 44 ff. with further references.

²⁹ GCSC (n. 6), 14.

however, the future paths have not yet been clearly defined for the time being.

2. Coping with Digital Sovereignty

The sovereignty principle has its roots in the 16th century. As term originally coined by the philosopher and legal scholar Jean Bodin (1576), the historical concept goes along with the building-out of nation States.³⁰ The first political document enshrining the sovereignty thinking and prominently reflecting this concept is the Westphalian Peace Treaty of 1648.³¹ Among others, this document contains the right of each State to monopolise certain exercises of power within its territory.

In the meantime, the global infrastructures as well as some international legal instruments (particularly the UN Charter) set limits to national legislation. Therefore, the traditional sovereignty concept must address alternative values in the context of power allocation. In other words, governance is changing under conditions of interconnectedness now happening. Such a new concept of cooperative sovereignty should lead to a shared responsibility for global resources and to the establishment of standards for interstate cooperation.³²

During the last few years, political sensitivities related to sovereignty aspects again gained importance. Nation States more frequently claim a right to control the infrastructures and the data flows. As a new term, the notion of digital (or data) sovereignty has been coined.³³ The respective right is invoked by States as a protective or empowerment stance regarding a multitude of stakeholders.³⁴

However, an extensive notion of digital sovereignty causes the risk that international governance principles will become re-nationalised and the global Internet evolves into a so-called 'Splinternet', particularly since some countries think of creating an independent national Internet.³⁵ Such a development that leads to fragmentation is undesirable; any kind of fragmentation

³⁰ Weber (n. 22), 87.

³¹ Kulesza and Weber (n. 1), 3.

³² For further details see Weber (n. 22), 87-88 with additional references.

³³ The term digital sovereignty is partly also used for the vision of digital self-determination being the autonomy of individuals and their right to control the data they own or generate. This notion is not further discussed hereinafter.

³⁴ See Internet & Jurisdiction Policy Network, *We Need to Talk About Data – Framing the Debate Around the Free Flow of Data and Data Sovereignty*, Paris 2021, 35 ff., 39, <<https://www.internetjurisdiction.net>>.

³⁵ Weber (n. 22), 88-89.

would not be future-oriented and have a negative impact on global infrastructures.³⁶

Consequently, in order to avoid fragmentation, the governance functions should remain embedded in horizontal structures creating a multistakeholder environment.³⁷ In addition, a political force is needed to stand up for the value of global connectivity and for the right of people everywhere to self-govern their online transactions.³⁸ The respective substantive foundation of the interrelations can be built by the hereinafter discussed international legal concepts.

IV. Fructification of Available Legal Concepts

Based on the described theoretical concepts of global governance, the general assessment can be made that Internet integrity might be reasonably warranted if the international community is ready to accept some basic and common legal standards being applicable around the globe (in addition to the mentioned international legal principles of the International Court of Justice Statute).³⁹ Several theoretical models have been developed so far; as the most important international legal notions, the concepts (i) of global public goods, (ii) of shared spaces, and (iii) of State responsibility will be further analysed hereinafter.

1. Concept of Global Public Goods

One of the starting points for a discussion on protecting the integrity of the Internet could be the concept of global public goods.⁴⁰ Although not

³⁶ Daniel Voelsen, *Risse im Fundament des Internets: Die Zukunft der Netzinfrastruktur und die globale Internet Governance*, SWP-Studie, Berlin 2021, 27-28; Milton Mueller, *Will the Internet Fragment?, Sovereignty, Globalization, and Cyberspace* (Cambridge: Polity 2017), 131.

³⁷ Roxana Radu, *Negotiating Internet Governance* (Oxford: Oxford University Press 2019), 194.

³⁸ See also Weber (n. 22), 88-89, and Mueller (n. 36), 131-132.

³⁹ Already 15 years ago, Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law' in: Max Planck UNYB, Vol. 10 (The Hague: Brill 2006), 191-272 (271), called on international law to 'take a normative stance' in respect of the Internet's future. Recently, Matthias C. Kettemann, *The Normative Order of the Internet* (Oxford: Oxford University Press 2020), 81 ff., analysed the general principles of international law in depth.

⁴⁰ For a general overview see Inge Kaul, Isabelle Grunberg and Marc A. Stern 'Defining Global Public Goods' in: Inge Kaul, Isabelle Grunberg and Marc A. Stern (eds), *Global Public Goods: International Cooperation in the 21st Century* (Oxford: Oxford University Press 1999), 2-19 (10 ff.); Rolf H. Weber and Valérie Menoud, *The Information Society and the Digital Divide: Legal Strategies to Finance Global Access* (Zurich: Schulthess 2008), 24 ff.; Gregory Shaffer, 'International Law and Global Public Goods in a Legal Pluralist World', *EJIL* 23 (2012), 669-693 (675 ff.); Nico Krisch, 'The Decay of Consent: International Law in an Age of Global Public Goods', *AJIL* 108 (2014), 1-40 (1 ff.).

perfectly aligned to the needs of Internet integrity and the network's architecture, it is worth a closer look. Ideally, global public goods are those which benefit humanity as a whole; accordingly, these goods should be advantageous to (i) more than one group of countries or geographic regions, to (ii) a broad spectrum of the global population, crossing population segments, and to (iii) present generations without jeopardising the ability of future generations to meet their own needs.⁴¹ Insofar, the global public goods contribute to the common heritage of mankind.

The idea of guaranteeing Internet integrity as a public core element of the international infrastructure or as a global public good can be perceived as a derivative of a policy concept: The ambiguous notion of global public goods, as generated in the era of globalisation, is derived from the economic literature on public goods.⁴² It refers to all globally available goods that are non-rivalrous (consumption does not influence the quantity available to others) and non-excludable (their use cannot be prevented); the examples of global public goods include knowledge as well as the common heritage of mankind.⁴³

International law in its traditional form with its consensus-based structure is not easily suitable to meet the requirements of the global public goods concept. Moreover, a structural bias exists; in particular, the Westphalian system leads to severe problems for this concept. As Nobel Memorial Prize (2018) laureate William N. Nordhaus pointed out:

'The requirement for unanimity is in reality a recipe for inaction. [...] To the extent that global public goods may become more important in the decades ahead, one of our main challenges is to devise mechanisms that overcome the bias toward the status quo and the voluntary nature of current international law in life-threatening issues.'⁴⁴

Nevertheless, experience over the last few years has shown that international law is not without solutions to such problems.⁴⁵

Furthermore, from an international law perspective, global public goods theories are not a totally new approach. The idea of a certain communality (or common interest) already lies at the core of the Roman law concepts of

⁴¹ Weber and Menoud (n. 40), 24.

⁴² Krisch (n. 40), 3 ff.; see also International Task Force on Global Public Goods, *Meeting Global Challenges: International Cooperation in the National Interest*, Final Report, Stockholm 2006, 15.

⁴³ Kulesza and Weber (n. 1), 4.

⁴⁴ William D. Nordhaus, Paul Samuelson and the Global Public Goods (New Haven: Yale University 2005), 8, <<http://www.econ.yale.edu>>.

⁴⁵ See also Krisch (n. 40), 4.

ius cogens as expression of compelling law or of a peremptory norm based on a universal agreement and of *erga omnes* encompassing rights and obligations being owed toward all.⁴⁶ Similarly, the concept of critical infrastructures and their protection is suitable to serve as another complementary point of reference.⁴⁷ In addition, the well-known public interest concept is also able to peremptorily impose binding obligations on States that have a similar foundation.⁴⁸ Based on these thoughts it can be argued that global public goods theories involve a relatively broad approach that considers political economy implications besides legal aspects⁴⁹ and, therefore, merits attention in future discussions.

2. Concept of Shared Spaces

a) Objective of the Concept

International cooperation in the context of infrastructure protection is not the only analogy to be drawn from existing legal frameworks.⁵⁰ Equally, for example, the concept of shared spaces, to be used by all States in a uniform, non-harmful way is quite well known to the international community and in international relations. Already Grotius in the 17th century explained the law of all Nations as the law ‘derived from nature, the common mother of us all, and whose sway extends over those who rule nations’.⁵¹

Many global legal areas, constituting a ‘law of international spaces’,⁵² have turned out to be relevant over time. From a substantive perspective, it can be said that a feature common to the international spaces encompasses the obligation of peaceful use of resources and the principle of equal rights of all

⁴⁶ Weber and Menoud (n. 40), 24; Kettemann (n. 39), 33–36; Peter-Tobias Stoll, ‘Global Public Goods: the Governance Dimension’ in: Volker Rittberger, Martin Nettesheim and Carmen Huckel (eds), *Authority in the Global Political Economy* (New York: Palgrave Macmillan 2008), 116–136 (116 ff.).

⁴⁷ See below chapter V.2.

⁴⁸ Weber (n. 8), 304.

⁴⁹ Weber and Menoud (n. 40), 25–27.

⁵⁰ Rolf H. Weber, *Realizing a New Global Cyberspace Framework* (Zurich: Schulthess 2014), 19.

⁵¹ Hugo Grotius, *The Freedom of the Seas or the Right Which Belongs to the Dutch to Take Part in the East Indian Trade: a Dissertation*, Leiden 1609, ed. by James Brown Scott (New York: 1916), 5. An impressive new analysis of the international rule of law has recently been given by Martti Koskenniemi, ‘Imagining the Rule of Law: Reading the Grotian “Tradition”’, *EJIL* 30 (2019), 17–52.

⁵² This term was introduced by John F. Kish, *The Law of International Spaces* (Leiden: Sijthoff 1973).

States. Indeed, several authors already expressed the opinion that Internet safety and security can be seen as a shared responsibility.⁵³

b) Examples: Comparable International Legal Instruments

Based on this understanding, several areas of international law appear to be suitable for reference as emanations of a legal order that guarantees common values similar to Internet integrity:⁵⁴

(i) *Air and space law*: The legal regime of outer space was basically established by the Treaty of Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies of 1976.⁵⁵ The main purpose of this treaty consists (i) in the submission of all outer space activities to international law, as well as (ii) in the implementation of the principles of non-discrimination and of non-appropriation by any claim of sovereignty.⁵⁶ Air law is also subject to many multinational treaties under the auspices of the International Civil Aviation Organization (ICAO).⁵⁷ In fact, the law of outer space appears to be the most prominent example for the implementation of the shared spaces concept.

(ii) *Law of the sea*: The most important rules for the maritime area are contained in the Convention on the High Seas of 1958 and the Convention on the Law of the Sea of 1982.⁵⁸ The main objective of these Conventions, being a good example of a wide multifaceted cooperation, consists in the establishment of the freedom of the seas' principle and in the regulation of the common space (i.e. the oceans) for the economic exploitation.⁵⁹ Therefore, the legal instruments governing the maritime environment are good examples for the concept of shared spaces.

(iii) The laws of outer space and of the seas are particularly showing the importance of cooperative efforts in protecting common interests.⁶⁰ But other areas of law equally know this underlying thought. Even if the parallelism is less

⁵³ See Vinton G. Cerf, Patrick Ryan, Max Senges and Richard Whitt, 'IoT Safety and Security as Shared Responsibility', *Business Informatics* (2016), 7-19 (15-16).

⁵⁴ Kulesza and Weber (n. 18), 88; see also the compilation of articles in Mads Andenas et al. (eds), *General Principles and the Coherence of International Law* (Leiden and Boston: Brill-Nijhoff 2019).

⁵⁵ 610 UNTS 205.

⁵⁶ See also Weber (n. 50), 21; Joanna Kulesza, *International Internet Law* (London and New York: Routledge 2012), 145-146.

⁵⁷ The original multilateral treaty is the Chicago Convention on International Civil Aviation (1944), followed by many Montreal Protocols.

⁵⁸ 450 UNTS 11; 1833 UNTS 397.

⁵⁹ See also Weber (n. 50), 20.

⁶⁰ For further details to the duty of cooperation see Rolf H. Weber, 'Duty of Co-operation as New Cybergovernance Concept', IT Jusletter, 25 February 2021.

obvious and the respective legal areas cannot always be easily linked to the shared spaces concept at first sight, the following legal instruments merit to be mentioned:⁶¹

- *Diplomatic and consular law*: The Vienna Convention on Diplomatic Relations of 1961 contains basic, partly even comprehensive rules about the principles to be observed and complied with in the diplomatic and consular world.⁶² In substance, the compliance with shared values is envisaged.
- *International human rights law*: The need to harmonise global rules in the context of human and fundamental rights has become obvious in the aftermath of the Second World War; the key documents are condensed in the International Bill of Human Rights, composed of the UN Universal Declaration of Human Rights (UDHR, 1948)⁶³ as well as the two UN Covenants on Civil and Political Rights and on Economic, Social and Cultural Rights (ICCPR and ICESR, 1966). Again, these international legal instruments express shared values of humankind.
- *International telecommunication law*: The International Telecommunications Union is the second-oldest international body having been founded in 1865; the need to harmonise the communications' rules has been obvious since then and has even become more important with the advent of the Internet.⁶⁴ As in case of outer space law, the telecommunications infrastructure is a space which needs to be shared by the interested players.
- *International environmental law*: The fact that environmental resources must be used respectfully, sustainably, and in a shared way is well known for decades; several international treaties are existing and have culminated in the declarations related to the climate change challenges (for example the Kyoto Agreement and the Paris Agreement).⁶⁵ Over time, environmental law will increasingly become an area that requires the implementation of common values in spaces to be shared by everybody.

⁶¹ This article cannot dig into all details of the mentioned legal instruments; further research deepening the analysis would be worthwhile; see also Weber (n. 14), nos 35-44.

⁶² 500 UNTS 95. Similar principles are contained in the Vienna Convention on Consular Relations of 1963.

⁶³ UN Resolution 217 A (III) of 10 December 1948.

⁶⁴ See also Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations* (Cambridge: Cambridge University Press 2017), 284 ff.; Richard Hill, *The New International Telecommunications Regulations and the Internet* (Zurich: Schulthess 2013), 141 ff.

⁶⁵ A very clear picture can be drawn from the different reports of the Intergovernmental Panel on Climate Change (IPCC); see for example: An IPCC Report on the impacts of global warming of 1,5°C above preindustrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty, Summary for Policymakers (October 2018).

- *International trade law*: The World Trade Organization, following the General Agreement on Tariffs and Trade and being in place since January 1995, is the best example for the acknowledgment that the liberalisation of global trade and a rule-based system on trade are of utmost importance.⁶⁶ Harmonised rules facilitate the realisation of common (economic) interests.
- *Money laundering and terrorism financing laws and policies*: The fight against money laundering and terrorism financing is a global task. The respective activities are exercised by the Financial Action Task Force (FATF) that has been created as an intergovernmental organisation in 1989 on the initiative of the G7; the standards of the FATF being domiciled at the Organisation for Economic Co-operation and Development (OECD) in Paris are accepted as international recommendations by the World Bank, the International Monetary Fund and the UN Security Council (Resolution 2462 of 28 March 2019).⁶⁷ The developed global measures of the FATF have some similarities with the measures combating the negative effects of cyberattacks; both initiatives attempt at safeguarding shared values.

So far, a concise assessment based on the mentioned areas of international law and relations is still outstanding; nevertheless, the basic principles can be made fruitful in the Internet integrity context.

c) Starting Point for Cooperation

From the analysis of the comparable international legal instruments the conclusion can be drawn that the main examples for a cooperative approach to shared spaces (law of outer space and of the seas) as well as the other legal segments pursuing similar objectives show the importance of further research that could deepen the concept of international spaces as well as the cooperation therein.

As mentioned, each of the referenced legal regimes offers interesting insights that can be useful to Internet integrity, however, a more focussed analysis is needed in order to develop a harmonised and stable framework of global policies. In particular, governments should closely cooperate in continuing efforts to arrive at an operable consensus that takes into consideration

⁶⁶ The re-nationalization of trade policies during the Covid-19-crisis and the subsequent sharp drop of the global trade volume shows the importance of the WTO-rules.

⁶⁷ According to its own mission, the FATF as inter-governmental body sets international standards that aim to prevent money laundering and terrorism financing activities and the harm they cause to society; as a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas, <<https://www.fatf-gafi.org>>.

global interoperability, network stability, reliable access, and cybersecurity due diligence.⁶⁸

3. Concept of State Responsibility and Due Diligence

The concept of State responsibility can be perceived as a general normative guideline, applicable in addition to all other specified international legal norms imposing obligations (for example the no harm principle) upon States.⁶⁹ Once an international obligation of a State is breached – be it an obligation of conduct or one of result – the consequences provided for in the law of State responsibility entail. In contrast to the already mentioned concepts (public goods, shared spaces), the State responsibility principle enshrines a more condensed legal apparatus as an international legal tenet due to its written implementation.⁷⁰

The development of legal rules related to the State responsibility was not an easy task; the efforts of the International Law Commission (ILC) lasted decades; the so-called Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001) have been adopted by UN General Assembly Resolution 56/83 and have become part of the customary law also applied by the International Court of Justice.⁷¹ The ILC based its work on two fundamental presumptions:⁷² (i) A breach of an international obligation of a primary norm leads to a responsibility if a ‘sanction’ is stated therein; otherwise, the responsibility is vested in the general international principle of responsibility as secondary norm. (ii) An international wrongful act causes a State responsibility.

The responsibility concept as of the ILC Draft Articles is materially linked to the due diligence requirements being an underlying in substance and implying a State’s duty to act with proper care in preventing a violation of international law. Indications of what is meant with due care in particular circumstances are to be derived from the legal practice within individual areas

⁶⁸ Wolff Heintschel von Heinegg, ‘Territorial Sovereignty and Neutrality in Cyberspace’, *International Legal Studies* 89 (2013), 123-156 (134 ff.). For concrete examples of cooperative approaches see chapters V.1 and V.2.

⁶⁹ Joanna Kulesza, *Due Diligence in International Law* (Leiden and Boston: Brill/Nijhoff 2016), 115 ff.

⁷⁰ See also Kulesza and Weber (n. 1), 9 with further references.

⁷¹ Draft Articles on Responsibility of States for Internationally Wrongful Acts, ILC Report, 2001, UN Doc. A/56/10 att. 10, (2001) ILCYB, Vol. II, Part Two.

⁷² Kulesza (n. 69), 149 ff. with further references; see also Jovan Kurbalija, ‘State Responsibility in Digital Space’, *Swiss Review of International and European Law* 26 (2016), 307-325 (318 ff.); Weber (n. 22), 95-96.

of international relations between States.⁷³ In the meantime, however, the due diligence principle has even been extended to non-State actors; apart from being a shared element of treaty-based regimes⁷⁴ its increasingly broad scope of application also encompasses private actors such as multinational enterprises (as for example shown in the OECD Due Diligence Guidance).⁷⁵

The concept of due diligence intending to prevent transboundary harm has mainly become important in environmental matters.⁷⁶ Nevertheless, by analogy, a due diligence standard for Internet integrity with shared responsibility⁷⁷ could equally build an entry point for the State's responsibility in respect of an omission resulting in transboundary harm, e. g. a disruption of communications channels within a State territory.⁷⁸ The existing community standards with regard to good business practices related to each of the specific Internet sectors (e. g. root zone operation, Internet Exchange Point [IXP] operation, Domain Name System [DNS], and Top-Level-Domain [TLD] management)⁷⁹ could be considered as harmonised guidelines to be complied with in order to avoid State responsibility.

Due diligence appears in almost all legal regimes, and it is even relevant for the law on neutrality in armed conflicts, which is, in principle, applicable to cyberspace.⁸⁰ In other words, governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access, and cyber-related due diligence.⁸¹

For the sake of completeness it may be added that according to the Tallinn Manual 2.0⁸² general international law must be taken into account in respect of four legal notions, namely (i) sovereignty, (ii) due diligence, (iii) jurisdiction, and (iv) State responsibility.⁸³ While sovereignty and the matrix of jurisdictional principles remain an unresolved challenge for critical infrastructure protection, subject to enhanced debate and still far from consensus, and while the Tallinn Manual 2.0 does not necessarily constitute a rule book for

⁷³ Weber (n. 22), 94-95, with further references.

⁷⁴ See also Kulesza (n. 69), 253 ff.; Kurbalija (n. 72), 323.

⁷⁵ OECD Due Diligence Guidance for Responsible Business Conduct, Paris 2018.

⁷⁶ Kulesza (n. 69), 205 ff.; Kurbalija (n. 72), 312 ff.; Kettemann (n. 39), 95-96; Jay Butler, 'The Corporate Keepers of International Law', AJIL 114 (2020), 189-220 (209-210).

⁷⁷ See also Cerf, Ryan, Senges and Whitt (n. 53), 8-9.

⁷⁸ For further details see Kulesza (n. 69), 276 ff. and 288 f. with further references.

⁷⁹ See below chapters V.1 and V.2 as well as Cerf, Ryan, Senges and Whitt (n. 53), 14.

⁸⁰ Schmitt (n. 64), 30 ff.

⁸¹ Kulesza and Weber (n. 1), 9; to the due diligence principle in other legal areas see Kettemann (n. 39), 97-101.

⁸² Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017.

⁸³ See also Schmitt (n. 64), 11 ff. with further references; Schmitt formulates not less than 31 specific Rules.

States,⁸⁴ the two other principles, namely due diligence and State responsibility, can be reasonably applied to the biggest international open networks and their key components.⁸⁵ As the Global Commission on the Stability of Cyberspace has identified, uniform standards of protection for the whole infrastructure and its services recognised as fundamental to the global networks' stable and reliable operations are necessary and can be expressed through (i) international cooperation, (ii) exchange of good practices, and (iii) benchmarking.⁸⁶

4. Further Potential Concepts

The three discussed concepts, namely the global public goods, the shared spaces and the State responsibility, appear to constitute the most important international legal guidelines. Nevertheless, further Internet-specific concepts have been developed that could also be made fruitful; in particular, the GCSC addressed the following legal notions:

(i) The *requirement of restraint* imposes on States and non-state actors the behavioural rule to act in accordance with general principles of international peace and security in order to avoid that harmful acts are undermining the resilience and stability of cyberspace.⁸⁷

(ii) The *requirement to act principle* contains a duty to take affirmative action for preserving the stability of cyberspace; States and non-state actors should take care that inadvertently escalating tensions or increasing instability are avoided.⁸⁸

(iii) Furthermore, *human rights* are important legal yardsticks that can safeguard cyberspace stability; the disruptive effect on human activity resulting from threats endangering the availability or integrity of information and communications technologies is obvious and impacts human rights of individuals in a severe way.⁸⁹

The mentioned concepts as developed by the GCSC in respect of cyberspace stability equally contribute to and should be part of Internet integrity.

⁸⁴ For a critical assessment of the Tallinn Manual 2.0 see Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *AJIL* 112 (2018), 583 ff.

⁸⁵ Weber (n. 8), 299.

⁸⁶ GCSC (n. 6), 95.

⁸⁷ GCSC (n. 6), 18.

⁸⁸ GCSC (n. 6), 19.

⁸⁹ GCSC (n. 6), 19.

In addition, the eight specific norms drafted by the GCSC⁹⁰ are also important in respect of the Internet integrity environment. For example, the first norm reads as follows: 'State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.'

The above discussed international legal concepts must be kept in mind when assessing the notion of soft law hereinafter.

V. Relevance of Soft Law for Internet Integrity

Having analysed the importance and contents of applicable international legal concepts, the follow-up question arises what legal quality can be attributed to these concepts. Obviously, traditional legal instruments constituting hard law are not largely available in this context. However, alternative legal sources are equally suitable for the implementation of the discussed concepts.

Experience has namely shown that the traditional hard law is not able to cope with all normative challenges appearing around the globe in all segments of society. Moreover, different forms of soft law increasingly play an important role in the normative environment.⁹¹ Indeed, legal doctrine is now stating that the dichotomy between hard law and soft law must be overcome.⁹² This assessment goes hand in hand with the acknowledgment that – in contrast to the traditional international public law understanding – private actors can also become 'keepers of international law'.⁹³ Alternative approaches of (private) rule-making equally encompass fundamental legal principles to be observed by the concerned actors; hereinafter, the two main forms, namely self-regulation and co-regulation, will be discussed.

1. Self-Regulatory Approaches

Self-regulation refers to the rules that are autonomously developed and implemented by the governed persons, independently from any structured

⁹⁰ GCSC (n. 6), 21-22.

⁹¹ Rolf H. Weber, *Regulatory Models for the Online World* (Zurich: Schulthess 2002), 85 ff.

⁹² Rolf H. Weber, 'Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crisis', *Journal of Governance and Regulation* 1 (2012), 8-14 (8 ff.).

⁹³ Term used by Butler (n. 76), 189.

form of rule-making. The legitimacy of self-regulation is based on the merits of the incentive- and need-driven rule-setting processes. Self-regulation is responsive to changes in the environment and can establish rules without regard to the territoriality principle.⁹⁴

A universally accepted theory as to the legal quality of self-regulation has not (yet) been formulated. Since self-regulation is not enforceable through public action, such rules do not have the quality of law in the traditional understanding.⁹⁵ However, compliance with self-regulatory guidelines is usually more than only an ethical undertaking because these provisions correspond to standards that reflect the common sense behaviour expected to be observed by the concerned actors.⁹⁶

The strengths of self-regulation encompass the following elements:⁹⁷ (i) The rules created by the concerned actors of a specific community are efficient since they respond to real needs and mirror the technology. (ii) Meaningful self-regulation provides the opportunity to adapt the regulatory framework to the changing technology. (iii) Self-regulation can usually be implemented at reduced costs. (iv) Due to the private initiatives the chances are high that the rules contain incentives for compliance. (v) Effective self-regulation induces the concerned actors to be open to a permanent consultation process related to the development and implementation of the rules.

Self-regulation has played in the past and is still playing an important role in the context of the critical Internet infrastructures: At least from a technical angle, the current Internet governance landscape was originally designed on the basis of bottom-up governance models, strongly rooted in the technical community, for example the Internet Society (ISOC) or the Internet Engineering Task Force (IETF) with its 'Requests for Comments' (RFC);⁹⁸ these bodies are implementing community-developed common standards to be voluntarily followed by their members, namely Internet service providers and software developers.⁹⁹

While security by design remains a common paradigm within both, ISOC and IETF, a connection between this extra-legal, community-based rule-making approach and the hard norm-setting models of States cannot easily

⁹⁴ Weber (n. 50), 23 with further references; see also Butler (n. 76), 199 ff.

⁹⁵ Weber (n. 91), 81-83; Andrew Guzman and Timothy L. Meyer, 'International Soft Law', *Journal of Legal Analysis* 2 (2010), 171-225 (179-183).

⁹⁶ Weber (n. 50), 25.

⁹⁷ Weber (n. 91), 83-84 with further references.

⁹⁸ Eric Rescorla, 'Guidelines for Writing RFC Text on Security Considerations' (2003), <<https://tools.ietf.org/>>; see also Butler (n. 76), 209-210.

⁹⁹ Kulesza and Weber (n. 18), 82.

be established.¹⁰⁰ Notwithstanding the fact that the Internet Corporation for Assigned Names and Numbers (ICANN), the ISOC, and the Internet Governance Forum (IGF) have been attending to the issue, this communications' gap holds crucial relevance for the development of any effective international Internet integrity policies and must be addressed by whatever model of global cyber governance.¹⁰¹ There can be no effective policy developed solely at governmental level without strong presence of the technical community and vigilant input from civil society. Experience has shown that a compromise between the protection of fundamental infrastructure (Internet) functions and community-based technical standards must be achieved.¹⁰²

Looking from the angle of self-regulatory initiatives, the already discussed policy paper of the GCSC also advocates for the inclusion of private rule-makers (multistakeholderism).¹⁰³ The developed principles to be observed by States and non-state actors have the objective of securing an environment in which the actors do not engage in any activities that impair the stability of the Internet and/or endanger the protection of the Internet's public core (enshrining its integrity).¹⁰⁴ In addition, actors are invited to implement appropriate measures to ensure basic cyber hygiene.¹⁰⁵ Taking into account the various approaches developed in the global arena of international organisations, private actors, and academic scholars, the norms and principles developed as private rule-making in the GCSC-Report merit to be further concretised.

2. Co-Regulatory Approaches

Self-regulatory initiatives can also be supported by international organisations or national governments. This approach is often called co-regulation being a term that has been coined more than 20 years ago in the context of broadcasting as public good (being one of the above discussed

¹⁰⁰ Kulesza and Weber (n. 18), 82 and 89.

¹⁰¹ For the parameters of a cyberspace framework see Weber (n. 50), 102 ff.

¹⁰² For a thorough study of the impact of technical standards on cybersecurity see Dennis Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and International Security', *Journal of Cyber Policy* 2 (2017), 366-376.

¹⁰³ GCSC (n. 6), 17. For a more detailed discussion of the multistakeholder approach see Christine Kaufmann, 'Multistakeholder Participation in Cyberspace', *Swiss Review of International Law and European Law* 26 (2016), 217-234; Rolf H. Weber, 'Legal Foundations of Multistakeholder Decision-Making', *ZSR* 135 (2016), 247-267.

¹⁰⁴ GCSC (n. 6), 18-19; see also Kettemann (n. 39), 25-26.

¹⁰⁵ See also Recital 8 of EU Cybersecurity Act 2019 (n. 17).

concepts).¹⁰⁶ An involvement of other stakeholders than the directly concerned actors is usually strengthening the rule-making processes. Apart from the term co-regulation such kind of cooperative rule-making is also called regulated self-regulation, directed self-regulation or audited self-regulation.¹⁰⁷

Co-regulation as a model is often designed by a general framework established in the form of governmental regulations which than is concretised by the private sector; in other words, the State legislator sets the legal milestones and leaves the qualification of the given principles by way of specific rules to private bodies. Thereby, regulation can remain flexible and innovation-friendly. In addition, the government remains involved in the private rule-making activities at least in a monitoring function supervising the progress and the effectiveness of the initiatives in meeting the perceived objectives.¹⁰⁸

In the Internet governance environment the participation models encompassing governmental bodies and private actors has been coined by using the term multistakeholderism; this concept attempts at including all potentially concerned stakeholders in the relevant decision-making processes.¹⁰⁹ Even if multistakeholderism as an increasingly important governance model that cannot be discussed in depth hereinafter is not a value as such and not a one-size-fits-all solution, the concept remains a possible approach for meeting salient public interest objectives. In addition, it should not be overlooked that multistakeholderism is crucial in the traditional Internet environment (for example regarding the processes in ICANN) as well as in the general infrastructure context (for example within the International Telecommunication Union [ITU]).¹¹⁰

Since it is often difficult to fully tackle the Internet integrity challenges by way of self-regulatory initiatives due to the lack of enforcement means, co-regulation can have a positive impact on the behaviour of the concerned

¹⁰⁶ For an early discussion see Gareth Grainger, 'Broadcasting, Co-Regulation and the Public Good' Paris 1999.

¹⁰⁷ Weber (n. 50), 23-24; Wolfgang Hoffmann-Riem, *Regulierung der dualen Rundfunkordnung* (Baden-Baden: Nomos 2000), 154-155.

¹⁰⁸ Myriam Senn, *Non-State Regulatory Regimes. Understanding Institutional Transformation* (Berlin: Springer 2011), 43, 139-148, 230; Chris Marsden, Trisha Meyer and Ian Brown, 'Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation', *Computer Law & Security Review* 36 (2020) 105373, 1-18 (9).

¹⁰⁹ The (in the meantime) far-reaching discussions about the multistakeholder concept (incl. its strengths and weaknesses) are not within the scope of this contribution (for a general overview see the authors cited in n. 103 with further references).

¹¹⁰ For further details see Kal Raustiala, 'Governing the Internet', *AJIL* 110 (2017), 491-503 (491, 495-496).

market participants. Joint efforts of various stakeholders also allow the governments to assess the representativeness of self-regulatory standards and to judge the appropriateness of best practices; interventions appear justified if a higher level of protection measures is desirable.¹¹¹ Reality shows that such kind of co-regulatory approaches are already existing in the field of critical infrastructures:

(i) An important intergovernmental attempt to directly address the issue of Internet's infrastructure at the policy level is the CoE Report of 2009 with the title 'Internet Governance and Critical Internet Resources'.¹¹² It identified *Critical Internet Resources* (CIR) that require particular care from the international community to ensure the free and reliable flow of information online. According to the CoE, the CIR include root servers, the Domain Name System (DNS), the Internet Protocol and the Internet backbone structures, as well as Internet Exchange Points (IXPs).¹¹³ The CoE emphasised the need to secure universal broadband access and network neutrality and linked the need to protect CIR with the existing critical resources perception, indicating the Internet itself as a 'critical resource' and arguing that for it to remain 'sustainable, robust, secure and stable' it must be protected 'in the same way than other critical common resources'.¹¹⁴

(ii) Critical infrastructure protection as provided by existing national regimes and international cooperation programmes, such as the European Programme for Critical Infrastructure Protection (EPCIP), usually encompasses networks being fundamental to the daily operation of any modern society: water and energy supply, mass transportation, health and emergency services and alike.¹¹⁵ The last and newest category included in Annex III to the NIS Directive covers 'digital infrastructures' and encompasses (i) IXPs, (ii) DNS service providers and (iii) Top-Level-Domain (TLD) name registries.¹¹⁶ These categories mirror the current EU approach to cyber resilience, viewing crucial Internet infrastructures as part of the European critical infrastructures ecosystem. Effectively, they all require a high level of protection by their operators, including e.g. security due diligence measures and risk assessments.¹¹⁷

¹¹¹ Marsden, Meyer and Brown (n. 108), 9. An example outside of the Internet scope is the UN Security Council Resolution 2462 of 28 March 2019 imposing a duty on the States to comply with the FATF-Guidelines (above chapter IV.2.b) at n. 67).

¹¹² Council of Europe, Internet Governance and Critical Internet Resources Report, Strasbourg 2009.

¹¹³ Council of Europe (n. 112), 13-15.

¹¹⁴ Council of Europe (n. 112), 23; see also Kulesza and Weber (n. 1), 6.

¹¹⁵ Kulesza and Weber (n. 1), 8.

¹¹⁶ NIS-Directive (n. 16), Annex II.

¹¹⁷ See also Kulesza and Weber (n. 18), 83-84.

VI. Forward-Looking Perspectives

1. Implementation of International Legal Concepts Based on Soft Law

The identification of international legal concepts and relevant soft law norms does not suffice. Moreover, it is important to fully implement the respective (binding or non-binding) guidelines. As experience has shown during the last years, enforcement of legal provisions is always difficult in the international context, even more so in case of soft law. Furthermore, general principles as well as international legal concepts need to be embedded into the overall normative framework; in this respect, additional elements such as cohesion, convergence, and coherence merit more attention in the future.¹¹⁸

A first step could consist in the improvement of the involved actors' commitments, for example by engaging in capacity building efforts and confidence building measures.¹¹⁹ Implementing norms in a more granular way helps developing a consensus on the inherent value of norms and can lead to a better understanding of their relevance. Global governance also means that the concerned persons are enabled to identify, understand, and address potential transnational problems.¹²⁰ Partly, the respective efforts have been introduced but much more needs to be done.

As experience has shown, capacity building and confidence building alone do not lead to an appropriate implementation of normative guidelines. The sharing of best practices and of resilience/security standards must be encouraged on the basis of the acknowledged international legal concepts. Indeed, concrete steps are necessary to give them force.¹²¹ The discussed international legal concepts (global public goods, shared spaces, State responsibility) are to be operationalised by incorporating them into global and national policies as well as into transgovernmental regulations.

2. Search of New Paths Leading to Internet Integrity

The governance of the Internet and its integrity is an objective that should eliminate or at least minimise risks caused by an inappropriate use of interna-

¹¹⁸ For more details see Mads Andenas and Ludovica Chiussi, 'Cohesion, Convergence and Coherence of International Law' in: Andenas et al. (n. 54), 9-34.

¹¹⁹ GCSC (n. 6), 23.

¹²⁰ See Weber (n. 20), 781.

¹²¹ GCSC (n. 6), 23-24.

tional electronic infrastructures. Risk is the function of the likelihood of an adverse event, interacting with the magnitude of harm upon its occurrence.¹²² Precautionary measures can also be taken by private actors, for example by way of standardisation, as the network security provisions of ISO/IEC 27001 of 2013 as well as the updated extension ISO/IEC 27701 of 2019 show.¹²³ In order to achieve a reasonable Internet integrity governance it is necessary to implement a new normative framework based on international legal principles through (i) private institutions with regulatory functions, (ii) hybrid intergovernmental-private arrangements, (iii) distributed regimes of regulators in cooperative schemes, and (iv) collective actions by transnational networks.¹²⁴

Previous experience in the field of cybercrime and cybersecurity has shown that the traditional international law approach operating on the State level through multilateral treaties, thereby failing to directly address duties of private actors, is hardly able to cope with the challenges of combatting ongoing interference measures with Internet integrity (in different forms). Therefore, the inclusion of various stakeholders into a new regulatory framework appears to be unavoidable. This attempt has been undertaken by Microsoft in 2017/18 when suggesting the adoption of an international treaty to guarantee the peaceful use of cyber space.¹²⁵ The proposal to develop a Digital Geneva Convention is referring to the Treaty on the Non-Proliferation of Nuclear Weapons and the Treaty on Chemical Weapons as examples of international regimes that intend to limit vital threats to human existence. However, this proposal met the scepticism of many States and it also seems unclear to what extent other Internet stakeholders could be included in such an arrangement.¹²⁶ In addition, the linkage to widely acknowledged international legal concepts appears to be underdeveloped.

The so far (incoherent) patchwork of Internet integrity rules does not really correspond to the political and societal requirements. As the recent developments show, Internet integrity indeed exceeds cybersecurity issues and also encompasses core elements of human rights and of human development.¹²⁷ Therefore, the need for a stable normative order is undoubtedly

¹²² Weber (n. 8), 307.

¹²³ International Standardisation Organisation, ISO/IEC 27001:2013, <<https://iso.org/>>.

¹²⁴ Weber (n. 8), 307.

¹²⁵ Microsoft, Cybersecurity Policy Framework, Geneva 2018, <<https://www.microsoft.com/>>.

¹²⁶ Brad Smith, CEO of Microsoft, proposed the name 'A Digital Geneva Convention' in order to underline that cyberspace in a broad scope should be protected (2017), <<https://blogs.microsoft.com/>>; for further details see Weber (n. 14), nos 65-66.

¹²⁷ For further details see Kettemann (n. 39), 36 ff.

given.¹²⁸ The only (partial) exception of normativity concerns the EU with the recently adopted (directly or indirectly applicable) legal cybersecurity regime (NIS-Directive, Cybersecurity Act, Cybersecurity Strategy of December 2020);¹²⁹ however, the practical implementation in the EU still needs to become successful. In addition, cyber stability and cyber resilience are only vaguely addressed.

On a global level, further efforts to achieve a better coordinated Internet integrity framework with a broad ambit are required: Amongst others, due diligence standards should be identified based on good business practice, benchmarking, exchange of information, and international cooperation.¹³⁰ In addition, the herein discussed commonly developed international legal concepts such as the concept of public goods, of shared spaces, and of State responsibility might be a good way for going forward and for paving a better path to Internet integrity. These concepts could assume a steersman task and thereby realise governance functions. In order to make such approach successful and to avoid disappointments of civil society about the '*Infinite Space*' (Star Trek), academics and businesses are called to contribute innovative ideas to the respective efforts and design possible new frontiers for international law.

¹²⁸ A respective framework is outlined in Rolf H. Weber, 'Elements of a Legal Framework for Cyberspace', *Swiss Review of International and European Law* 26 (2016), 195-215 (202 ff.); see also the recent considerations of Kettemann (n. 39), 182 ff. and 233 ff.

¹²⁹ See also Weber (n. 14), no. 17.

¹³⁰ Kulesza and Weber (n. 1), 12.

Equality as a Principle of the Networked World? An Exploratory Search for ‘Cyber-Equality’ in the Field of Internet Governance

Nula Frei*

Institute for European Law, University of Fribourg, Fribourg, Switzerland
nula.frei@unifr.ch

Abstract	627
Keywords	628
I. Introduction	628
II. The Principle of Equality and Its Foundations in International Law	631
III. Networked Inequality	635
IV. Tracking Down Equality in Internet Governance	638
1. ICANN Bylaws	638
2. WSIS Outcome Documents	640
3. NETmundial	643
4. EU Digital Services Act Proposal	644
5. The State of Equality in Internet Governance: An Interim Conclusion	647
V. Equality in Internet Governance: The Way Forward	648

Abstract

Even though equality is a fundamental and transversal norm of international law, not much has been written about its role for cyberspace. The utopia of the ‘inventors’ of the internet was to create an open, transparent, and democratic space, and early proponents of cyberfeminism even believed that gender differences in general would disappear by improving technology. However, a look at the status quo suggests that cyberspace might currently be even farther away from an egalitarian ideal than the offline world. While openness, universality, and bottom-up procedures, inter alia, are widely accepted as foundational values of cyberspace and of internet governance, it seems that equality has not yet been discussed in depth, despite the apparent signs of what can be called ‘cyber-inequality’. This article undertakes a first step in this direction. It critically examines cyber-equality, i. e., the status quo of equality in cyberspace, and analyses several key documents of internet

* The author would like to thank the anonymous reviewer as well as Dr Raffaella Kunz for helpful comments on the manuscript.

governance from an equality perspective. This analysis allows for some preliminary conclusions, and to lay a foundation for future research, which will be outlined in the final section of this article. The article reveals that there is currently no consistent or comprehensive approach to addressing equality issues in internet governance and that much more research will be needed to better understand the topic and to embed equality considerations in internet governance.

Keywords

internet governance – equality – non-discrimination – technology

I. Introduction

Equality is a fundamental value and a basic principle of liberal democratic societies and is mirrored in several international treaties, customs, principles, and procedures. Deriving directly from the principle of human dignity, it forms a cornerstone of justice and fairness: Treating people differently because of personal, innate or immutable characteristics, such as their gender, ethnicity, class, religion, sexual orientation, would be unfair and a violation of the inherent human dignity of every human being.¹

However, even though equality is of such fundamental value in the ‘offline world’, not much is known about its role for cyberspace. While the utopia of the ‘inventors’ of the Internet was to create an open, transparent, and democratic space, and theorists such as Donna Haraway believed that technology would help making our societies more egalitarian,² a look at the status quo suggests that cyberspace might currently be even farther away from an egalitarian ideal than the offline world: As this contribution will show, not only is the technology needed for the running of Internet applications mostly *designed* by white, well-educated men, but also is *access* to Internet distributed unequally along lines of race, class, and gender.³ Moreover, once access is gained, the possibilities for *enjoyment* of the Internet are unequally dis-

¹ Walter Kälin and Jörg Künzli, *The Law of International Human Rights Protection* (2nd edn, Oxford, New York: Oxford University Press 2019), 336; Charles Taylor and Amy Gutmann (eds), *Multiculturalism and ‘The Politics of Recognition’* (Princeton: Princeton University Press 1992), 13 f.

² Donna Haraway, ‘A Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s’, *Socialist Review* 80 (1985), 65-108.

³ See below, section III.

tributed, with women, queer persons, persons of colour, or religious minorities being more often hindered from fully participating online by different forms of cyber violence and other acts with chilling effect on their enjoyment of this technology. Despite these apparent signs of what will hereinafter be called ‘cyber-inequality’, and despite the fact that cyberspace is not a value-free space *per se*,⁴ equality in cyberspace has not yet been discussed in depth. Some soft-law documents of Internet governance do mention equality, but the academic discussion has so far only highlighted specific aspects of the problem, for example, participation of women in Internet governance,⁵ queer approaches to Internet governance,⁶ the digital divide,⁷ or online violence.⁸ While the academic discussion on Internet and Human Rights has advanced

⁴ For example, openness, universality, and bottom-up procedures, *inter alia*, are widely accepted as foundational values of cyberspace and of Internet governance, see Lawrence Lessig, ‘Open Code and Open Societies: Values of Internet Governance’, *Chicago-Kent Law Review* 74 (1999), 1405-1420; Hans Morten Haugen, ‘The Crucial and Contested Global Public Good: Principles and Goals in Global Internet Governance’, *Internet Policy Review* 9 (2020), 1-22.

⁵ Association for Progressive Communications (APC) and Humanist Institute for Development Cooperation (Hivos), *Global Information Society Watch 2013: Women’s Rights, Gender and ICTs* (1st edn, Montevideo: APC/Hivos 2013); Heike Jensen, ‘Whose Internet Is It Anyway? Shaping the Internet – Feminist Voices in Governance Decision Making’ in: APC/Hivos, *Global Information Society Watch 2013: Women’s Rights, Gender and ICTs*, (1st edn, Montevideo: APC/Hivos 2013), 55-59; Judy Wajcman, *Feminism Confronts Technology* (Cambridge: Polity Press 1991).

⁶ Monika Zalnieriute, ‘The Anatomy of Neoliberal Internet Governance. A Queer Critical Political Economy Perspective’ in: Diane Otto (ed.), *Queering International Law: Possibilities, Alliances, Complicities, Risks* (New York: Routledge 2017), 53-73.

⁷ Jan A. G. M. van Dijck, ‘A Theory of the Digital Divide’ in: Massimo Ragnedda and Glenn W. Muschert (eds), *The Digital Divide: The Internet and Social Inequality in International Perspective* (London: Routledge 2013), 29-53; Jan A. G. M. van Dijk, ‘Digital Divide Research, Achievements and Shortcomings’, *Poetics* 34 (2006), 221-235; Paul DiMaggio, Eszter Hargittai, Coral Celeste and Steven Shafer, ‘Digital Inequality: From Unequal Access to Differentiated Use’ in: Kathryn Neckerman (ed.), *Social Inequality* (New York: Russell Sage Foundation 2004), 355-400; Eszter Hargittai and Yuli Patrick Hsieh, ‘Digital Inequality’ in: William H. Dutton (ed.), *The Oxford Handbook of Internet Studies*, Vol. 1 (Oxford: Oxford University Press 2013); Pippa Norris, *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide* (Cambridge: Cambridge University Press 2001); OECD, *Bridging the Gender Digital Divide* (2018); Bridgette Wessels, ‘The Reproduction and Reconfiguration of Inequality: Differentiation and Class, Status and Power in the Dynamics of Digital Divides’ in: Massimo Ragnedda and Glenn W. Muschert (eds), *The Digital Divide: The Internet and Social Inequality in International Perspective* (London: Routledge 2013), 17.

⁸ Kim Barker and Olga Jurasz, *Online Misogyny as a Hate Crime: A Challenge for Legal Regulation?* (London: Routledge 2019); Kim Barker and Olga Jurasz, ‘Online Violence against Women as an Obstacle to Gender Equality: A Critical View from Europe’, *European Equality Law Review* 1 (2020), 47-60; Maeve Duggan, *Online Harassment 2017*, 11 July 2017, <<https://www.pewresearch.org/>>.

considerably in the last years⁹ and it is widely accepted that International Human Rights Law also applies in cyberspace,¹⁰ the specific topic of equality and non-discrimination remains under-researched and under-theorised.

This article undertakes a first step in closing this research gap and aims to find out to what extent the principle of equality is already implicitly or explicitly addressed in the field of Internet governance. To this end, an exploratory content analysis of key documents of Internet governance, most of them soft law, will be conducted. This analysis will make it possible to draw initial conclusions about the role and place of equality in Internet governance and to identify existing gaps. While this study is only a first step with a limited selection of cases, and hence cannot answer all the questions that arise around equality in Internet governance, it will allow me to formulate a research agenda to advance the cause of anchoring equality in international Internet law. The article therefore proceeds as follows: It briefly describes the principle of equality in international law (II.) as well as the status quo of equality in cyberspace by identifying three dimensions of networked inequality (III.). It then analyses a selection of key documents of Internet governance from an equality perspective (IV.). This section undertakes a content analysis of those documents while paying particular attention to the three dimensions of networked inequality as described in section III. The goal of this section is to come to preliminary conclusions, and to lay a foundation for future research, which will then be outlined at the end of this contribution. The following documents will be examined: The bylaws of the Internet Corporation for Assigned Names and Numbers (ICANN) (IV. 1.), the outcome documents of the two World Summits on the Information Society (WSIS) (IV. 2.), the multistakeholder statement of the NETmundial conference (IV. 3.) and the Proposal for an European Union (EU) Digital

⁹ See, inter alia, Jonathan Andrew and Frédéric Bernard (eds), *Human Rights Responsibilities in the Digital Age: States, Companies, and Individuals* (London: Hart Publishing 2021); Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge: Cambridge University Press 2018); Meryem Marzouki and Rikke Frank Joergensen, 'A Human Rights Assessment of the World Summit on the Information Society', *Information Technologies and International Development* 1 (2005), 86-88; Milton Mueller and Farzaneh Badii, 'Requiem for a Dream: On Advancing Human Rights via Internet Architecture', *Policy & Internet* 11 (2019), 61-83; Anne Peacock, *Human Rights and the Digital Divide* (London: Routledge 2019); Susan Perry and Claudia Roda, *Human Rights and Digital Technology: Digital Tightrope* (London: Palgrave Macmillan 2017); Ben Wagner, Matthias C. Kettmann and Kilian Vieth (eds), *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations* (Cheltenham: Edward Elgar Publishing 2019); Monika Zalnieriute and Stefania Milan, 'Internet Architecture and Human Rights: Beyond the Human Rights Gap', *Policy & Internet* 11 (2019), 6-15.

¹⁰ ECtHR, *Delfi AS v. Estonia*, judgement of 16 June 2015, no. 64569/09; *Beizaras and Levickas v. Lithuania*, judgement of 14 January 2020, no. 41288/15.

Services Act (IV. 4.). The actors examined are private regulators (ICANN), an intergovernmental forum (WSIS), an international bottom-up multistakeholder initiative (NETmundial), and a supranational organisation (European Union) and thus represent the variety of actors active in Internet governance. This part will reveal that there is currently no consistent or comprehensive approach to addressing equality issues in Internet governance and that more research will be needed to better understand the topic and to embed equality considerations in Internet governance. By way of a conclusion, the chapter draws a research agenda that should inspire and help guide future enquiries (V.).

II. The Principle of Equality and Its Foundations in International Law

The principle of equality speaks to our intuitive understanding of fairness and justice: Treating likes unlike or treating unlikes alike is perceived as unjust or unfair.¹¹ Equality has a centuries-old intellectual tradition.¹² The classical principle of equality goes back to Aristotle:¹³ that what is equal should be treated equally and what is unequal should be treated unequally. In the Enlightenment, the idea of equality achieved a renaissance in the struggle against feudal social relations and was seen as an important foundation of the modern social order as well as of democracy. Equality is also an important element of liberal state theories.¹⁴ In this understanding, equal treatment is not only a fundamental right, but also a basic principle of every democratic constitutional state, which must treat all of its citizens equally.

However, equality in and of itself is an ‘empty idea’.¹⁵ What equality means exactly, who is to be treated equally with whom, and which situations,

¹¹ Kristin Henrard, ‘Equality of Individuals’ in: Rüdiger Wolfrum (ed.), *MPEPIL* (online edn. Oxford: Oxford University Press 2008); John McMillan and Jeanne Snelling, ‘Equality: Old Debates, New Technologies’ in: Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* 1 (2017), 73.

¹² Jarlath Clifford, ‘Equality’ in: Dinah Shelton (ed.), *The Oxford Handbook of International Human Rights Law* (2013), 422.

¹³ Aristotle, *Nicomachean Ethics* (Cambridge: Cambridge University Press 2000), Book V3, paras 1131a-b.

¹⁴ Daniel Moeckli, ‘Equality and Non-Discrimination’ in: Daniel Moeckli, Sangeeta Shah and Sandesh Sivakumaran (eds), *International Human Rights Law* (2nd edn, Oxford: Oxford University Press 2018), 148.

¹⁵ Peter Westen, ‘The Empty Idea of Equality’, *Harv. L. Rev.* 95 (1982), 537-596; Kent Greenawalt, ‘How Empty Is the Idea of Equality?’, *Colum. L. Rev.* 83 (1983), 1167-1185; Moeckli (n. 14), 149.

circumstances, characteristics are considered equal or comparable, does not result from the philosophical foundations of equality itself, but awaits to be filled with normative content.¹⁶ This, in turn, is a political question that often depends on the prevailing views of a time. Aristotle, for example, could still assume the equality of only the male active citizens of Athens. The Enlightenment thinker John Locke also primarily had male equality in mind,¹⁷ which per se excluded all women as well as the unfree (slaves) from the claim to equality.¹⁸ Today, equality on the basis of immutable characteristics such as gender, race, and ethnic origin, as well as religion and other characteristics, is undisputed in international law.¹⁹

While equality as the ultimate social ideal is widely accepted, the way of achieving equality is not determined by the mere ideal of equality itself. Essentially, two different types of equality can be distinguished, namely formal and substantive equality.²⁰ The concept of *formal equality* requires equal treatment. This is, to a certain extent, the most intuitive concept of equality.²¹ Formal equality is based on a procedural understanding of equality: in a concrete case of application, comparable situations must not be treated unequally.²² Within the concept of formal equality, a distinction is made between direct and indirect unequal treatment: While direct unequal treatment is linked to a protected characteristic and thus creates a clearly recognisable inequality, indirect unequal treatment happens when a seemingly neutral criterion, rule, or practice has considerably more negative consequences on certain protected groups than on others.²³ Formal equality obliges the state, legally speaking, to an abstention: it must refrain from any unequal treatment, whether direct or indirect.

The second concept of equality is the so-called *substantive equality*. This concept looks not at the process, but at the result. Only when a state of substantive equality (for example, equal number of female and male representatives, equal income for work of equal value, etc.) has been reached, is

¹⁶ Clifford (n. 12), 424.

¹⁷ John Locke, *Two Treatises of Government* (2nd ed., 2003), second treatise, para. 2.

¹⁸ Sandra Fredman, *Discrimination Law* (2nd edn, Oxford: Oxford University Press 2011), 4.

¹⁹ Moeckli (n. 14), 154.

²⁰ See, for example, Fredman (n. 18), 4; Henrard (n. 11); Moeckli (n. 14), 149; Judith Squires, 'Equality and Difference' in: John S. Dryzek, Bonnie Honig and Anne Phillips (eds), *The Oxford Handbook of Political Theory* (Oxford: Oxford University Press 2009), 471.

²¹ Fredman (n. 18), 8; Moeckli (n. 14), 157.

²² Fredman (n. 18), 8 ('Treating likes alike'); Henrard (n. 11), 601; Moeckli (n. 14), 149.

²³ Moeckli (n. 14), 156; See also the legal definition of indirect discrimination in the EU equality directives: Art. 2(2) Directive 2000/43/EC; Art. 2(2) Directive 2000/78/EC; Art. 2(1) Directive 2006/54/EC.

the ideal of equality achieved.²⁴ Substantive equality deviates from the procedural understanding of equality in the sense of equal treatment in that it allows, for example, for preferential treatment of members of certain groups in order to compensate for the effects of past unequal treatment and to achieve substantive equality. Substantive equality requires the State not only to abstain, as in the case of formal equality, but under certain circumstances also to take action, and therefore constitutes a positive obligation to take measures.

Unequal treatment that is linked to a characteristic protected under Human Rights Law, namely gender, race or ethnicity, disability, religion, and, at least in the European context, age, and sexual orientation, is particularly reprehensible and can only be justified legally if certain specific conditions are met. As a rule, unequal treatment based on one of these characteristics can only be justified if it pursues a particularly important, legitimate aim and if the measure is proportionate.²⁵

In international law, equality is enshrined in all universal Human Rights treaties and can be considered a structural principle of International Human Rights Law.²⁶ The Universal Declaration of Human Rights²⁷ (Articles 1 and 2), the International Covenants on Civil and Political Rights²⁸ (Articles 2(1), 3 and 26) and on Economic, Social and Cultural Rights²⁹ (Articles 2(2) and 3), as

²⁴ Catherine Barnard and Bob Hepple, 'Substantive Equality', CLJ 59 (2000), 562-585; Sandra Fredman, 'Changing the Norm: Positive Duties in Equal Treatment Legislation', *Maasticht J. Eur. & Comp. L.* 12 (2005), 369-397; Sandra Fredman (n. 18), 14; Sandra Fredman, 'Emerging from the Shadows: Substantive Equality and Article 14 of the European Convention on Human Rights', *HRLR* 16 (2016), 273-301; Sandra Fredman, 'Substantive Equality Revisited', *I CON* 14 (2016), 712-738; Catharine A. MacKinnon, 'Substantive Equality Revisited: A Reply to Sandra Fredman', *I CON* 14 (2016), 739-746; Moeckli (n. 14), 150.

²⁵ See generally, Human Rights Committee, General Comment No. 18 (1989), para. 13; Human Rights Committee, *Gillot v. France*, A/57/40 (15 July 2002), para. 13.2; ECtHR, *Case Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium* (Belgian Linguistics Case) (No 2), judgement of 23 July 1968, 1 EHRR 252, para. 10; CERD, UN Committee on the Elimination of Racial Discrimination: Concluding Observations, Australia, CERD/C/AUS/CO/14 (14 April 2005), para. 24; CESCR, General Comment No. 20: Non-Discrimination in Economic, Social and Cultural Rights (Art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights), E/C.12/GC/20, para. 13; Moeckli (n. 14), 158.

²⁶ Clifford (n. 12), 430.

²⁷ UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

²⁸ UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171 (ICCPR); see Human Rights Committee, General Comment No. 18 (1989).

²⁹ UN General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, 993 UNTS 3 (ICESCR), see UN CESCR General Comment No. 20 (n. 25).

well as all regional Human Rights treaties,³⁰ acknowledge the principle of equality and the prohibition of discrimination that flows from this principle. On a global level, the Convention against Racial Discrimination,³¹ the Convention on the Abolition of all Forms of Discrimination against Women,³² the Convention on the Rights of the Child,³³ and the Convention on the Rights of Persons with Disabilities³⁴ contain group-specific provisions that aim to achieve equality.

While the principle of equality and its corresponding prohibition of discrimination under international law are primarily directed at the State in the form of a negative obligation, is not limited to this. Rather, the prohibition of discrimination and the principle of equality contain both an obligation to protect as well as an obligation to take measures to implement the principle of equality in the private sphere as well, and thus to strive for substantive equality. While there is no obligation under International Human Rights Law for private individuals (e.g. businesses or self-regulating actors) to treat others equally or to strive for substantive equality, there is an obligation on States to seek the realisation of this principle by regulating areas that are susceptible to inequality without State intervention.³⁵ It is generally accepted under Human Rights Law that States must, under their obligation to protect, intervene and impose requirements for compliance with this principle if it is determined that self-regulation is not sufficient to prevent breaches of International Human Rights Standards.³⁶ Since Internet governance is to a large extent dominated and regulated by private actors, this obligation to protect becomes particularly relevant. So far, however, there is only very limited

³⁰ Such as the European Convention on Human Rights of 4 November 1950, 213 UNTS 221, ETs No. 5 in its Articles 14 ECHR and 1 of Additional Protocol No. 12, and the Inter-American Convention on Human Rights of 22 November 1969, 1144 UNTS 123, OAS TS No. 36 in its Articles 1(1) and 24. See Caballero Ochoa and Aguilar Contreras, 'New Trends on the Right to Non-Discrimination in the Inter-American System of Human Rights', *Inter-American & European Human Rights Journal* 8 (2016), 80-94; Oddný Mjöll Arnardóttir, *Equality and Non-Discrimination under the European Convention on Human Rights* (The Hague: Martinus Nijhoff 2003).

³¹ International Convention on the Elimination of All Forms of Racial Discrimination of 7 March 1965, 660 UNTS 13 (CERD).

³² Convention on the Elimination of All Forms of Discrimination against Women of 18 December 1979, 1249 UNTS 13 (CEDAW).

³³ Convention on the Rights of the Child of 20 November 1989, 1577 UNTS 3 (CRC).

³⁴ Convention on the Rights of Persons with Disabilities of 13 December 2006, 2515 UNTS 3.

³⁵ Kälén and Künzli (n. 1), 343. See CESCR, General Comments Nos 16 of 11 August 2005, para. 18, and 20 of 2 July 2009, para. 39, as well as HRC, General Comments Nos 28 of 29 March 2000, paras 3 ff, and 18 of 10 November 1989, para. 5.

³⁶ HRC, General Comment No. 31 of 26 May 2004, para. 8.

practice by the international monitoring mechanisms on questions of equality in cyberspace.³⁷

III. Networked Inequality

In the following paragraphs, I will take a closer look at the status of equality in cyberspace and in Internet governance in particular. Like technology in general, the Internet is often seen as ‘neutral’ and machines, programs, and code are often perceived to be free from human feelings and distortions. When looking at cyberspace through an equality lens however, one rapidly comes to the conclusion that cyberspace is not as ‘objective’ and ‘neutral’ as it is often perceived. For the sake of analysis, I will look at three³⁸ dimensions of inequality in cyberspace, namely design of, access to, and enjoyment of the Internet. These three dimensions do not exist in isolation from each other. They are interlinked, mutually reinforcing, and influencing each other.

Firstly, the *design and administration of the technologies necessary to keep the Internet operational* is characterised by a significant underrepresentation of women and minorities amongst developers,³⁹ which ultimately leads to an ‘inherent masculinity’⁴⁰ of the Internet infrastructure. It is no secret that the

³⁷ The only judgement so far known is of the European Court of Human Rights, ECtHR, *Buturugă v. Romania*, judgement of 10 February 2020, no. 56867/15, where the Court pointed out that cyberbullying was currently recognised as an aspect of violence against women and girls, and that it could take on a variety of forms, including cyberbreaches of privacy, intrusion into the victim’s computer and the capture, sharing and manipulation of data and images, including private data. The Court recognised a violation of Art. 3 i. c. w. Art. 14 ECHR.

³⁸ DiMaggio, Hargittai, Celeste and Shafer (n. 7), distinguish between five aspects of inequality related to information and communication technologies: (1) the quality of hardware, software, and network connection; (2) autonomy of use; (3) skill; (4) availability of social support; and (5) extent and quality of use. Hargittai and Hsieh (n. 7), differentiate between (1) access and (2) skills and uses.

³⁹ See, for example, already the ‘Pioneers Gallery’ of the World Wide Web, available at <<http://www.wiwiw.org/>>. Ironically, it was a woman who invented the first programming language (Ada Lovelace), and the first ‘computers’ were mainly women. In fact, in the 1940s to the 1960s, programming was seen as a typical women’s job: Programming was seen as similar to following a recipe or putting together a menu. In addition, programming did not require much physical strength, which was also seen as a clear advantage for women. Only in the 1970s did programming become a typically male profession, which went hand in hand with an increased reputation and higher salaries. See Isabelle Collet, *L’informatique a-t-Elle Un Sexe? Hackers, Mythes et Réalités* (Paris: Editions L’Harmattan 2006); Isabelle Collet, ‘Effet de genre: le paradoxe des études d’informatique’, *Tic & Société* 5 (2011), 12–34.

⁴⁰ Some theorists argue that male values have been institutionalised in the technology through its creators, embedding a cultural association with masculine identity in the technology itself: Cheri Kramarae (ed.), *Technology and Women’s Voices: Keeping in Touch* (London: Routledge 1988); Wajcman (n. 5). In the terminology of Green, Owen, and Pain (1993), the technology may be ‘gendered by design’, see Eileen Green, Jenny Owen and Den Pain (eds), *Gendered by Design? Information Technology and Office Systems* (London: Taylor & Francis Ltd. 1993).

profession of computer science, computer engineers, programming, is to a large extent a 'male profession', despite ongoing efforts by governments and companies, for example, to inspire and promote women for these professions.⁴¹ Also, women are less represented in decision-making processes on Internet governance.⁴² This might cause worries from an equality perspective, since code itself can be seen as a form of law,⁴³ leading to potentially discriminatory outcomes such as search engines reinforcing racism.⁴⁴ Choices made about technologies of Internet governance do not merely depend upon technical questions, but on balancing the interests and values of the social groups involved in these choices.⁴⁵ This underrepresentation of certain groups and overrepresentation of others might also have implications for the *governance* of the Internet. The multistakeholder approach,⁴⁶ as well as the bottom-up approach, which are supposed to stand for greater inclusion of all those affected by Internet regulation, come to a limit if those working in this area all belong to the same group.

Secondly, *access to Internet* is distributed unequally along lines of race, class, age, and gender. Not only does access to Internet and information depend on (Internet) literacy, but also on the place of residence (including country of residence) and on economic resources, which are themselves distributed unequally amongst the abovementioned lines. Essentially, the 'digital divide' mirrors existing power structures and lines of inequality in the offline world.⁴⁷ This 'digital divide', and in particular the 'digital gender divide', has been known for many decades now. However, it has been mostly the subject of sociological inquiry.⁴⁸ Legal analyses of this phenomenon are largely lacking.⁴⁹

⁴¹ See, for example, Barker and Jurasz, *Online Violence* (n. 8), 55. To the evolution from a female to a male profession see Collet (n. 39).

⁴² Association for Progressive Communications, *Critically Absent: Women's Rights in Internet Governance* (2012), available at <<https://internetdemocracy.in/>>; Jensen (n. 5).

⁴³ Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999).

⁴⁴ Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press 2018).

⁴⁵ Laura DeNardis, 'Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance', *Information, Communication & Society* 15 (2012), 720-738 (722); Andrew Feenberg, *Questioning Technology* (London: Routledge 1999); Helen Nissenbaum, 'How Computer Systems Embody Values', *Computer* 34 (2001), 118-120.

⁴⁶ Christine Kaufmann, 'Multistakeholder Participation in Cyberspace', *SRIEL* 26 (2016), 217-234.

⁴⁷ Wessels (n. 7).

⁴⁸ See, for example, Norris (n. 7); van Dijk (n. 7); Jan A. G. M. van Dijk, 'A Theory of the Digital Divide' in: Massimo Ragnedda and Glenn W. Muschert (eds), *The Digital Divide: The Internet and Social Inequality in International Perspective* (London: Routledge 2013), 29-51; OECD (n.7); Wessels (n. 7).

⁴⁹ One notable exception is: Peacock (n. 9).

Finally, also the possibilities for *enjoyment of the Internet* are unequally distributed. Women, queer persons, Persons of Colour (PoC), or religious minorities are more often subject to forms of cyber violence such as cyber-harassment or cyberstalking, image-based sexual abuse (also referred to as ‘revenge pornography’) and other forms of technology-mediated harm.⁵⁰ Studies show that the majority of those particularly affected by digital violence are of female self-assignment.⁵¹ Online violence, on one hand, negatively affects the enjoyment of other rights of the victims.⁵² For example, hate speech or threats have a chilling effect on the exercise of the right to freedom of expression or participation in democratic discourse (e.g. in social media). Online stalking affects the victims’ right to privacy. On the other hand, since those crimes happen more often to certain groups, they also amount to discriminatory violation of other rights, such as the right to privacy and the right to freedom of expression. While those acts are typically committed by private actors and therefore do not constitute direct violations of Human Rights guarantees, a State is certainly in violation of his obligation to protect if no preventive and/or repressive measures are taken against those acts.

These dimensions of inequality influence each other. For example, a causal relationship is discernible between the underrepresentation of women and Persons of Color in the process of designing Internet technology and those groups’ difficulties in the enjoyment of cyberspace, due to, for example, a lack of technological remedies to discriminatory online harm.

In sum, we can observe that the picture about the Internet’s role for equality seems to be more complicated than was imagined by the ‘inventors’ of the Internet, who heralded it as the great potential equalizer⁵³ and aspired to create an open, transparent, and democratic space. While early proponents of cyberfeminism such as Donna Haraway believed that society would become more equal by improving technology,⁵⁴ a look at the status quo is rather disenchanting and leads the observer to feel that cyberspace might be even less egalitarian than the offline world.

⁵⁰ Barker and Jurasz, *Online Violence* (n. 8).

⁵¹ Maeve Duggan, *Online Harassment 2017* (Washington D.C.: Pew Research Center, July 2017). An EU-wide study came to similar conclusions, see Amnesty International, *Amnesty Reveals Alarming Impact of Online Abuse against Women*, 20. November 2017, <<https://www.amnesty.org/>>.

⁵² Barker and Jurasz, *Online Violence* (n. 8), 55. The European Commission has recently acknowledged that online violence against women acts as a barrier to women’s participation in public life, see European Commission, ‘A Union of Equality: Gender Equality Strategy 2020-2025’, COM(2020) 152 final, 5 March 2020, 5.

⁵³ Hargittai and Hsieh (n. 7).

⁵⁴ Haraway (n. 2).

IV. Tracking Down Equality in Internet Governance

Having established the fundamental nature of equality in the ‘offline world’ and in international law entails (section II.) as well as the existing inequalities in cyberspace (section III.), the coming section will analyse whether this situation is remedied in existing documents of Internet Governance. It therefore undertakes a content analysis of key documents of Internet governance from a variety of actors. The analysis pays particular attention to the three dimensions of networked inequality as described in section III. The goal of this section is explanatory: It will allow for an overview as well as preliminary conclusions, and thereby laying the foundations for future research. The following documents will be examined: The bylaws of the Internet Corporation for Assigned Names and Numbers ICANN (IV. 1.), the outcome documents of the two World Summits on the Information Society WSIS (IV. 2.), the multistakeholder statement of the NETmundial conference (IV. 3.), and the Proposal for an EU Digital Services Act (IV. 4.). While there are many more soft law⁵⁵ and hard law⁵⁶ documents that await to be analysed from an equality perspective, the documents examined here have been chosen for analysis because they represent regulations from a variety of actors (a private regulator, an intergovernmental forum, an international bottom-up multistakeholder initiative, and a supranational organisation) and therefore also exemplify the fragmented and multipolar landscape of Internet governance.

1. ICANN Bylaws

ICANN, the Internet Corporation for Assigned Names and Numbers, is a private non-profit organisation under Californian law and coordinates the allocation of unique names and addresses on the Internet (namely the coordination of the Domain Name System and the allocation of IP addresses). This makes ICANN one of the most important players when it comes to regulating the infrastructure of the Internet. The role of Internet infrastructure for

⁵⁵ This includes the various outcome documents of the annual Internet Governance Fora, further Internet-related regulations and directives of the European Union, recommendations and statements of the Council of Europe and the OECD, laws at the national level, basic documents of bottom-up initiatives such as the Internet Society and the Internet Engineering Task Force, statements and reports of the various organs and rapporteurs of the United Nations, and many more.

⁵⁶ Especially the Council of Europe Convention on Cybercrime of 23 November 2001, CETS No. 185.

fundamental rights is increasingly appreciated, recognising that arrangements of technical architecture are inherently arrangements of power.⁵⁷ The ICANN Bylaws, which could be described as the ICANN's 'constitution', have been revised and replaced several dozens of times.⁵⁸ The current version dates from November 2019.⁵⁹

Right at the very beginning of the Bylaws, ICANN commits to its 'Core Values', which include that ICANN carries out its activities 'in conformity with relevant principles of international law and international conventions and applicable local law [...]'.⁶⁰ Even though the Bylaws do not specify the 'relevant principles' that should be observed, it can be assumed that the principle of equality, due to its structural nature,⁶¹ would also form part of this list. The relevant principles of international law and conventions should also include the principle of equality and non-discrimination under international law. The non-discriminatory application of ICANN's policies is also mentioned as a special obligation under this Bylaw: 'Make decisions by applying documented policies consistently, neutrally, objectively, and fairly, without singling out any particular party for discriminatory treatment (i. e. making an unjustified prejudicial distinction between or among different parties).'⁶² ICANN thus commits itself to a non-discriminatory application of its policies in practice. However, this Bylaw is formulated in a very general and imprecise manner; one does not know, for example, which types of distinctions are inadmissible and which ones might be required to avoid indirect discrimination.

When it comes to the composition of its Board of Directors, the Bylaws place great emphasis on diversity. According to Bylaw 7.2 (b), 'the Nominating Committee shall ensure that the Board is composed of Directors who, in the aggregate, display diversity in geography, culture, skills, experience, and perspective'. As discussed above in section III., one of the causes and also one of the dimensions of inequality in cyberspace is that Internet policy makers are often male and white. Bylaw 7.2 (b) attempts to address this through an explicit commitment to diversity in the composition of the Board of Directors. However, 'classic' discrimination categories recognised under International Human Rights Law such as gender, race, religion, age, or sexual orientation are not included, and instead emphasis is placed on geographic

⁵⁷ DeNardis (n. 45), 721; Zalnieriute and Milan (n. 9), 6; for a more critical account on the linking of human rights and internet architecture see Mueller and Badiei (n. 9), 61.

⁵⁸ See the ICANN Bylaws archive: <<https://www.icann.org/>>.

⁵⁹ Available at <<https://www.icann.org/>>.

⁶⁰ ICANN Bylaw 1.2 (a).

⁶¹ See above, section II.

⁶² ICANN Bylaw 1.2 (a)(v).

and cultural diversity as well as skills, experience and perspectives. Of course, persons with different gender, religion, race, age, or sexual orientation also have different ‘experiences’ or ‘perspectives’, but this interpretation of the Bylaw is not the only one possible. ‘Experience and perspective’ can also simply be interpreted as covering different professional backgrounds, which could still lead to a homogenous composition of the Board, since, as has been explained in section III. above, white men are overrepresented in most fields of tech and Internet governance.

Finally, the topic of Human Rights (and thus, implicitly, also equality) is mirrored in the recently added ‘Human Rights Bylaw’ of 2019. According to this provision, one of ICANN’s Core Values is the ‘respecting [of] internationally recognised human rights as required by applicable law’.⁶³ However, the Bylaws directly limit this commitment by specifying that ‘This Core Value does not create, and shall not be interpreted to create, any obligation on ICANN outside its Mission, or beyond obligations found in applicable law. This Core Value does not obligate ICANN to enforce its Human Rights obligations, or the Human Rights obligations of other parties, against other parties.’ Furthermore, Bylaw 27.2 (b) states that the Human Rights Bylaw cannot be invoked in the reconsideration process (Section IV. 2.), or in the independent review process (Section IV. 3.) and is therefore not an enforceable obligation in internal complaints procedures, which somehow contradicts ICANN’s above-mentioned commitment to non-discriminatory application of its policies. The idea that ICANN would commit itself to strong Human Rights obligations, particularly in the field of equality, is thus very quickly dashed here.⁶⁴ Rather, equality seems to be conceptualised as a value without further operationalisation for daily practice.

2. WSIS Outcome Documents

The World Summit on the Information Society (WSIS) was a United Nations-sponsored world summit on information and communications that was organised by the International Telecommunication Union (ITU) and consisted of two parts. The first part took place in Geneva (Switzerland) from 10 to 12 December 2003 and had about 12,000 participants. The second part,

⁶³ ICANN Bylaw 1.2 (b)(viii).

⁶⁴ See also the criticism of the ‘Human Rights Bylaw’ by Monika Zalnieriute, ‘From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Example of Internet Governance and ICANN’, *Yale Journal of Law & Technology* 21 (2019), 278-336 and Monika Zalnieriute, ‘Human Rights Rhetoric in Global Internet Governance: New ICANN Bylaw on Human Rights’, *Harvard Business Law Review* 10 (2020), 1-40.

held in Tunis (Tunisia) from 16 to 18 November 2005, was attended by about 17,000 delegates from 175 countries.⁶⁵

The Outcome Documents of these two summits have no legally binding force, but they express the common views of the participants to the Summits and can therefore be seen as international soft law and provide insights into the role of equality in Internet governance. They consist of the Geneva Declaration of Principles, the Geneva Plan of Action, the Tunis Commitment and the Tunis Agenda for the Information Society.⁶⁶

The first principle of the Geneva Declaration is called 'Our Common Vision of the Information Society'. There, the representatives express their 'common desire and commitment to build a people-centred, inclusive, and development-oriented Information Society, where everyone can create, access, utilise, and share information and knowledge, enabling individuals, communities, and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.' One of the key principles of this 'Information Society for All' is 'Access to information and Knowledge', which also includes universal access to the Internet,⁶⁷ and therefore one of the above-mentioned dimensions of inequality in cyberspace. However, the Geneva Declaration only refers to universal access in relation to geographical location, so that no region or country of the world should be cut off from access to the Internet, while the 'digital gender divide' is not addressed. Principle 8 calls for 'cultural diversity and identity, linguistic diversity and local content'.⁶⁸ Here, too, it is not a diversity of identities that is meant, but rather geographical, cultural, and linguistic diversity.

Principle 6 calls for an 'Enabling Environment' and states that '[t]he rule of law [...] is essential for building a people-centred Information Society. Governments should intervene, as appropriate, to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT [Information and Communication Technology] infrastructure and applications, to maximise economic and social benefits, and to serve national priorities'.⁶⁹ From an equality point of view (and a Human Rights perspective in general) it seems striking that no intervention by governments is foreseen regarding the compliance with Human Rights, especially the realisation of the principle of equality.

⁶⁵ See <<https://www.itu.int/>>.

⁶⁶ The WSIS Outcome Documents are available at <<https://www.itu.int/>>.

⁶⁷ Geneva Declaration of Principles (n. 66), No. 28.

⁶⁸ Geneva Declaration of Principles (n. 66), Nos 52-54.

⁶⁹ Geneva Declaration of Principles (n. 66), No. 39.

Human Rights are only mentioned under the title ‘Ethical dimensions of the Information Society’ (principle 10).⁷⁰ According to this principle, the Information Society should ‘respect peace and uphold the fundamental values of freedom, equality, solidarity, tolerance, shared responsibility, and respect for nature.’⁷¹ Equality is thus conceptualised not as a right but as a value, in a line with other rather open concepts such as solidarity, tolerance, responsibility and the respect for nature. If one continues reading, one also sees that only personal privacy, and the right to freedom of thought, conscience, and religion are mentioned as Human Rights to be protected: ‘The use of ICTs and content creation should respect Human Rights and fundamental freedoms of others, including personal privacy, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments.’⁷² Equality is not mentioned as a Human Right worth protecting in cyberspace.

At least, principle 10 addresses the need to combat discriminatory content online: ‘All actors in the Information Society should take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.’⁷³ However, important forms of discriminatory online harm are not mentioned, especially transphobia, religious intolerance, and online violence against women, which can lead to the creation of a ‘hierarchy of harms’.⁷⁴

A few additional issues were raised in the Tunis Commitment, which, for example, explicitly recognises the existence of a digital gender divide:⁷⁵ ‘We reaffirm our commitment to women’s empowerment and to a gender equality perspective, so that we can overcome this divide. We further acknowledge that the full participation of women in the Information Society is necessary to ensure the inclusiveness and respect for Human Rights within the Information Society. We encourage all stakeholders to support women’s participation in decision-making processes and to contribute to shaping all spheres of the Information Society at international, regional and national levels.’⁷⁶ The

⁷⁰ See, more generally, Marzouki and Joergensen (n. 9).

⁷¹ Geneva Declaration of Principles (n. 66), No. 56.

⁷² Geneva Declaration of Principles (n. 66), No. 58.

⁷³ Geneva Declaration of Principles (n. 66), No. 59.

⁷⁴ This term was coined, with reference to European (non-)regulation of online harm, by Barker and Jurasz, *Online Violence* (n. 8), 57.

⁷⁵ Tunis Commitment (n. 66), No. 23.

⁷⁶ Tunis Commitment (n. 66), No. 23.

equality dimensions of design and of access to Internet are thus implicitly addressed in the Tunis Commitment.

To conclude, while some sensitivity to equality online can be identified in the WSIS outcome documents, it can be observed that the full dimension of inequality in cyberspace was not addressed by the drafters of those documents. Equality seems to be understood as a value rather than an enforceable Human Right.

3. NETmundial

The NETmundial initiative was a transnational platform that followed the multistakeholder approach and aimed to provide a forum for discussion on Internet regulation.⁷⁷ The first and, so far only meeting took place in São Paulo in April 2014 and gathered a total of 1,480 stakeholders from 97 countries, representing governments, business, and civil society. The key outcome was the non-binding Multistakeholder Statement, which sets out a series of principles for Internet governance and outlines a roadmap for the future of Internet regulation. The NETmundial initiative was not without controversy and, due to different factors, collapsed not long after its taking place. Nevertheless, and despite its legally non-binding nature, the Multistakeholder Statement remains an important document for Internet governance and for analysing the place of equality in it.

The Multistakeholder Statement lists ‘Human Rights and Shared Values’ as the first in a series of Internet Governance Principles. In remarkable contrast to the other documents examined so far, the statement formulates that ‘[r]ights that people have offline must also be protected online, in accordance with international Human Rights legal obligations, including the International Covenants on Civil and Political Rights and Economic, Social and Cultural Rights, and the Convention on the Rights of Persons with Disabilities’. This corresponds to the principle of ‘what applies offline, also applies online’ developed by the United Nations Human Rights Council.⁷⁸ However, as promising as the NETmundial Multistakeholder Statement starts, as disappointing it continues. Reading on, the Statement only mentions the ‘traditional’ rights that are usually invoked when talking about matters online: Freedom of expression, freedom of association, privacy, freedom of information, as well as accessibility (for persons with disabilities), and a right to development, but it does not mention equality.⁷⁹

⁷⁷ <<https://netmundial.br/>>.

⁷⁸ UNHRC Res 20/8 of 5 July 2012.

⁷⁹ NETmundial Multistakeholder Statement available at <<https://netmundial.br/>>, 4.

The Multistakeholder Statement goes on to enumerate the so-called ‘Internet Governance Process Principles’. The process of Internet governance shall be ‘inclusive and equitable’, among other characteristics such as multistakeholder, open, participative, consensus driven, transparent, accountable, distributed, collaborative, and enabling meaningful participation. This could be understood as addressing the problem of under-representation of certain groups (see above, section III.) in the design of Internet governance. However, this principle is formulated so vaguely that such a conclusion is not necessarily compelling and is probably more wishful thinking by the author. In any case it could also be interpreted differently, since it is only mentioned that ‘Internet governance institutions and processes should be inclusive and open to all interested stakeholders. Processes, including decision making, should be bottom-up, enabling the full involvement of all stakeholders, in a way that does not disadvantage any category of stakeholder.’⁸⁰

Equality is also mentioned in the ‘Roadmap for the future evolution of the Internet Governance’. As one of the ‘Issues that deserve attention of all stakeholders in the future evolution of Internet governance’, the statement also mentions that ‘[t]here should be meaningful participation by all interested parties in Internet governance discussions and decision-making, with attention to geographic, stakeholder and gender balance in order to avoid asymmetries’.

Apart from this, however, equality is not present in the NETmundial Multistakeholder Statement, and the question of cyberviolence, for example, is not addressed at all. We can conclude that, although the Multistakeholder Statement appears advanced compared to the other documents analysed so far in terms of mentioning Human Rights and equality or non-discrimination, the overall result is rather dire as well.

4. EU Digital Services Act Proposal

The European Union is increasingly becoming an important player when it comes to regulating the Internet. Of all the actors analysed here, it is the only one that has a state-like character and can issue legally binding and enforceable regulations. I will analyse here the proposal for a ‘Digital Services Act’,⁸¹ which was presented by the European Commission in December 2020

⁸⁰ NETmundial Multistakeholder Statement (n. 79), 6.

⁸¹ European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM (2020) 825 final.

after a long period of drafting and consultations. At the time of writing, the package has not yet been discussed and adopted by Parliament and Council and it can be expected that the proposal will still undergo considerable amendments. Nevertheless, it is not too early to examine the proposal from an equality perspective.

Already in its Explanatory Memorandum, the proposal promises to be ‘fully consistent [with] and further supports equality strategies adopted by the Commission in the context of the Union of Equality’.⁸² However, the Explanatory Memorandum does not enter into more detail, so that this sentence sounds more like an empty phrase that needed to be included for formal reasons in order to show that the proposal is in line with ‘other Union policies’. At least, the Explanatory Memorandum accepts that ‘specific groups or persons may be vulnerable or disadvantaged in their use of online services because of their gender, race or ethnic origin, religion or belief, disability, age, or sexual orientation. They can be disproportionately affected by restrictions and removal measures following from (unconscious or conscious) biases potentially embedded in the notification systems by users and third parties, as well as replicated in automated content moderation tools used by platforms.’⁸³ The Memorandum then promises that ‘The proposal will mitigate discriminatory risks, particularly for those groups or persons and will contribute to the protection of the rights of the child and the right to human dignity online.’⁸⁴ The proposal thus takes account of the ‘enjoyment’ dimension of networked inequality explained in section III.

The recitals of the proposed regulation on a Digital Services Act contain equality considerations in several instances: Recital 3 combines the duty of responsible and diligent behaviour by providers of intermediary services with the right of Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union, in particular the freedom of expression and information and the freedom to conduct a business, and the right to non-discrimination.⁸⁵ Recital 12 clarifies that the concept of ‘illegal content’ should be defined broadly and should also cover content such as illegal hate speech or terrorist content and unlawful discriminatory content, unlawful non-consensual sharing of private images or online stalking. This partly addresses the critique of a ‘hierarchy of harms’ mentioned above.⁸⁶ Recital 41 states that ‘notice and action mecha-

⁸² European Commission, DSA Proposal (n. 81), 6.

⁸³ European Commission, DSA Proposal (n. 81), 12.

⁸⁴ European Commission, DSA Proposal (n. 81), 12.

⁸⁵ European Commission, DSA Proposal (n. 81), Recital 3.

⁸⁶ See above, IV.2., and Barker and Jurasz, Online Violence (n. 8), 57.

nisms',⁸⁷ should have rules that provide for robust safeguards to protect the rights and legitimate interests of all affected parties, including the right to non-discrimination as well as the right to non-discrimination of parties affected by illegal content. Recitals 52 to 63 are remarkable in that they mention the potential dangers of online advertisement, and in particular also recognises that online advertisement can contribute to significant risks, including the discriminatory display of advertising with an impact on the equal treatment and opportunities of citizens. This topic has recently become the subject of academic scrutiny⁸⁸ and it is remarkable that the EU is taking it up already, including the subject of online behavioural advertising which poses risks of discrimination. And finally, what is notable is that Recital 91 states that the European Board for Digital Services should not only be allowed to cooperate with Union bodies in the field of data protection, electronic communications, audio-visual services, and others, but also Union bodies in the fields of 'equality, including equality between women and men, and non-discrimination'. Such cooperation could ensure that equality considerations are taken seriously when deciding on matters of Internet governance within the European Union.

The attention devoted to equality in the Explanatory Memorandum and the Recitals is remarkable, particularly in comparison to the other documents analysed here. However, the Recitals themselves are not binding. They mainly serve to clarify the content and meaning of the substantive articles. Therefore, the more concrete and more important provisions are to be found in the articles of the proposed regulation. These, on the other hand, are rather thin as far as equality and non-discrimination are concerned. In that sense, equality only figures as one of the additional obligations for very large online platforms to manage systemic risks, in the sense that they have to conduct a risk assessment (Article 26), in which they identify, analyse, and assess at least once a year any significant systemic risks stemming from the functioning and use made of their services in the Union. This assessment shall include, amongst others, the risks of any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child. If such a risk is found, the platform has to take measures to mitigate

⁸⁷ Such mechanisms facilitate the notification of specific items of information that the notifying party considers to be illegal content to the provider of hosting services concerned, pursuant to which that provider can decide whether or not it agrees with that assessment and wishes to remove or disable access to that content, see European Commission, DSA Proposal (n. 81), Recital 12.

⁸⁸ See Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising', *Berkeley Technology Law Journal* 35 (2020), 1-74.

the risks, such as, for example, adapting content moderation or recommender systems or the display of advertisements in association with the service they provide (Article 27). The only other provision where equality and non-discrimination are mentioned is Article 37, which would allow the EU Commission to set up so-called ‘crisis protocols’ for addressing crisis situations affecting public security or public health. Those protocols, according to Article 37(4)(d), must contain safeguards to avoid negative effects on, *inter alia*, the freedom of expression and the right to non-discrimination.

All in all, the Proposal for a Digital Services Act does go further than previous Internet governance documents in some areas by recognising different dimensions of inequality. Ultimately, however, the proposal does not go as far as it could have, because the noble words and promises in the recitals are not mirrored as concrete commitments in the substantive articles.

5. The State of Equality in Internet Governance: An Interim Conclusion

The content analysis of key documents of Internet governance from a variety of actors reveals no consistent or comprehensive approach to addressing the problem of networked inequality. While all the documents examined address some elements of equality, many of them seem more like a general commitment to abstract values rather than to concrete and enforceable rights, and all of them are incomplete because they address only one of the different dimensions of cyber-equality. Moreover, none of the documents examined seems to address the root causes of cyber-inequality.

Insofar as the analysed documents originate from private actors, it cannot be said that these actors have a direct duty to conform with International Human Rights standards of equality and non-discrimination, because private actors are not duty-bearers.

However, the lack of sensitivity to equality issues that emerges in these documents is problematic for the issue of cyber-equality for there is a danger that existing inequalities will be perpetuated, and new ones might not be detected. In fact, research has shown that inequalities that exist in the analogue world are reproduced in the digital world. Existing societal power structures are transferred to the Internet and repeated and sometimes even amplified there.⁸⁹ Technodeterminism and the perceived neutrality of technology contribute to the public and academia turning a blind eye to such

⁸⁹ See Hargittai and Hsieh (n. 7); Wessels (n. 7).

inequality dynamics. This might also lead to ‘covered-up’ inequalities, inscribed into technology, hidden behind a seemingly neutral Internet architecture, and difficult to challenge legally.

Also, the characteristics of the current Internet governance regime provide little incentives for those responsible to act. It seems, for example, that the libertarian ‘hands off’-approach to Internet governance, such as mirrored, inter alia, in the Declaration of independence of cyberspace,⁹⁰ can have inegalitarian outcomes. And unclear regulatory patterns, diffuse accountability structures, obscured responsibilities, a variety of actors, polycentric regulation, rule-making pluralism, and fragmentation,⁹¹ as well as privatised Human Rights governance,⁹² further add to this situation. In sum, there are several structural barriers that hinder the effective embedding of equality considerations in Internet governance. This is reason enough to trigger an obligation for States to intervene under their Human Rights duties to guarantee equality and protect individuals against discrimination.

V. Equality in Internet Governance: The Way Forward

Equality is a fundamental value and a basic principle of liberal democratic societies and is mirrored in several international treaties, customs, principles, and procedures. This contribution has analysed key documents of Internet governance from an equality perspective, paying particular attention to three dimensions of networked inequality. The analysis revealed that there is no consistent or comprehensive approach to addressing the problem of networked inequality. In view of the various existing cyber-inequalities and the lack of engagement with equality issues in key documents of Internet governance, there seems to be a need for State intervention. The present study can be seen as a first step with a limited selection of cases. More research will be needed to better understand the topic and to embed equality considerations in Internet governance. To conclude this article, I will therefore sketch a research agenda to define a way forward that would help advance the cause of anchoring equality in international Internet law.

First, to gain a more complete overview of equality in Internet governance, more sources could be analysed. This could include the various outcome

⁹⁰ John P. Barlow, *A Declaration of the Independence of Cyberspace*, 1996, available online at <<https://www.eff.org/>>.

⁹¹ See Rolf H. Weber, ‘Elements of a Legal Framework for Cyberspace’, *SRIEL* 26 (2016), 195-215 (203).

⁹² Zalnieriute (n. 6), 66.

documents of the annual Internet Governance Fora, further internet-related regulations and directives of the European Union, recommendations and statements of the Council of Europe and the Organisation for Economic Co-operation and Development (OECD), laws at the national level, basic documents of bottom-up initiatives such as the Internet Society and the Internet Engineering Task Force, statements and reports of the various organs and rapporteurs of the United Nations, and many more. Existing international *hard law* instruments such as the Budapest Convention on Cybercrime should also be critically examined.

In a next step, it would be necessary to engage with the topic on a more abstract, theoretical level. This would involve a critical study of cyber-equality in international and European law, especially in their sub-fields of Human Rights protection. The Human Rights doctrine and practice in the field of cyberlaw must be developed further beyond freedom of expression and the right to privacy to also include the right to equality and non-discrimination. Important questions arise here, including: In cyberspace, with its fragmented and sometimes unclear governance structures, who is responsible for guaranteeing equality and non-discrimination? Which inequalities do constitute a violation of Human Rights? What positive obligations do States and the international community have to enforce the principle of equality and non-discrimination between private parties? What negative obligations do states have in the field of cyber-equality (for example, when it comes to preventing negative side-effects of platform regulation on Human Rights)?

Since the intersecting categories of inequality that exist in the offline world usually continue online and are sometimes even amplified, research on cyber-equality must apprehend equality both as a structural principle as well as an individual right. To make cyberspace more egalitarian, it is therefore not enough to create individual measures against discrimination (e.g. complaint possibilities), but systems must be designed in such a way that they prevent discrimination and inequalities in cyberspace as far as possible or do not allow them in the first place. One example could be the technique of ‘equality mainstreaming’,⁹³ which could be applied in the design of Internet governance. However, it is no longer sufficient to focus exclusively on binary categories of equality (e.g. men/women). A contemporary engagement with cyber-equality must also take into account intersectional, queer-feminist, and postcolonial approaches.

⁹³ Mainstreaming was developed in the context of gender equality and refers to the process of assessing the implications for men and women of any policy, program, or legislation, with the ultimate aim to achieve gender equality, see Hilary Charlesworth, ‘Not Waving but Drowning: Gender Mainstreaming and Human Rights in the United Nations’, *Harvard Human Rights Journal* 18 (2005), 1-18.

Engaging with equality theory in Internet research would allow us to critically question existing and accepted values of Internet governance such as openness or universality.⁹⁴ While laudable and important from a democratic perspective, these values represent ideas of formal equality which can, when applied to situations characterised by structural inequality, lead to outcomes that are at odds with the principle of substantive equality. Meritocratic ideas, which are underlying statements such as the following one, turn a blind eye to structural imbalances based on gender, race, and class:⁹⁵ ‘it is the craft of your work and the elegance and power of your solution that commends it and gives it power. Not your status, not your rank, not your corporate position, not your friendships, but your code: running code, that by its power produces rough consensus.’⁹⁶ It is equality and diversity theory which enables us to critically engage with such long-held values and beliefs in Internet governance and thus ultimately to avoid the ‘online world’ to further drift apart from established democratic values and principles from the ‘offline world’.

⁹⁴ For those values see for example Lessig (n. 4).

⁹⁵ See, for example, Jo Littler, *Against Meritocracy: Culture, Power and Myths of Mobility* (London: Routledge 2017); Squires (n. 20), 478.

⁹⁶ Lessig (n. 4), 1418.

Sovereignty Fever: The Territorial Turn of Global Cyber Order

Chien-Huei Wu*

Institute of European and American Studies, Academia Sinica, Taipei, Taiwan
wch@sinica.edu.tw

Abstract	651
Keywords	651
I. Introduction	652
II. Contesting Global Cyber Governance: The Revisionist's Challenges	654
III. Sovereignty Fever and Its Driving Forces	657
1. The Proliferation of Sovereignties	658
2. Driving Forces Leading to Sovereignty Fever	660
a) Political Ambition	660
b) Economic Value	663
c) Security Concerns	667
d) Human Rights	672
IV. Concluding Remarks: The Territorial Turn and Two-Speed Internet	675

Abstract

This paper argues that the utopia of a borderless and interconnected cyberspace loses its charm and the global cyber order is witnessing a territorial turn. The proliferation of the notion of cyber sovereignty and its variances is a symptom reflecting sovereign states' attempt to retain autonomy and control gradually eroded with the digitalisation of societies and economies. The sovereignty fever can be attributed to four reasons: political ambition, economic value, security concerns, and human rights. However, sovereignty is not the last word in debates concerning the future of digital society, for even liberal democracies have advanced ideas of technological or digital sovereignty, and data sovereignty, for their own very different purposes.

Keywords

internet sovereignty – digital sovereignty – data sovereignty – cybersecurity – *Schrems* – China's Cybersecurity Law

* Associate Research Professor, PhD in Law, European University Institute.

I. Introduction

In 2010, China published its first White Paper on the Internet wherein China referred to the building, utilisation, and administration of the Internet as ‘an issue that concerns national economic prosperity and development, state security and social harmony, state sovereignty and dignity, and the basic interests of the people’.¹ It went on: ‘The Chinese government believes that the Internet is an important infrastructure facility for the nation. Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected.’²

The idea of Internet sovereignty, or cybersovereignty (*wangluo zhuquan*, 网络主权),³ is reaffirmed and expressed in legal terms for the first time in China’s National Security Law, effectuated in 2015, where in Article 25, the State is instructed to ‘safeguard national sovereignty, security and development interests in cyberspace’.⁴ Such an idea was further promoted and disseminated in the international arena when Chinese President Xi Jinping gave his keynote speech, calling for respect of Internet sovereignty, during the Second World Internet Conference (WIC) held in Wuzhen, in December 2015.⁵

China’s jurisdictional and territorial claim of Internet sovereignty is in stark contrast to the United States (US) prevailing characterisations of cyberspace, which are conceptualised as ‘global commons’⁶ or ‘multi-stakeholders governance’.⁷ Internet sovereignty denotes that it is the State that exercises its

¹ China Daily, ‘The Information Office of the State Council, White Paper on Internet in China’, China Daily, 8 June 2010, available at <<https://www.chinadaily.com.cn>>.

² China Daily (n. 1).

³ Before Internet sovereignty gained its popularity in Chinese official statements and academic writings, a similar term, information sovereignty (*xunxi zhuquan*, 信息主权) had been proposed, referring to the State’s sovereign rights to regulate information flows.

⁴ National Security Law of the People’s Republic of China, 1 July 2015, Art. 25.

⁵ Ministry of Foreign Affairs, the People’s Republic of China, ‘Remarks by H. E. Xi Jinping President of the People’s Republic of China at the Opening Ceremony of the Second World Internet conference’, 16 December 2015, available at <<https://www.fmprc.gov.cn>>. [The principle of sovereign equality enshrined in the *Charter of the United Nations* is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation, and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries’ internal affairs, or engage in, connive at, or support cyber activities that undermine other countries’ national security.]

⁶ On cyberspace as ‘global commons’, see, e.g. Milton Mueller, ‘Against Sovereignty in Cyberspace’, *International Studies Review* 22 (2019), 779–801.

⁷ On multi-stakeholderist’ approach on Internet governance, see, e.g. Jeanette Hofmann, ‘Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice’, *Journal of Cyber Policy* 1 (2016), 29–49.

sovereignty over its territorial Internet. In accordance with this sovereign power, the State is competent and capable of delimitation, control, and regulation.⁸ Free flow of information is only possible to the extent that is not against the laws and regulations of the State and in line with the national security and development interests.

Apart from Internet sovereignty, in the digital age emerge digital sovereignty, technological sovereignty, and data sovereignty, which are introduced with a view to reclaiming and retaining control, autonomy, and sufficiency over informational technologies and data flows. Surprisingly, these three types of sovereignty are advanced by not only those countries which guard sovereignty jealously, such as India, but also by countries embracing liberal democracy, such as Germany and France, under the auspice of the European Union (EU).

In view of the proliferation of these sovereignty terms, this paper aims to ascertain whether a 'liberal' cyber world embodied in free flows of expression, information, and data has evidenced a territorial turn. By territorial turn, I mean countries' attempt to delimit the boundary and erect barriers for information inflows/outflows, regardless of the considerations and motivations. The term 'territorial turn' here focuses on the countries' efforts or initiatives to control or regulate information flows and confine them in a given territorial realm.⁹ If so, this paper aims to examine factors and actors driving this turn, and to imagine the future of this territorialised cyber order. Given that China is the most vocal advancing Internet Sovereignty and represents the key force reforming liberal cyber order shaped by the US, the contrast of US and China on their perceptions of global cyber order best evidences the territorial turn of global cyber order, if any. In addition, the EU represents an economic and political project aspiring to transcend national border and encourage 'integration of all countries into the world economy',¹⁰ pursuing technological sovereignty or digital sovereignty in the name of autonomy and self-sufficiency signals a retreat from an open and liberal Europe. A comparison between these three key actors in embracing or

⁸ Ronald J. Deibert and Masashi Crete-Nishihata observe a trend of Internet filtering, turning cyberspace from open commons to controlled access. Ronald J. Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls', *Global Governance* 18 (2012), 339-361 (341-346). See also Ronald Deibert and Rafal Rohozinski, 'Liberation vs. Control: The Future of Cyberspace', *Journal of Democracy* 21 (2010), 43-57.

⁹ Given the cross-border nature of information flows, such efforts and initiatives might impact third countries or give rise to extraterritorial effects, but these side effects are not the main concern of this paper. Rather, I am more interested in the driving forces and rationale why countries delimit the cyberspace, originally conceived as 'global commons', and subsequently control and regulate activities in the territorialised cyberspace.

¹⁰ Art. 21 para. 2 lit. a) TEU.

rejecting the sovereignty terms in global cyber governance contributes to our understanding on the changing dynamics underpinning international politics and the digital world.

With these aims, this paper first traces the evolution of mainstream conceptions of cyber order in the US context and then explores challenges introduced by China's rise in international relations and its expansionist ambition under the "Chinese Dream". The paper then examines the contagion of sovereignties, explains the reasons for this proliferation, and concludes with the future of this liberal, free, and open cyber order.

II. Contesting Global Cyber Governance: The Revisionist's Challenges

The rise of China, along with that of other emergent powers, has shaken every part of the globe and the concomitant threats to liberal international order have elicited discussion in international relations¹¹ and international law¹² fora, and led some scholars to argue that the authoritarian turn of international law is happening¹³ and authoritarianism is going global.¹⁴ However, it is misleading to argue that emergent countries, such as Brazil, Russia, India, China, and South Africa, collectively known as the BRICS, maintain one and unified position that are contrary to and compete with that of the US and other Western countries.¹⁵ Moreover, the US and EU diverge on a number of Internet regulatory issues, in particular over privacy, as seen in the debate over involuntary surveillance and data collection by corporations and governments.¹⁶

That said, a consensus has held that the US and China each compete to shape the global cyber order in their favour. The US is the predominant cyber power

¹¹ See, e.g. G. John Ikenberry, 'The End of Liberal International Order?', *Int'l Aff.* 94 (2018), 7-23; Naná De Graaff and Bastiaan Van Apeldoorn, 'US-China Relations and the Liberal World Order: Contending Elites, Colliding Visions?', *Int'l Aff.* 94 (2018), 113-131.

¹² See, e.g. Eric A. Posner and John Yoo, 'International Law and the Rise of China', *Chinese Journal of International Law* 7 (2006), 1-15; Congyan Cai, *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously* (Oxford: Oxford University Press 2019).

¹³ Tom Ginsburg, 'Authoritarian International Law?', *AJIL* 114 (2020), 221-260.

¹⁴ Ron Deibert, 'Authoritarianism Goes Global: Cyberspace Under Siege', *Journal of Democracy* 26 (2015), 64-78.

¹⁵ Hannes Ebert and Tim Maurer, 'Contested Cyberspace and Rising Powers', *TWQ* 34 (2013), 1054-1074 (1055).

¹⁶ See, David Drissel, 'Internet Governance in a Multipolar World: Challenging American Hegemony', *Cambridge Review of International Affairs* 19 (2006), 105-120 (111-113).

possessing the core component of cyber resources, including infrastructures, networks, and servers, and leader shaping the multi-stakeholder Internet governance regime.¹⁷ As a latecomer, and given its relatively weak position in the Internet governance regime, China calls for ‘multilateral, democratic and transparent’ global cyber governance, but interprets these terms differently than Western countries do. Multilateralism on Internet governance is to be built upon, and underpinned by, the United Nations (UN) framework.¹⁸ Democracy dictates global cyber governance be subject to sovereign equality without being monopolised by a few countries, whereas transparency relates to the decision-making processes which are to be made known to all countries.¹⁹ As this paper focuses on the proliferation of sovereignties, the contrast between multi-stakeholderism and multilateralism is most relevant.

Multi-stakeholderism departs from the traditional Westphalian system engaging actors other than governments in the global decision and policy-making processes.²⁰ Whereas some see multi-stakeholderism as a prerequisite for an inclusive and practice-oriented approach, it is opposed not only by those who embrace traditional state sovereignty, but also by critics who question the legitimacy, transparency, and accountability of multi-stakeholder initiative.²¹ Internet governance based on multi-stakeholderism is best reflected in a report by the Working Group on Internet Governance, referring to ‘the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet’.²² Therefore, the objective of multi-stakeholderist Internet governance is to bring those affected into the policy-making processes and thus enhance procedural legitimacy and reach better policies.²³ The

¹⁷ As the former Secretary of State, John Kerry spoke at the University of Korea in 2015, ‘[u]nlike many models of government that are basically top-down, the Internet allows all stakeholders – the private sector, civil society, academics, engineers, and governments – to all have seats at the table. And this multi-stakeholder approach is embodied in a myriad of institutions that each day address Internet issues and help digital technology to be able to function.’ John Kerry, Secretary of State, ‘An Open and Secure Internet: We Must Have Both’, *VOAnews*, 18 May 2015, available at <<https://www.voanews.com>>.

¹⁸ Cuihong Cai, ‘China and Global Cyber Governance: Main Principles and Debates’, *Asian Perspective* 42 (2018), 647–662 (656–657).

¹⁹ Cai (n. 18), 652–653.

²⁰ On the multiple actors in global cyber governance, see generally, Joseph S. Nye, Jr., ‘The Regime Complex for Managing Global Cyber Activities’, *Global Commission on Internet Governance Paper Series*, 1 May 2014, available at <<https://www.cigionline.org>>.

²¹ Christine Kaufmann, ‘Multistakeholder Participation in Cyberspace’, *Swiss Review of International & European Law* 26 (2016), 217–234 (217–218).

²² Working Group on Internet Governance, Document WSIS-II/PC-3/DOC/5-E, para. 10.

²³ Hofmann (n. 7), 29.

difficult question nonetheless relates to how to decide the scope of those affected, and to what extent decision making is improved.²⁴ Moreover, as powerful multi-national Internet companies and influential non-governmental organisations are located mostly in developed countries, worries arise as to whether developing or less developed countries are marginalised or prejudiced. In fact, this is the reason why China asserts the multi-stakeholderist approach in Internet governance is not 'democratic' and calls instead for multilateral Internet governance.

China's proposal for multilateral cyber governance is based on the Westphalian system and consistent with its attachment to national sovereignty and efforts to import into cyberspace a concept of sovereignty under which only sovereign states are entitled to decide the form and substance of the global cyber governance regime.²⁵ Multilateral models of global cyber governance are to be found in various UN groups, including the Group of Governmental Experts (GGE),²⁶ the Open-Ended Working Group (OEWG) and expert commissions, such as the Global Commission on the Stability of Cyberspace.²⁷ Within these multilateral frameworks, the most noteworthy attempts by China, in cooperation with Russia and other Shanghai Cooperation Organization (SCO) countries, to shape global cyber norms are their submissions of an International Code of Conduct for the Emerging Information Society to the UN General Assembly for debates in 2011²⁸ and 2015.²⁹ The Code of Conduct unsurprisingly underlines sovereignty, territorial integrity and political independence, and calls for UN members to refrain from using information and communications technologies and networks to interfere in

²⁴ Alexander Klimburg and Louk Faesen, 'A Balance of Power in Cyberspace' in: Dennis Broeders and Bibi Van Den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (Lanham/Boulder/New York/London: Rowman & Littlefield 2020), 151-152.

²⁵ Andrew N. Liaropoulos, 'Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics', *Journal of Information Warfare* 15 (2016), 14-26 (15).

²⁶ The UNGGE constitutes a good forum to explore States' perception on Internet sovereignty, digital sovereignty, technological sovereignty, and data sovereignty. By investigating the practices and statements of States in this forum, it contributes to our understanding on the divergence and convergence of States in these complex concepts. The author owes this point to the anonymous reviewer.

²⁷ Christian Ruhl, Duncan Hollis, Wyatt Hoffman and Tim Maurer, 'Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads', Carnegie Endowment for International Peace, 2020, 4-9.

²⁸ Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, 14 September 2011.

²⁹ Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, 13 January 2015.

the internal affairs of other States, or with the aim of undermining their political, economic and social stability. Such attempts were seen as an effort to use multilateral fora to justify domestic suppression of Internet freedoms by China and other authoritarian regimes.³⁰

On the other hand, China aims to reduce the US' influence over key multi-stakeholderist cyber governance institutions, the best example being the *Internet Corporation for Assigned Names and Numbers (ICANN)*. China and other countries, emergent and developed alike, continue to complain about the privileged position of the US in the ICANN owing to the Internet Assigned Numbers Authority functions contract. Due to the growing resentment of other countries, the US Department of Commerce finally agreed to eliminate its contractual oversight of ICANN and handed over authority to the global multi-stakeholder community.³¹ The case of ICANN illustrates the dominant position of the US in key multi-stakeholderist global cyber governance institutions and explains why China aims to pursue a multilateral cyber governance regime, as under such a system it would have an equal say with the US.

III. Sovereignty Fever and Its Driving Forces

While China's proposed concept of Internet sovereignty and a multi-lateral governance model is unsurprising, sovereignty has gained popularity in recent decades, not only in authoritarian regimes but also in liberal democracies. I argue that four key factors contribute to the sovereignty fever in cyberspace and the digital world: political control, economic value, security concerns, and human rights. However, it should be made clear that these four factors are not clear-cut. Security considerations may be of economic value, which at the same time contributes to political ambition, while security considerations may also be linked to human rights as a means of safeguarding ways of life or values. The four factors I propose and the relevant examples discussed in this paper are to advance a set of angles to perceive the proliferation of sovereignties and delineate the underlying rationale. Below, I will first trace the proliferation of sovereignties and explain their driving forces.

³⁰ Jinghan Zeng, Tim Stevens and Yaru Chen, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"', *Politics & Policy* 45 (2017), 432-464 (440).

³¹ Milton Mueller, 'Detaching Internet Governance from the State: Globalizing the IANA', *Georgetown Journal of International Affairs* 4 (2014), 35-44 (35).

1. The Proliferation of Sovereignities

When the Internet was first invented, it was expected that it would be transnational and boundaryless, and thus know no border. When John Perry Barlow presented the well-known *A Declaration of the Independence of Cyberspace*, it was proclaimed that governments of the industrial world exercise no sovereignty over cyberspace.³² That vain hope soon faded. On the contrary, sovereignty became common parlance in cyberspace over the past decade among liberal democracies and authoritarian regimes alike.

Empirically, Marie Baezner and Patrice Robin review national cybersecurity strategies and explore how the concept of sovereignty is understood and applied in cyberspace. Some states use the word to highlight the need to protect governmental information systems, defence forces, and critical infrastructures in order to safeguard state sovereignty. Second, states refer to cyberattacks or other malicious cyber-activities as threats to their sovereignty. Third, states may also go beyond cybersecurity strategies and use the word ‘sovereignty’ in other policy documents. Finally, states argue that a secure cyberspace would protect their sovereignty.³³ However, the relevance of sovereignty in cyberspace is not limited to cybersecurity. In fact, when China pronounces Internet sovereignty, its scope is much more comprehensive than cybersecurity alone. Further, security concerns in cyberspace relate not only to safety from theft, disruption, destruction, or espionage, but also include insufficiency, unavailability, or inadequacy. In correspondence with their divergent views on cyberspace and their different values and interests, China, the US, and the EU conceive of cyberspace differently, and pursue different cyber strategies.³⁴

In 2015, Chinese President Xi Jinping declared the concept of ‘Internet sovereignty’, illustrating cyberspace’s territorial concept under the jurisdiction of a country. Contrary to conventional ideas of international freedom embraced by western countries, China attempts to include the cyberspace in the domestic jurisdiction and legitimises its governance and supervision of the Internet.³⁵ Under international law, countries enjoy supreme dominance

³² John Perry Barlow, ‘A Declaration of the Independence of Cyberspace’, Davos, Switzerland, 8 February 1996, available at <<https://www.eff.org>>.

³³ Marie Baezner and Patrice Robin, *Cyber Sovereignty and Data Sovereignty*, (Zurich: Center for Security Studies, ETH 2018), 9.

³⁴ Andrés Ortega Klein, ‘The U.S.-China Race and the Fate of Transatlantic Relations’, CSIS Report, 23 April 2020, available at <<https://csis-website-prod.s3.amazonaws.com/>>.

³⁵ Michael Kolton, ‘Interpreting China’s Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence’, *The Cyber Defense Review* 2 (2017), 119-154.

over their own territory, and China wishes to see the application of sovereignty to the cyberspace extends this dominance.³⁶

By contrast, the EU proposes the concepts of ‘digital sovereignty’³⁷ or ‘technological sovereignty’ to address the challenges facing Europe arising from digitalisation of the economy and society. The President of the European Commission, Ursula von der Leyen, in her 2019 inauguration speech, claimed: ‘we must have mastery and ownership of key technologies in Europe’.³⁸ The digital sovereignty strategy is intended to maintain the EU’s independence in cyberspace and to safeguard the privacy of its people. The term ‘sovereignty’ as used by the European Commission, addresses economic issues but also extends to the EU’s political operations and strategic concerns.

The EU, following others’ lead, embraced the idea of ‘data sovereignty’, meaning that online data and information are subject to domestic jurisdiction.³⁹ Namely, all information which has been stored in binary digital form is subject to the laws of the country in which it is located;⁴⁰ the same applies to data/information inflows into and outflows out of this country. Many of the current concerns surrounding data sovereignty relate to enforcing privacy regulations and preventing data that is stored in a foreign country from being subpoenaed by the host country’s government. The concept of data sovereignty addresses stored data and its flows (data in transit), not overall jurisdiction of cyberspace.

The US does not use the term of ‘sovereignty’ but rather addresses cyberspace in security terms. As it stands, the US possesses the largest number of root servers and treats data as an asset⁴¹ to be leveraged for the public good;⁴²

³⁶ Zeng, Stevens and Chen (n. 30), 434–464.

³⁷ Silvia Amaro, ‘Europe’s Dream to Claim Its “Digital Sovereignty” Could Be the Next Big Challenge for US Tech Giants’, CNBC, 20 November 2019, available at <<https://www.cnbc.com/>>; Luciano Floridi, ‘The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU’, *Philosophy & Technology* 33 (2020), 369–378.

³⁸ Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme, 27 December 2020, available at <<https://ec.europa.eu/>>; see further, Tyson Barker, ‘Europe Can’t Win the Tech War It Just Started’, *Foreign Policy*, 26 January 2020, available at <<https://foreignpolicy.com/>>.

³⁹ Dana Polatin-Reuben and Joss Wright, ‘An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet’ in: *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)* (San Diego, CA: USENIX Association 2014), available at <<https://www.usenix.org/>>.

⁴⁰ Stephane Couture and Sophie Toupin, ‘What Does the Notion of “Sovereignty” Mean When Referring to the Digital?’, *New Media & Society* 21 (2019), 2305–2322.

⁴¹ U.S. Department of Defense, ‘U.S. Dep’t of Defense’, DoD Data Strategy, 30 September 2020, available at <<https://media.defense.gov/>>.

⁴² Federal Data Strategy, ‘Components of the Federal Data Strategy’, Official website of the United States Government, available at <<https://strategy.data.gov/>>.

it emphasises limitless, free flow of data across borders with the goal of reducing the regulation of data as much as possible.⁴³ In 2013, the Open Data policy required government agencies to provide data in a machine-readable format to strengthen democracy and efficiency.⁴⁴ However, challenges stemming from China's claims of cyber sovereignty, together with cyberattacks originating in China, led the US to announce a revised cybersecurity policy. Thus, in 2018, the White House published the *National Cyber Strategy of the United States of America* (the USNCS),⁴⁵ contending that the competitors and adversaries of the US hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities.⁴⁶ With a view to address these threats, the USNCS aims to

[...] defend the homeland by protecting networks, systems, functions, and data; promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; reserve peace and security by strengthening the ability of the United States – in concert with allies and partners – to deter and, if necessary, punish those who use cyber tools for malicious purposes; and expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.⁴⁷

While the USNCS does not speak of sovereignty in cyberspace, its overarching aim is to safeguard American interests, a function of the exercise of sovereignty.

2. Driving Forces Leading to Sovereignty Fever

a) Political Ambition

The leading proponent of Internet sovereignty is undoubtedly China, motivated by its need to maintain regime stability. China's capacity to control and regulate information flows is a key instrument of its censorship and surveillance of its citizens, and a means of ensuring that the Chinese Commu-

⁴³ Adil Nussipov, 'How America and Europe Deal with Data', Central European University School of Public Policy, 7 January 2020, available at <<https://cmds.ceu.edu>>.

⁴⁴ Exec. Order No. 13642, 3 CFR 13642, Making Open and Machine Readable the New Default for Government Information (2013), available at <<https://www.govinfo.gov>>.

⁴⁵ U.S. White House, 'National Cyber Strategy of the United States of America', September 2018, available at <<https://www.whitehouse.gov>>.

⁴⁶ See III. 1.

⁴⁷ See II.

nity Party is not challenged. Consistent with its ‘peaceful rise’,⁴⁸ China is no longer content with being a ‘rule-taker’ but rather strives to be a ‘rule-shaper’ or ‘rule-maker’; as such it desires to shape international order to its ends.⁴⁹ China’s promotion of the concept of Internet sovereignty internationally is reflective of its willingness to set new norms in cyber governance.⁵⁰ Budnitsky and Jia thus argue that Internet sovereignty is not only an expression of digital policy, but also an instrument of ‘nation branding’ employed to promote China’s national identity as a great power on the international scene. Thus, cyber sovereignty extends beyond traditional state territorial authority and rather functions as an expression of nationalism; that is, it promotes a distinct national identity, or national vision of what the Internet should be.⁵¹

Chinese political leaders see Internet sovereignty as a cornerstone of its overarching cybersecurity strategy, part and parcel of its national security, and comprised of three dimensions: governance, internal influence, and national defence.⁵² The governance dimension relates to a State’s right to participate in international cyber governance on an equal footing, which corresponds to the principle of sovereign equality. The internal influence dimension concerns a State’s paths and models of cyber development and regulation free from foreign interference – reflective of China’s preference for the principle of non-interference. The national defence dimension addresses third countries’ online activities undermining its national security. In a word, China’s concept of Internet sovereignty is an extension or application of its preferred interpretation of the conventional Westphalian sovereignty concept to cyberspace. Internally, it can justify its regulatory or suppressive measures against its citizens. Externally, it can claim due representation in international cyber governance and seek to safeguard itself from foreign threats and influence in the name of national security.

China’s efforts to monitor and censor information flows comprise a dense web of sophisticated measures. After the crackdown of student protests in

⁴⁸ See, e.g. Zheng Bijian, ‘China’s “Peaceful Rise” to Great-Power Status’, *Foreign Aff.* 84 (2005), 18–24; Barry Buzan, ‘China in International Society: Is “Peaceful Rise” Possible?’, *The Chinese Journal of International Politics* 3 (2010), 5–36; Herbert S. Yee (ed.), *China’s Rise – Threat or Opportunity* (London: Routledge 2011).

⁴⁹ Shiping Tang, ‘China and the Future International Order(s)’, *Ethics & International Affairs* 32 (2018), 31–43; G. John Ikenberry, ‘The Rise of China and the Future of the West – Can the Liberal System Survive?’, *Foreign Aff.* 87 (2008), 23–37; Shaun Breslin, ‘China and the Global Order: Signalling Threat or Friendship?’, *InternInt’l Aff.* 89 (2013), 615–634.

⁵⁰ Zeng, Stevens and Chen (n. 30), 434.

⁵¹ Stanislav Budnitsky and Lianrui Jia, ‘Branding Internet Sovereignty: Digital Media and the Chinese-Russian Cyber Alliance’, *European Journal of Cultural Studies* 21 (2015), 594–613.

⁵² Sarah McKune and Shazeda Ahmed, ‘The Contestation and Shaping of Cyber Norms Through China’s Internet Sovereignty Agenda’, *International Journal of Communication* 12 (2018), 3835–3855 (3837).

Tiananmen Square, Chinese leaders pondered how to fence China off from the intrusion of Western liberal ideas from the Internet. To this end, the Golden Shield project, which gave rise to the so-called ‘Great Firewall of China’, enabled the government to block access to blacklisted Internet resources and to censor network traffic related to banned keywords and phrases.⁵³ A more recent instrument with which China has strengthened its online monitoring and surveillance of its citizens is its ‘social credit system (*shehui xinyong tixi*, 社会信用体系)’ which enables the State to trace the digital footprint of every individual.⁵⁴ The underlying feature of China’s Internet control and regulatory regimes is a real-name requirement complemented by biometric data. Under China’s Cybersecurity Law the real-identity requirement applies when seeking: access to a stationary or mobile network; registration of a domain name; information publication; or instant messaging;⁵⁵ mandatory facial recognition is required for the purchase of a SIM card in accordance with a circular issued by the Ministry of Industry and Information Technology in 2019.⁵⁶

Externally, China is keen to export its Internet regulatory model to other authoritarian countries, Russia and African countries in particular, and to project it onto the global cyber order, which contributes to the legitimacy of its Internet monitoring and control regime. This objective may be achieved via different channels: bilaterally, regionally or multilaterally. *Bilaterally*, China concluded an agreement on information security with Russia on 8 May 2015, where the Parties reaffirm that ‘the sovereignty and international norms and principles derived from the state sovereignty, apply to the conduct of States in the framework of activities related to the use of information and communication technologies, and the jurisdiction of States over information’.⁵⁷ *Regionally*, China has used the SCO as a platform to promote the concept of Internet sovereignty and participant countries of the SCO are also

⁵³ Zeng, Stevens and Chen (n. 30), 438. Some illustrative words and phrases are ‘4 June 1989’, ‘Tiananmen Square’ and ‘Arab Spring’.

⁵⁴ On this social credit system, see, e.g. Yu-Jie Chen, Ching-Fu Lin and Han-Wei Liu, ‘“Rule of Trust”: Powers and Perils of China’s Social Credit Megaproject’, *Columbia Journal of Asian Law* 32 (2018), 1-36.

⁵⁵ Art. 24 Cybersecurity Law of the People’s Republic of China (China’s Cybersecurity Law), Effective 1 June 2017.

⁵⁶ BBC, ‘China Due to Introduce Face Scans for Mobile Users’, 1 December 2019, available at <<https://www.bbc.com>>.

⁵⁷ Agreement between the Government of the Russian Federation and the Government of the People’s Republic of China on Cooperation in Ensuring International Information Security (China-Russia Information Security Agreement), 8 May 2015, Preamble, available at <<http://treaty.mfa.gov.cn>> (Chinese version); an unofficial English version is available at <<https://cyber-peace.org/>>. It should be noted that whereas the English version use ‘jurisdiction’, the Chinese version uses ‘sovereign rights (*zhuquan quanli*, 主权权利)’.

prominent attendees of the WIC. Therefore, the SCO and Wuzhen processes are two fora/platforms through which China can promote its Internet governance model and cement the concept of Internet sovereignty.⁵⁸ *Multilaterally*, China, in collaboration with Russia and other SCO members, has attempted to project the concept of Internet sovereignty to global cyber order. As already mentioned, in 2011 and 2015, they submitted to the United Nations General Assembly an International Code of Conduct for Information Security with a view to create a consensus for preferred norms surrounding Internet sovereignty and information security.⁵⁹ While these attempts were rejected by the US and other Western countries, which see them as an effort to establish a strict national sovereignty model for information flows on the Internet and a potential instrument for suppressing dissents,⁶⁰ the attempts demonstrate the ambition of China and other SCO members to shape global cyber governance around the concept of sovereignty.

b) Economic Value

Economic value – the second driver contributing to the sovereignty fever – ranges from E-commerce to digital economy and has spread in both China and European countries. The US is no exception, although it does not spell out sovereignty *per se*.

When China joined the World Trade Organisation (WTO) in 2002, it was expected that China would open its market to foreign enterprises, including online services providers. This hope was soon dampened. Google withdrew from China in 2010, ten years after the launch of its Chinese version. During that decade, Google had sought a license from China and succeeded in securing one, but its search engine was nonetheless blocked from time to time. At the same time, Google was accused of sacrificing its commitment to business ethics and human rights for access to China's market.⁶¹ Following repeated compromises and frustrations, Google decided to withdraw from the Chinese market. One of the key reasons for Google's withdrawal is believed to have been hacking attacks targeting everything from Google's intellectual property to the email accounts of Chinese activists. By the time it withdrew, Google accounted for more than one-third of the Chinese search

⁵⁸ McKune and Ahmed (n. 52), 3841-3850.

⁵⁹ McKune and Ahmed (n. 52), 3835-3842; Zeng, Stevens and Chen (n. 30), 440.

⁶⁰ Zeng, Stevens and Chen (n. 30), 440.

⁶¹ See, e. g. G. Elijah Dann and Neil Haddow, 'Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China's Internet', *Journal of Business Ethics* 79 (2008), 219-234.

market, while China's domestic search engine, Baidu, had captured the lion's share with 58 percent.⁶² The same story applies to Yahoo, except that Yahoo decided to sell its China operations to Alibaba, China's E-commerce giant, in exchange for a 40 percent stake in Alibaba,⁶³ which Yahoo sold back to Alibaba in 2012.⁶⁴ Most social media sites are not available in China; notably, Facebook has attempted to gain access to China but without success.

The exclusion or deterrence of foreign Information and Communications Technology (ICT) enterprises from China's domestic market is complemented and supplemented by subsidies, and an industrial policy favouring local firms modelled on state-capitalism. According to a study by the European Centre for International Political Economy, trade barriers targeting the ICT sectors and online markets substantially increased in the years 2007 to 2016, accounting 54 out of total of 76 measures.⁶⁵ Such an increase in trade barriers corresponded with China's 13th Five-Year Plan for the period of 2015 to 2020, which called upon ICT to 'underpin China's rise as a global power and its internal transformation.'⁶⁶ Jean-Christophe Plantin and Gabriele de Seta further detail how WeChat (*Weixin*, 微信), first developed as a mobile-oriented messaging application by Tencent, has evolved to be a part of the infrastructure for China's techno-nationalist digital economy. They note, 'protectionist environment resulting from the demanding regulatory conditions to operate in the Chinese market and the outright ban of foreign companies still allow Chinese platforms to easily reach the criticality and scale'.⁶⁷ The dominance of domestic social media or other online services in turn contributes to China's capacity to enforce censorship and maintain regime stability.⁶⁸

Money talks not only in China but also in the EU and the US, albeit in different currencies. The EU frames the economic value with 'digital sover-

⁶² Matt Sheehan, 'How Google Took on China – and Lost', MIT Technology Review, 19 September 2018, available at <<https://www.technologyreview.com/>>.

⁶³ David Barboza, 'Yahoo Is Paying \$1 Billion for 40 % Stake in Alibaba', New York Times, 11 August 2005, available at <<https://www.nytimes.com/>>.

⁶⁴ Kevin Voigt, 'Yahoo, Alibaba Reach \$7.1 Billion Deal', CNN, 20 May 2012, available at <<https://edition.cnn.com/>>.

⁶⁵ Martina E. Ferracane and Hosuk Lee-Makiyama, 'China's Technology Protectionalism and Its Non-Negotiable Rationales', ECIPE Working Paper, 27 June 2017, 3.

⁶⁶ Yu Hong, 'Reading the 13th Five-Year Plan: Reflections on China's ICT Policy', International Journal of Communication 11 (2017), 1755-1774 (1755).

⁶⁷ Jean-Christophe Plantin and Gabriele de Seta, 'WeChat as Infrastructure: the Techno-Nationalist Shaping of Chinese Digital Platforms', Chinese Journal of Communication 12 (2019), 257-273 (267-268).

⁶⁸ Jennifer Pan, 'How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship', Problems of Post-Communism 64 (2017), 167-188 (168).

eignty' based on digital economy whereas the US sees dependence on China's ICT products and services as a threat to US economic security, a central element of national security under the National Security Strategy of the Trump Administration.⁶⁹ The President of the European Commission, Ursula von der Leyen, in seeking for her nomination, proclaimed that digital technologies are transforming the world at an unprecedented speed, changing both societies and economies, and digitalisation and cyber are two sides of the same coin. 'It may be too late to replicate hyperscalers, but it is not too late to achieve technological sovereignty in some critical technology areas.'⁷⁰ The concept of technological sovereignty is further elaborated by the European Commission in its Communication on Shaping Europe's Digital Future: 'European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks, and communications. It requires creating the right conditions for Europe to *develop and deploy its own key capacities, thereby reducing our dependency* on other parts of the globe for the most crucial technologies. Europe's ability to define its own rules and values in the digital age will be reinforced by such capacities.'⁷¹

According to a briefing paper by the European Parliament Research Service, the notion of technological or digital sovereignty is proposed and portrayed as 'a means of promoting the notion of European leadership and strategic autonomy in the digital field'.⁷² Concerns have been raised over the social and economic influence of non-EU technology companies, exemplified by contact tracing apps during the COVID-19 pandemic, which may undermine the EU's capacity to enforce its law and regulations, constrain European companies' potential for growth and weaken European citizens' control over their personal data.⁷³ Conceived of thus, digital sovereignty has economic value. As Frances Burwel and Kenneth Propp point out, the underlying rationale running through various legislative proposals by the European

⁶⁹ National Security Strategy of the United States of America, December 2017, 13.

⁷⁰ Ursula von der Leyen, 'A Union that Strives for More: My Agenda for Europe by Candidate for President of the European Commission', October 2019, 13. The concept of digital sovereignty as a new paradigm for Internet governance in fact emerged in European discourse before the von der Leyen Commission. Among the EU Member States, France is one of the most vocal in proposing such an idea. See, e.g. Farid Gueham, Digital Sovereignty – Steps Towards a New System of Internet Governance (translated by Caroline Lorriaux and Michael Scott, the Fondation pour l'innovation politique 2017).

⁷¹ COM(2020) 67 final, p. 2 (emphasis added).

⁷² Tambiama Madiaga, 'Towards a More Resilient EU: Digital Sovereignty for Europe', EPRS Ideas Paper, PE 651.992 – July 2020, 1. Several Members of European Parliament, including Viviane Reding and Axel Voss, also promote enthusiastically the concept of 'digital sovereignty'.

⁷³ Madiaga (n. 72).

Commission, ranging from development and use of artificial intelligence and the participation of high-risk vendors in critical networks and management of data, lies in the EU's desire to strengthen its competitiveness vis-à-vis dominant players in the digital space.⁷⁴

Upholding Internet sovereignty, digital sovereignty or data sovereignty in the interests of economic competitiveness will inevitably lead to suspicion and critiques of digital-protectionism or techno-protectionism. In a paper published by the European Political Strategy Centre (EPSC) in 2019, it is argued that China adopts techno-protectionism by pursuing a state-centric approach built-upon comprehensive industrial strategic instruments and reduced dependence on imported foreign technologies. In this context, the EPSC underlines China's concept of cyber sovereignty contributes to this techno-protectionism.⁷⁵ Interestingly, Susan Ariel Aaronson, a professor at George Washington University, sees the EU (as well as the US) as hypocritical on the grounds that while the EU condemns digital protectionism, it adopts policies and practices which it would target and label as trade-distorting if adopted by other countries.⁷⁶

In fact, economic competitiveness is situated in a broad context of economic independence or self-sufficiency,⁷⁷ which digital sovereignty aims to safeguard through the preservation of strategic autonomy. In this way, the EU is able to decide to maintain or reshape European ways of life. This thus links to the security rationale for the sovereignty fever in the cyber governance; the forerunner is undoubtedly the Trump Administration, but the Juncker Commission was also supportive of a technological race in the name of economic security and such position is followed and strengthened by the

⁷⁴ Frances Burwel and Kenneth Propp, 'The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World, Atlantic Council Future Europe Initiative', Atlantic Council – Future Europe Initiative, Issue Brief, June 2020, 2. See Matthias Bauer and Fredrik Erixon, 'Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls', ECIPE Occasional Paper, 02/2020, 18-26. It should also be noted that the EU's desire to strengthen competitiveness extends from digital sovereignty to data sovereignty. According to the European Commission, the current situation of a small number of Big Tech firms dominating a large part of the world's data suppresses the potential of data-driven economy. The European Commission thus calls for finding a European way of data strategy to unleash the potential by 'balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards'. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: a European Strategy for Data, Brussels, COM(2020) 66 Final, 19 February 2020, 3.

⁷⁵ European Political Strategy Centre, 'Rethinking Strategic Autonomy in the Digital Age', EPSC Strategic Notes, Issue 30, July 2019, 12.

⁷⁶ Susan Ariel Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', *World Trade Review* 18 (2019), 541-577 (557).

⁷⁷ European Political Strategy Centre (n. 75), 8-11.

von der Leyen Commission.⁷⁸ As for China, national security is the upmost imperative and safeguarding cybersecurity in the name of Internet sovereignty is no surprise.

c) Security Concerns

Security concerns regarding the Internet are equally shared by the US, China, and the EU, but each conceives security differently. On the one hand, the US and China accuse one another of cyber theft and cyber espionage; on the other hand, China's conception of cybersecurity endorses giving greater weight to maintaining control of the Internet in the name of national security.

China's cybersecurity policy is built upon its National Security Law and specified and amplified in Cybersecurity Law. Article 59 of the National Security Law instructs the State to establish a national security review and oversight mechanism for foreign investments, critical materials and technologies, *the Internet and information technologies and services*. Under this overarching objective, the Cybersecurity Law regulates cybersecurity in two dimensions: network security and information security. Regarding network security, two provisions are most controversial: Articles 23 and 27. *Article 23* of the Cybersecurity Law instructs Chinese cybersecurity and information departments, together with the relevant departments of the State Council, to formulate and release a catalogue of critical network equipment and specialised cybersecurity products which are to comply and be certified with national security standards before coming to market.⁷⁹ Given the vague definitions of critical network equipment and specialised products, the scope of its application relies heavily on the discretion and interpretation of the administrative agencies.⁸⁰ Moreover, there are concerns that intellectual property rights may be infringed,⁸¹ or malicious items or software inserted during

⁷⁸ In the wake of the COVID-19 pandemic, the European Commission in its recent communication on 2030 Digital Compass proclaims that '[t]he pandemic has also exposed the vulnerabilities of our digital space, its dependencies on non-European technologies, and the impact of disinformation on our democratic societies'. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European Way for The Digital Decade, COM(2021) 118 final, 9 March 2021.

⁷⁹ Art. 23 China's Cybersecurity Law.

⁸⁰ Jyh-An Lee, 'Hacking into China's Cybersecurity Law', Wake Forest Law Review 53 (2017), 57-104 (72).

⁸¹ It is argued that foreign companies may be forced to hand over intellectual property to operate in China. Also, there is a danger of leakage of trade secrets during the security review processes as politically well-connected competitors may have a chance to see their profiles. Lee, (n. 80), 85.

the inspection and certification process. *Article 23* of Cybersecurity Law further obliges network operators to provide technical support and assistance to public security organs and national security organs safeguarding national security and investigating criminal activities.⁸² Worries are voiced that network operators may lose their confidential information or trade secrets; or they may act as an instrument of Chinese cyber theft, surveillance and control, or espionage.⁸³

In addition to enacting national legislation to safeguard cybersecurity, China has also pursued cybersecurity through diplomacy both with its allies and adversaries. Under the China-Russia Information Security Agreement, the two sides have attempted to strengthen cooperation in addressing threats to international information security arising from the application of information technologies, including national security and territorial integrity, critical information technology infrastructure, terrorism, crimes; also interference in countries' internal affairs, breaches of public order, and subversions of social-economic systems.⁸⁴ The broad scope and wide application of this agreement is reflective of the two countries' overly-inclusive conception of cybersecurity, and their obsessions with regime stability. Regionally, China has used SCO to address cybersecurity and fight what SCO members describes as three-evils: extremism, separatism, and terrorism.⁸⁵ The SCO led to the Agreement on Cooperation in Ensuring International Information Security in 2009 (SCO Information Security Agreement). Importantly, the parties see the 'use of *dominant position* in information space to the detriment of interests and safety of other states'⁸⁶ as a threat to their cybersecurity. The dominant position referred to here is, without doubt, that of the US.

Interestingly, whereas China sees the dominant position of the US as a threat to its cybersecurity, the US (and its allies) view China's cyber intrusions and operations against their governments, enterprises, and civil organisations, as threats to their cybersecurity. The US Department of Justice, under the Obama Administration, for the first time filed a criminal charge against known state actors, Chinese military hackers, for computer hacking and economic espionage.⁸⁷ The Chinese Defence Ministry responded with a strongly-worded statement which, referring to the Snowden and WikiLeaks,

⁸² Art. 27, China's Cybersecurity Law.

⁸³ Lee (n. 80), 75.

⁸⁴ Art. 2 China-Russia Information Security Agreement.

⁸⁵ McKune and Ahmed (n. 52), 3842.

⁸⁶ Art. 2.4 SCO Information Security Agreement.

⁸⁷ Office of Public Affairs, Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage', 19 May 2014, available at <<https://www.justice.gov>>.

accused the US of implementing worldwide surveillance based on its advantage in critical information technology infrastructure.⁸⁸ Diplomatic tensions between the US and China were resolved, or at least deescalated, with the signing of the US-China Cybersecurity Agreement in the lead up to President Xi Jinping's state visit to the US.⁸⁹ This agreement soon lost its relevance as Xi decided to pursue his China Dream and more aggressive diplomacy, and relations were complicated by the victory of Donald Trump in the 2016 US presidential election. The vulnerabilities of information and communication technologies and services to foreign actors, notably, China, are exposed and felt first by the US, and then the EU.

On 15 May 2019, US President Donald Trump issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain wherein he found that 'foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services [...] in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.'⁹⁰ He further found that the unrestricted acquisition, or use in the US, of information and communication technologies or services by foreign adversaries 'constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States'.⁹¹ President Trump thus declared a national emergency with regards to that threat and ordered a halt to transactions on information and communication technologies, or services with foreign adversaries.⁹² With this order, the participation of Huawei, a giant China telecom supplier, in US information and communication technologies and services have been effectively excluded.

Given the critical role of Huawei in the fifth-generation (5G) communications infrastructure and its close relations with the Chinese military, the US has strengthened its efforts to contain Huawei. Internally, on 16 May 2019, the Bureau of Industry and Security (BIS) of the Department of Commerce announced its decision to add Huawei and its sixty-eight non-US affiliates onto the Entity List of the Export Administration Regulations (EAR) as the BIS found that there was 'reasonable cause to believe that Huawei has been

⁸⁸ The statement of the Ministry of Defense on the Decision of the US Department of Justice in Filing a Charge against Chinese Soldiers (国防部新闻发言人耿雁生就美司法部起诉中国军人发表谈话), 20 May 2014, available at <<http://news.mod.gov.cn>>.

⁸⁹ On this agreement, see, e.g. Gary Brown and Christopher D. Yang, 'Evaluating the US-China Cybersecurity Agreement', *The Diplomat*, 19 January 2017, available at <<https://thediplomat.com/>>.

⁹⁰ Executive Office of the President, Securing the Information and Communications Technology and Services Supply Chain, 15 May 2019, 84 Federal Register 22689.

⁹¹ Executive Office of the President (n. 90).

⁹² Executive Office of the President (n. 90), Sect. 1.

involved in the activities contrary to national security or foreign policy interests of the United States'.⁹³ Externally, the US has exercised a number of foreign policy instruments encouraging or coercing its allies to exclude Huawei from their telecommunications networks.

Built upon existent efforts in enhancing security in critical information and communication infrastructure and containing Huawei, the US intends to collaborate with its allies to form a coalition of trusted partners and establish a clean network, rooted in 'internationally accepted digital trust standards and is a reflection of our commitment to an open, interoperable, and secure global Internet based on shared democratic values and respect for human rights',⁹⁴ and covering clean carriers, stores, apps, cloud services, and cables. 'The Clean Network initiative is a comprehensive effort to address the long-term threat to data privacy, security, and human rights posed to the free world from authoritarian malign actors.'⁹⁵ The Clean Network initiative, if implemented successfully, would lead to a two-speed or divided information and communication network between liberal democracies and authoritarian regimes, China in particular.

However, even though the Trump Administration sees economic dependence on China as a threat to US national security and the threat of China's potential exploitation of the vulnerabilities in information and communication technologies and services as a national emergency, the US has been cautious to avoid the term Internet sovereignty or its relevant variations. That said, in Trump's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, a section on Internet freedom and governance supporting multi-stakeholder process, nearly made it into the final text, being edited out of the final version.⁹⁶ Similarly, whereas President Trump issued an Executive Order on Preventing Online Censorship, 'Internet freedom', the underlying value sustaining the US Internet policy, is not mentioned.⁹⁷ This reflects a shift in the Trump Administration's attitude toward cyber governance.

In contrast to the Trump Administration's resolute antipathy towards China, the EU's position is rather ambiguous on a number of measures to

⁹³ Bureau of Industry and Security, Commerce. Addition of Entities to the Entity List, 16 May 2019, 84 Federal Register 22961.

⁹⁴ U.S. Department of State, 'The Clean Network Safeguards America's Assets (Fact Sheet)', 11 August 2020, available at <<https://www.state.gov>>.

⁹⁵ U.S. Department of State (n. 94).

⁹⁶ Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', Aegis Paper Series No. 1703 (Hoover Institution), 2.

⁹⁷ White House, Executive Order on Preventing Online Censorship, 28 May 2020. See the Remarks of Hillary Clinton, former Secretary of State, on Internet Freedom, 21 January 2010, available at <<https://2009-2017.state.gov>>.

strengthen cybersecurity, both at the EU- and Member State-level. The EU firstly established the European Union Agency for Cybersecurity (ENISA) through Regulation (EC) No 460/2004, the latest revision of Regulation (EU) 2019/881 that sets up a cybersecurity certification scheme for information and communications technologies.⁹⁸ Before this revision, it also adopted Directive 2016/1148 of the European Parliament and the Council concerning measures for common, high-level security of networks and information systems across the Union (the 'NIS Directive'), which obliges the Member States to identify operators of essential services and aims to pursue minimum level of harmonisation in safeguarding security of network and information systems.⁹⁹ Moreover, the European Commission published its recommendation on cybersecurity of 5G networks in 2019.¹⁰⁰ For the ENISA's part, it updated the Guideline on Security Measures under the European Electronic Communications Code (EECC),¹⁰¹ released 5G Supplement to the Guideline on Security Measures under the EECC,¹⁰² and published NIS investment reports based on survey of 251 organisations in France, Germany, Italy, Spain, and Poland.¹⁰³ However, these measures relate largely to coordination and exchange of information among Member States, but fail to address cybersecurity in a strategic way. Crucially, the EU's position on Huawei is not yet defined. 'The EU finds itself squeezed between an emergent China and a US fighting to retain its global tech supremacy.'¹⁰⁴

With some hesitation, the EU, or at least some of its Members States, decided to join with the US in safeguarding cybersecurity. On 23 September 2019, on the side-lines of the General Debates of the UN General Assembly, 21 of 28 EU Members States, in conjunction with the US, issued a Joint Statement on Advancing Responsible State Behaviour in Cyberspace. The statement, without naming China, calls out irresponsible cyber behaviour targeting critical infrastructure and citizens, undermining democracies and international institutions and organisations, and undercutting fair competi-

⁹⁸ Regulation (EU) 2019/881 of The European Parliament and of The Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 of 7 June 2019 on (Cybersecurity Act), OJ L 151/15.

⁹⁹ OJ L 194/1, 19 July 2016.

¹⁰⁰ Commission Recommendation of 26 March 2019, Cybersecurity of 5G networks, C (2019) 2335 final, Strasbourg, 26 March 2019.

¹⁰¹ ENISA, Guideline on Security Measures under the EECC, December 2020, 3rd edn, available at <<https://www.enisa.europa.eu>>.

¹⁰² ENISA, 5G Supplement-to the Guideline on Security Measures under the EECC, December 2020, available at <<https://www.enisa.europa.eu>>.

¹⁰³ ENISA, NIS Investment Reports, December 2020, <<https://www.enisa.europa.eu>>.

¹⁰⁴ European Political Strategy Centre (n. 75), 14.

tion in the global economy through cyber theft and cyber espionage, and called for 'safeguarding the benefits of a free, open, and secure cyberspace for future generations'.¹⁰⁵ The coordinated action of the Member States of the EU foreshadows the EU's realisation of its vulnerability to cyberattacks, which eventually led to the joint communication on *The EU's Cybersecurity Strategy for the Digital Decade*.¹⁰⁶ The European Commission and High Representative for the Common Foreign and Security Policy see cybersecurity as integral part of European security and propose three dimensions of the EU cybersecurity: (1) resilience, technological sovereignty, and leadership, (2) building operational capacity to prevent, deter, and respond, and (3) advancing a global and open cyberspace.¹⁰⁷ Most notably in this joint communication is its global dimension. On the one hand, the EU aims to work with international partners to advance and promote a global, open, stable, and secure cyberspace where international law and voluntary non-binding norms, rules, and principles of responsible state behaviour are respected.¹⁰⁸ On the other hand, the joint communication cautions that 'increased global connectivity should not lead to censorship, mass surveillance, data privacy breaches and repression against civil society, academia and citizens'.¹⁰⁹ In this connection, the promotion of human rights and fundamental freedoms online is critical and will be addressed below.

d) Human Rights

The divergent views on freedom of information vis-à-vis privacy against corporate collection on personal information are the underlying rationale that results in the different attitudes of the US and EU on global internet governance. Whereas internet freedom may arguably be upheld as a human right,¹¹⁰ where the boundary of such freedom lies and how to reconcile and balance internet freedom/freedom of information and other human rights and public interests are the challenges facing sovereign states or regional integration organisations in this digital society. The US in its external (trade) agreements promote the free flows of data and information, which dictates

¹⁰⁵ U.S. Department of State, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', Other Release, 23 September 2019, available at <<https://www.state.gov>>.

¹⁰⁶ Joint Communication to the European Parliament and to the Council: the EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020.

¹⁰⁷ Joint Communication to the European Parliament and to the Council (n. 106), 4.

¹⁰⁸ Joint Communication to the European Parliament and to the Council (n. 106), 20.

¹⁰⁹ Joint Communication to the European Parliament and to the Council (n. 106), 21.

¹¹⁰ See, e.g. Daniel Joyce, 'Internet Freedom and Human Rights', EJIL 26 (2015), 493-514 (493).

the contracting parties, subject to limited exception, not to ‘prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person’.¹¹¹ By contrast, the EU, in accordance with the European Charter of Fundamental Rights and General Data Protection Regulation (GDPR);¹¹² sets out the default position to prohibit data flows out of the EU unless similar degree of protection of personal information is ensured. In the past decade, three agreements between the US and EU (passenger name record, safe harbour, and shield) were held unconstitutional due to the insufficiency of US human rights protection). Therefore, the different weight endorsed to internet freedom and freedom of information on the one hand, and privacy and data protection on the other by the US and the EU is reflected in their respective regulatory approaches on cyber governance. Of greater relevance to this paper is privacy and data protection, which the EU relies on to defend its data sovereignty and this is one of the key divergences between the perceptions of the US and EU on cyber governance.

The GDPR recognises the threat posed to the protection of personal data arising from cross-border flows of personal data,¹¹³ and dictates that in cases of personal data transferred to controllers, processors, or other recipients in third countries or to international organisations, the level of protection of natural persons ensured by the GDPR is not to be undermined.¹¹⁴ Therefore, the GDPR sets up a default position that any transfer of personal data to a third country or an international organisation, subject to other provisions thereof, can only take place when the conditions laid down in Chapter V of the GDPR are complied with by the controllers and processors.¹¹⁵ The legal effect arising from this provision is that unless equivalent level of protection on personal data is ensured, its cross-border transfer is prohibited, introducing a key feature of data sovereignty.

The incompatibility of the US legal regime on privacy and personal information with the EU data protection standard has given rise to several disputes, including *Passenger Name Records Agreement*,¹¹⁶ *Schrems I* on safe

¹¹¹ Art. 19.11.1 UMSCA and Art. 11.1 US-Japan Digital Trade Agreement.

¹¹² See generally, Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler(eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press 2020).

¹¹³ Recital 2, GDPR.

¹¹⁴ Recital 3, GDPR.

¹¹⁵ Art. 44, GDPR.

¹¹⁶ Joined cases *European Parliament v. Council of the European Union* (C-317/04) and *Commission of the European Communities* (C-318/04), judgement of 30 May 2006, ECLI:EU:C:2006:346.

harbour decision,¹¹⁷ and *Schrems II* on shield decision.¹¹⁸ The main thrust of this series of decisions basically relates to the delicate balance between national security, public interest, or law enforcement, and individual rights on data protection; the Court of Justice of the European Union (CJEU) ruled in all three cases that the transfer of personal data from the EU to US is not permissible as an equivalent level of protection is not ensured in the US legal system and thus poses a threat to the personal information of EU citizens.

As the CJEU declares in *Schrems II*, ‘the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter [of Fundamental Rights of the European Union] [...]. The same is true of the retention of personal data and access to that data with a view to its use by public authorities.’¹¹⁹ The CJEU nonetheless cautions that such rights are not absolute rights, but must be considered in relation to their function in society.¹²⁰ The CJEU holds that ‘any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms’,¹²¹ and the principle of proportionality shall guide this limitation. The CJEU thus arrives at the conclusion that the privacy shield decision does not comply with the requirements of the GDPR and Charter as Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333 excessively interfere individual rights and undermine protection of personal data.¹²²

The reasoning of the CJEU marks a sharp contrast with the position of the US, in particular under the Trump Administration. Whereas the US places great weight on national security and less on data protection obligations, the CJEU emphasises the role of the Charter in regulating cross-border transmission of personal data and the importance of principle of proportionality in constraining such regulation. Seen from this perspective, the reason for preventing cross-border transfer of personal information and localising of data within the EU is to ensure the high degree of data protection enjoyed under the European legal order is not undermined through its export to third countries.

¹¹⁷ Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) in the proceedings *Maximillian Schrems v. Data Protection Commissioner (Schrems I)*, judgement of 6 October 2015, case no. C-362/14, ECLI:EU:C:2015:650.

¹¹⁸ Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) in the proceedings *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*, judgement of 16 July 2020, case no. C-311/18, ECLI:EU:C:2020:559.

¹¹⁹ CJEU, *Schrems II* (n. 118), para. 171.

¹²⁰ CJEU, *Schrems II* (n. 118), para. 172.

¹²¹ CJEU, *Schrems II* (n. 118), para. 174.

¹²² CJEU, *Schrems II* (n. 118), para. 184.

IV. Concluding Remarks: The Territorial Turn and Two-Speed Internet

The rise of emergent countries in general, and China in particular, has challenged the liberal global Internet, which evolved in a multi-stakeholder environment. In territorialising cyberspace and translating the concept of national sovereignty into cyberspace, China has introduced a concept of Internet sovereignty designed to serve its domestic needs: the maintenance of regime stability by controlling information flows. The concept of Internet sovereignty has also an external dimension, for China aims to transform the multi-stakeholderist cyber governance model into a multilateral one, wherein countries enjoy sovereignty and the ultimate authority to shape their online spaces. As a country that guards sovereignty jealously, China's preference for bringing sovereignty into the cyberspace is not surprising. However, sovereignty is not the last word in debates concerning the future of digital society, for even liberal democracies have advanced ideas of technological or digital sovereignty, and data sovereignty, for their own very different purposes.

This article argues that the proliferation of the notion of Internet sovereignty and its variances can be attributed to four reasons: political ambition, economic value, security concerns, and human rights. A sharp contrast can be seen in the divergences between the EU and the US on the cross-border transfer of personal data, giving rise to several disputes in the CJEU. On the one hand, these disputes illustrate the delicate balance between national security and human rights, and the different weights the EU and US give to these two competing values. On the other hand, the EU's struggle for technological sovereignty also reflects the security threat posed by the digital transformation of society. If the EU aims to persevere its values and ways of life, it has to retain strategic autonomy and technological sufficiency. This reflects a critical change in economic interdependence and a return to economic independence, at least self-sufficiency.

Seen in this light, the sovereignty fever is a symptom reflecting sovereign states' attempt to retain autonomy and control gradually eroded with the digitalisation of societies and economies. The utopia of a borderless and interconnected cyberspace thus loses its charm and the global cyber order is witnessing a territorial turn. China has long established the Great Firewall to control and filter information flows. The EU, in the name of data protection, erects substantial barriers for personal information from transferring outside the Union. Most importantly, in the long race of 5G competition and safeguarding critical information and communication infrastructure, the US and its allies aim to build a Clean Network by bypassing China, which will result

in a two-speed network between liberal democracies and authoritarian regimes, China in particular.

Probing into the future, the trend for territorialising the cyberspace and the ambition to regulate and control information and data flows and retain technological autonomy in the digital society will be intensified as one of the bitter lessons learnt from the global pandemic of COVID-19 is how weak the global supply chain is. Countries thus rush for technological independence and self-sufficiency in the name of technological sovereignty. The global pandemic also exposes the threats of disinformation in the digital age and how to regulate social media becomes a top priority for sovereign states and regional integration organisations. Digital and data sovereignty will be the catchy words for the years to come and the sovereignty fever will persist.

The Role of the Internet in International Law-Making, Implementation and Global Governance

Annalisa Ciampi*

University of Verona, Florence, Italy

annalisa.ciampi@univr.it

Abstract	677
Keywords	678
I. Introduction	678
II. International Law-Making Processes	680
III. Implementation of International Law	683
1. Identification of Customary International Law	685
2. International Responsibility	690
IV. Technological Power as a Leverage of Global Governance	694
V. Concluding Remarks	697

Abstract

This paper delves into influence of the internet on international law and global governance, a phenomenon that increased incrementally over the last decade before the COVID-19 emergency precipitated it.

It posits that the *digital world* birthed whole new ‘territories’ where the practice of states and other actors is recorded and displayed, but it also exists independently from the physical realm. With respect to *law-making*, the internet acts as both a sounding board for, and an originator of, international practice. New technologies and social networks have also certainly increased the availability of information to governments and the public regarding violations of international norms. Yet, they have created a new – online – environment in which internationally wrongful acts can be committed. This further qualifies, yet does not make less significant, the relevance of the internet for the *implementation* of international law.

* Harvard LL. M.; Ph. D. University of Rome La Sapienza; Professor of International Law, University of Verona; former UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association. The author would like to thank the Editors of this HJIL issue for their invitation to contribute, and the anonymous HJIL reviewer for his/her invaluable comments and suggestions. This article was developed by the author within the research activities of the Team ‘Processi decisionali e fonti del diritto’, within the Project of Excellence of the Law Department of the University of Verona Diritto, Cambiamenti e Tecnologie.

The paper further submits that technological power has become a fundamental force of leverage in *global governance*, akin to economic, military, and political might for states and a wide range of non-state actors alike. Big Tech companies and other corporations but also civil society, social and political groups, and individuals are all potential stakeholders participating formally and informally (or to be included) in the sharing of power.

Notwithstanding the difficulty to articulate a concept that comprehensively rationalises the impact of the internet on the processes and structures of international law and governance, the paper highlights a gap between the theory and practice of international law and offers a contribution in this direction.

Keywords

internet – international law-making – implementation of international law – customary international law – global governance – technology’s power

I. Introduction

To date, legal scholarship has generally focused on the ways international law governs opportunities and dangers arising from ‘the internet’.¹ Little attention, if any, has been given to the question of how new technologies have changed traditional international law-making processes as well as the implementation of international rules. Hence, this paper does not dwell on the role that international law plays for ‘the internet’.² It rather aims to understand how the internet has changed the very concept, nature and internal structures of international law. This question is addressed by distinguishing between

¹ The term ‘the internet’ is here and henceforth used to refer to all ‘Internet Protocol (IP)-based services’, as defined by Matthias K. Kettemann, *The Normative Order of the Internet. A Theory of Rules and Regulations Online* (Oxford: Oxford University Press 2020).

² On *Internetvölkerrecht* (‘international internet law’ or ‘international law of the internet’) see the seminal work by Antonio Segura-Serrano, ‘Internet Regulation and the Role of International Law’ in: Armin von Bogdandy and Rüdiger Wolfrum (eds), *Max Planck UNYB* (online edn, Leiden: Koninklijke Brill 2006), 191-272; and Michael N. Schmitt, ‘Taming the Lawless Void: Tracking the Evolution of International Law Rules on Cyberspace’, *Texas National Security Review* 3 (2020), 32-47; In the extensive literature on the internet and international law, see also Jack Goldsmith, ‘Unilateral Regulation of the Internet: a Modest Defence’, *EJIL* 11 (2000), 135-148; Franz C. Mayer, ‘Europe and the Internet: the Old World and the New Medium’, *EJIL* 11 (2000), 149-169; Yochai Benkler, ‘Internet Regulation: a Case Study in the Problem of Unilateralism’, *EJIL* 11 (2000), 171-185; Thomas Schultz, ‘Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface’, *EJIL* 19 (2008), 799-839; Martha Finnemore and Duncan B. Hollis, ‘Constructing Norms for Global Cybersecurity’, *AJIL* 110 (2016), 425-479; Kal Raustiala, ‘Governing the Internet’, *AJIL* 110 (2016), 491-503; Eyal Benvenisti, ‘Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?’, *EJIL* 29 (2018), 9-82.

international law-making and implementation of international law, the latter including ascertainment, interpretation, and international responsibility.

As we shall see, information and communication technologies have mostly indirectly affected the procedure for the conclusion of treaties. With respect to the impact of the internet on the formation of international rules, therefore, the focus will be on international customary law. Moreover, because the interactions between law-making and implementation are particularly strong in relation to customs, the analysis will also show that the impact of the internet on implementation is stronger on customs than on treaties. Paragraphs II and III provide insights, but they do not tackle directly question of legitimacy of the primary sources of international law as a result of the internet's role for international law and, in particular, for customary international law.³ They highlight, however, the existence of a gap between the theory and practice of international law and aim to offer a contribution in this direction.

Paragraph II submits that the *digital realm* has birthed whole new 'territories' where the practice of states and other actors is recorded and displayed, but it also exists independently from the physical realm. It does not only provide for a wide range of materials that may serve as *evidence of lex lata* but it also offers a range of normative materials that global actors, in the ordinary course, use and treat as customary international law *de lege ferenda*. With respect to *law-making*, therefore, the internet acts as both a sounding board for, and an originator of, international practice.

Albeit mostly indirectly, the procedure for the conclusion of treaties is also affected by information and communication technologies.

Paragraph III advances the proposition that the internet does not generally contribute to make international law more effective.

The internet has certainly increased the availability of information regarding breaches of international law – particularly but not exclusively human rights violations, as all fields are affected by the pervasiveness of the internet. Yet, to more information available to governments and the public has not necessarily corresponded a decrease in the violations of international norms or a major advancement in the effectiveness of international law. New technologies and social networks have also created a new – online – environment in which internationally wrongful acts can be committed. This qualifies, but it does not diminish or make less significant, the relevance of the internet for the *implementation* of international law.

While the issue of internet governance *per se* is beyond the scope of this paper, paragraph IV discusses some of the implications of the internet for

³ For a general appraisal of the issue, see Julian Kulaga, 'The Legitimacy of Rules of Customary International Law and the Right to Justification', HJIL 79 (2019), 785-814.

global governance and the socio-legal changes brought about by it. It submits that technological power has become a fundamental force of leverage in *global governance*, akin to economic, military, and political might for states and a wide range of non-state actors. The interface between international law and the internet affects the relationships and the power balance between the Global South and Global North in terms of positive law and participation in processes of norm development. Moreover, Big Tech companies and other corporations but also civil society, social and political groups, and individuals are all potential stakeholders participating formally and informally in the sharing of power – or to be included therein.

Paragraph V draws some preliminary conclusions and attempts to rationalise the impact of the internet on global governance and the formation and implementation of international law. That the impact of the internet particularly on the making of international law remains elusive, and hard to articulate as a concept, does not make this work's contribution to the effort less important. The changes brought by the internet to the processes and structures of international law and global governance are real and only bound to become more evident in the future. This phenomenon has been going on for several decades now, although modern technologies increased incrementally over the last decade. The COVID-19 emergency precipitated it.

II. International Law-Making Processes

Legal scholarship has long acknowledged the increase in the number and frequency of multilateral forums where States meet to develop or discuss new rules of written international law. There is wide recognition that the intensification of practice within international organisations and conferences (such as the United Nations General Assembly's Sixth Committee, codification conferences, etc.) has increased the adoption of multilateral treaties.

States have also 'many more occasions than they used to have to express views as to customary international law. This has increased the quantity of what States say'.⁴ Information and communication technologies therefore

⁴ Tullio Treves, 'Customary International Law' in: Rüdiger Wolfrum (ed.), *MPEIL* (online edn, Oxford: Oxford University Press 2006), para. 11. In his dissenting opinion in the ICJ, *South West Africa Cases* (Ethiopia v. South Africa), back in 1966 Judge Tanaka already argued that when a court is trying to discern whether a certain customary norm of international law exists, General Assembly Resolutions can be used as evidence of general practice, suggesting that the General Assembly can accelerate the formation of customary law by serving as a forum in which a state 'has the opportunity, through the medium of the organization, to declare its position to all members of the organization and to know immediately their reaction on the same matter' (ICJ Reports 1966, 248, 291-293 [291]).

have also contributed to the acceleration of the formation of customary rules in various fields of international law.⁵

What has gone largely unnoticed, however, is the qualitative, rather than quantitative, changes brought about by the internet in relation to international law-making processes. This phenomenon is directly relevant to the formation of customary rules.

The impact of the internet is widespread and could probably be detected in relation to most, if not all, general rules. For the purposes of this essay, two instances will show the interaction between international law-making processes and the internet.

Perhaps the most compelling evidence of the power of the internet arose out of ‘September 11’, when broadcast images of the smoking twin towers backed President Bush’s declaration of ‘no safe havens for terrorists’ and the US right of intervention, i.e. the right to target terrorists wherever they are found. The internet did not only show the whole world the terrorist attack against United States at the same time as it was happening. It was in and by itself one of the components of the armed response by the United States leading a coalition of the willing.

As a result, no one did at the time – or would nowadays – seriously challenge that on 11 September 2001 the US suffered an armed attack legitimately triggering the exercise of the right of individual and collective self-defence, within the terms of Article 51 United Nations (UN)-Charter and international solidarity clauses drawing upon it.

Hadn’t we all witnessed the twin towers falling and disintegrate carrying with them the life of almost three thousand men and women and leaving more than six thousand others injured, would North Atlantic Treaty Organization (NATO) allies have immediately issued a declaration invoking NATO’s Article 5 mutual assistance clause? Would statements of solidarity have been made at all corners of the world? Would the US and the international community’s response have been the same?

Actions happened on the ground, declarations in international forums and state chancelleries. But they also took place through and on the *virtual space* of the internet.

It is submitted that the internet played a *pivotal role* in the decision-making and law-making processes which led to the encapsulation of terrorist attacks in the notion of ‘armed attack’ for the purposes of self-defence, and to the expansion of its legitimate targets. It is further submitted that this role cannot be described merely in terms of an *accelerator* of processes already

⁵ See, e.g. Luigi Condorelli, ‘Consuetudine internazionale’, in: Rodolfo Sacco (ed.), *Digesto delle Discipline Pubblicistiche III* (Torino: Utet 1989), 490-512.

underway and/or of an *amplifier* of state and other actors' behaviours. The internet did affect the very formation, and the content, of international law. A further instance, taken from the most recent practice, will help to enlighten this dimension of the internet's role on international law-making.

The COVID-19 emergency, even before it unleashed its catastrophic economic and social consequences, raised in a dramatically topical way the problem of the *existence* of an international duty of states to cooperate with one another in the fight to contain the pandemic.

In the very aftermath of the COVID-19 outbreak, we witnessed teams of medical experts departed from China to be deployed to Russia and Western Europe, as well as from Russia to Italy and other European Union countries. Accounts spread over the internet. The internet did not only serve the purpose of political propaganda for the states plastically and physically deploying their men and means on the territory of other states. By offering instances of cooperation, the internet provided the evidence needed to state that a general obligation to cooperate in the fight against the pandemic existed and was effective. But it also played a more substantive role – a constitutive one, so to say.

The internet provided a platform – the *virtual space* – which added itself to the material space on the ground (where real men and means were deployed). Unlike the latter, the virtual space is visible worldwide and can be viewed simultaneously and at multiple times at all corners of the world.

The 'digital realm birthed whole new territories'⁶ where the practice of states and other international actors is recorded and displayed for all to see, but it is also given a distinct existence, independently from the physical realm. The internet acts as both a sounding board for, and an *originator* of, international practice.⁷

It is submitted that digital behaviours are a form of international practice that can *generate* customary law, even in the absence of a corresponding practice outside the internet and the digital realm generated by it.⁸

In contemporary international setting, international practice is not simply spread through recourse to modern technologies of written and visual representation. The internet does not only enhance the relevance of a state behav-

⁶ The expression is taken from Shoshana Zuboff, *The Age of Surveillance Capitalism* (London: Profile Books Ltd 2009), 4.

⁷ The term 'international practice' is used here and elsewhere as encompassing the two traditional components of customs (*usus* and *opinio juris*), on which see *infra*, III.1.

⁸ And the often-repeated criticism *vis-à-vis* UN General Assembly resolutions – that they can only reflect *opinio juris sive necessitatis* but may not be constitutive of state practice – should not apply to digital behaviours – unless one can point to a divorce between digital behaviour and 'real' world state practice.

ious with the corresponding *opinio juris*.⁹ The internet advances knowledge about existing rules, but it also influences current and future developments of international law.

What has been said about the *virtual* deployment of doctors and medical equipment may apply to other state behaviours during the pandemic. And similar considerations could also be extended with suitable contextualisations to many rules of customary international law.

Because international practice is directly relevant only to the formation of international customs, the impact of the internet on the conclusion of treaties is less evident. Nevertheless, it exists and can be traced at least in the following two respects.

First of all, the so-called ‘virtual diplomacy’ bears its most immediate fruits on treaties, rather than customs. Zoom and other platforms have taken the place of diplomatic conferences as we traditionally had known them for the past two centuries. In this respect, the use of information technologies to help conduct international relations activities has profoundly affected the *procedure* for the conclusion of treaties – a development only accelerated by the COVID-19 emergency.

Moreover, and most importantly, there is an osmosis between the formation of customs and the conclusion of treaties.¹⁰ Treaties may be concluded to codify or in derogation of general rules. Subsequently, such treaties can provide guidance on the content of customary international law. Additionally, treaties can expand obligations of states in comparison with customary international law. Sometimes treaty rules precede the emergence of corresponding customs. Or treaty practice can simply help to consolidate and/or clarify the content of customary rules.

Treaty making processes and the formation of customary international law are intertwined in many and multiple ways. In so far as the internet and the digital realm affect the existence of customs, therefore, they also have an impact, depending on the context and the circumstances, on treaties.

III. Implementation of International Law

For the purposes of this article, implementation refers to the identification of international rules as well as to international responsibility, dispute-settlement, and enforcement.

⁹ The two traditional components of customs (*usus* and *opinio juris*), generally referred to here and elsewhere as ‘international practice’, are examined *infra*, III.1.

¹⁰ See Treves (n. 4), para. 92: ‘What increasingly characterizes contemporary customary international law is the strict relationship between it and written texts.’

Identification encompasses both rule ascertainment and interpretation. Interpretation is commonly understood as the process of determining the content and scope of rules, while a rule ascertainment is concerned with whether the rule exists – for instance, whether an international agreement exists. Now, while the existence of treaty rules is generally undisputed, in relation to customary international law, rule ascertainment and content determination are tightly intertwined and may be difficult to distinguish.¹¹

Another point that needs to be clarified concerns the area of overlap and interconnection between formation, on the one hand, and identification of international law, on the other hand. Again, while the two concepts are interlinked also with respect to treaties, the interrelations are particularly strong in relation to customary international law.

‘Formation and Evidence of Customary International Law’¹² was the original title and theme of the topic dealt with by the International Law Commission (ILC) between 2012 and 2018, before it decided, in 2013, to eliminate from the title ‘formation’ and to substitute ‘evidence’ with ‘identification’.¹³ ‘Identification of Customary International Law’ is the title finally retained by the ILC and the output of that ILC’s work, the ‘Draft conclusions on identification of customary international law’,¹⁴ concern the methodology for identifying rules of customary international law. While no instrument was concluded under the auspices of the UN on their basis, the ILC Draft conclusions offer a practical guidance on how the existence and content of customary rules are to be determined but also, notwithstanding their changed title, on the formation processes of customary international law.

¹¹ There are cases where the existence of a rule is undisputed but where its content is imprecise or disputed, but usually both the existence and the content of a customary international law rule need to be determined. Very few rules of customary international law are clear and straightforward. Customary international humanitarian law is a good example: A study by the International Committee of the Red Cross provided a list of detailed rules (the prohibition of indiscriminate attack, precautions, and other fundamental principles of humanitarian law) that can be considered as customary rules. Also, certain fundamental aspects of the law on the use of force (such as the right to self-defence and the prohibition of interventions) are reflected in customary international law with more or less clear meaning.

¹² ILC, ‘Report on the Work of its Sixty-fourth Session’, (2012) *General Assembly Official Records*, Sixty-seventh Session, Supplement No. 10 (UN Doc. A/67/10), 108, para. 157.

¹³ ILC, ‘Report on the Work of its Sixty-fifth Session’, (2013) *General Assembly Official Records*, Sixty-fifth Session, Supplement No. 10 (UN Doc. A/68/10), 93, para. 64. On the initial phase of the work of the ILC on this topic, see Lorenzo Gradoni, ‘La Commissione del diritto internazionale riflette sulla rilevazione della consuetudine’, *Riv. Dir. Int.* 97 (2014), 667–698.

¹⁴ ILC, ‘Identification of Customary International Law: Text of the draft conclusions as adopted by the Drafting Committee on second reading’, (2018) ILCYB, Vol. II, Part One (UN Doc. A/CN.4/L.908, <<http://legal.un.org>>). For an analytical guide to the work of the ILC on the topic of the identification of customary international law, see <<http://legal.un.org>>.

As the ILC's commentary to draft conclusion 1, adopted on first reading in 2016, notes:

'Dealing as they do with the identification of rules of customary international law, the draft conclusions do not address, directly, the processes by which customary international law develops over time. Yet in practice identification cannot always be considered in isolation from formation; the identification of the existence and content of a rule of customary international law may well involve consideration of the processes by which it has developed. The draft conclusions thus inevitably refer in places to the formation of rules; they do not, however, deal systematically with how rules emerge, or how they change or terminate.'¹⁵

Identification and formation are obviously not the same thing, but they are in many ways closely related, for it would be impossible to proceed to the identification of customs, without gaining at least a general conception of its formation. In this respect, the analysis the follows sheds light also on the internet's role in relation to international law-making, as outlined in the previous paragraph.

In particular, the requirement – for the identification of customary international law – to ascertain 'a general practice' that is 'accepted as law' reflects the fact that rules of customary international law evolve through a general practice and *opinio juris*. In other words, the two constituent elements of customary international law are also the twin criteria for its identification,¹⁶ as we shall now see.

The next paragraph reviews the scholarly debate about the nature of customary international law and assesses the content of the Draft conclusions, with a view to exploring the role played by the internet – in the ILC's view – in the identification of customary rules. The subsequent paragraph examines case studies of implementation of international rules through information and communication technologies and draws some preliminary conclusions on the relevance of the internet for the purposes of the implementation – both in the theory and practice – of international law.

1. Identification of Customary International Law

According to its most widely accepted definition, an international custom arises out of a general practice (*usus*) that is accepted as law (*opinio*

¹⁵ ILC, 'Report on the Work of its Sixty-eighth Session', (2016) *General Assembly Official Records*, Sixty-eighth Session (UN Doc. A/71/10), 81, para. 4 of Commentary to Conclusion 1.

¹⁶ Michael Wood, 'The Evolution and Identification of the Customary International Law of Armed Conflict', *Vand. J. Transnat'l L.* 51 (2018), 727-736 (728).

juris).¹⁷ It thus requires a repeated behaviour, sufficiently widespread and representative as well as consistent, undertaken with a sense of legal right or obligation, i.e. accompanied by the belief that that behaviour is mandated by law.

While commentators have taken very different positions on the connection between acceptance and *opinio juris*, it is generally recognised that practice does not need to be constant or absolutely uniform for a custom to be established.¹⁸ To the contrary, a breach may even reinforce the existence of the rule; this happens when the actor infringing the rule seeks to justify its behaviour by invoking an exception, or because of possible circumstances precluding wrongfulness, in the particular case.¹⁹ It follows that a state can be bound by customary international law even if it has not agreed to or accepted the rule.²⁰

Implied in the notion of custom is also the element of time. The requirement of time is a relative one: the more widespread is the practice, the less

¹⁷ See Art. 38 para. 1 lit. b) ICJ-Statute, which defines ‘international custom, as evidence of a general practice accepted as law’. For a recent, thorough critique of this traditional approach – espoused here –, as a ‘rulebook conception’ of international customary law, which ‘does not accurately describe the range of normative materials that global actors, in the ordinary course, use and treat as customary international law’, see Monica Hakimi, ‘Making Sense of Customary International Law’, *Mich. L. Rev.* 118 (2020), 1487-1537 (1487).

¹⁸ See Anthea Elisabeth Roberts, ‘Traditional and Modern Approaches to Customary International Law: A Reconciliation’, *AJIL* 95 (2001), 757-791 (773): ‘deducing modern custom purely from *opinio juris* can create utopian laws that cannot regulate reality. For a reaffirmation that *opinio juris* and acceptance are two distinct, different but correlative concepts and phenomena, see László Blutman, ‘Conceptual Confusion and Methodological Deficiencies: Some Ways that Theories on Customary International Law Fail’, *EJIL* 25 (2014), 529-552, according to whom, however, a practice’s ‘generality suggests that, in international interactions, the number or weight of the state actions belonging to this class overwhelmingly exceed the number or weight of state actions that are inconsistent with this pattern. [...] In this sense, general practice is not material or objective in nature’ (543).

¹⁹ ICJ, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States), merits, judgement of 27 June 1986, ICJ Reports 1986, 14, 88, para. 186: ‘It is not to be expected that in the practice of States the application of the rules in question should have been perfect, in the sense that States should have refrained, with complete consistency, from the use of force or from intervention in each other’s internal affairs. The Court does not consider that, for a rule to be established as customary, the corresponding practice must be in absolutely rigorous conformity with the rule. In order to deduce the existence of customary rules, the Court deems it sufficient that the conduct of States should, in general, be consistent with such rules, and that instances of State conduct inconsistent with a given rule should generally have been treated as breaches of that rule, not as indications of the recognition of a new rule. If a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State’s conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule.’

²⁰ On the existing tension between the principle of consent and non-consensual international rulemaking, see Andrew T. Guzman and Jerome Hsiang, ‘Some Ways that Theories on Customary International Law Fail: A Reply to László Blutman’, *EJIL* 25 (2014), 553-559.

time is needed for the formation of an international custom. As with general practice, there exists no agreed upon formula for identifying with precision 'how much time must transpire to generate a rule of customary international law'.²¹ Recent developments show that customary rules may come into existence rapidly.²²

Following the classical two-element approach, the ILC Draft conclusions state that it is not sufficient to identify a general practice; it is necessary to verify that this practice be accompanied or motivated by a belief that it is mandated (or permitted) under international law.²³ The requirement that a general practice be accepted as law (*opinio juris*) means that the practice in question must be undertaken with a sense of legal right or obligation. It is acceptance as law (*opinio juris*) that distinguishes a general practice, as an element of customary international law, and other conduct that, even if general, is not creative, or expressive, of customary international law.²⁴ The requirements of practice and *opinio juris* are addressed separately.²⁵

²¹ Michael P. Scharf, Milena Sterio and Paul R. Williams, *The Syrian Conflict's Impact on International Law* (Cambridge: Cambridge University Press 2020), 50.

²² On the rapid formation of customary rules in times of rapid flux – explained through the 'Grotian Moment' concept, see Michael P. Scharf, *Customary International Law in Times of Fundamental Change: Recognizing Grotian Moments* (Cambridge: Cambridge University Press 2013) as well as Michael P. Scharf, 'Accelerated Formation of Customary International Law', *ILSA J. Int'l & Comp. L.* 20 (2014), 305-341: In the cases of Nuremberg, the continental shelf, and space law, the Grotian Moments led to rapid formation of fundamental principles of customary international law: 'the case studies indicate that in addition to responding to technological, economic, or societal change, Grotian Moments are in part made possible by geopolitical realignment, often following war' (338). The 'Grotian Moment' concept is to be distinguished from the controversial notion of instant custom: 'Grotian Moments represent instances of rapid, as opposed to instantaneous, formation of customary international law. Grotian Moments require some underpinning of State practice, whereas advocates of the concept of instant custom argue that customary law can form in the absence of State practice' (340). On so-called 'instant' international customary law, see Bin Cheng, 'United Nations Resolutions on Outer Space: "Instant" International Customary Law?', *IJIL* 5 (1965), 23-48, reprinted in Bin Cheng, *Studies in International Space Law* (Oxford: Oxford University Press 1997), 125; Diego Germán Mejía-Lemos, 'Some Considerations Regarding "Instant International Customary Law", Fifty Years Later', *IJIL* 55 (2015), 85-108.

²³ See ILC Draft conclusion 2: 'To determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (*opinio juris*).'

²⁴ Draft conclusion 8 states that practice 'must be sufficiently widespread and representative, as well as consistent. Provided that the practice is general, no particular duration is required.' Draft conclusion 9 further provides: 'The requirement, as a constituent element of customary international law, that the general practice be accepted as law (*opinio juris*) means that the practice in question must be undertaken with a sense of legal right or obligation. A general practice that is accepted as law (*opinio juris*) is to be distinguished from mere usage or habit.'

²⁵ See Draft conclusion 3, para. 2: 'Each of the two constituent elements is to be separately ascertained. This requires an assessment of evidence for each element.'

Dealing with ‘identification’, the Draft conclusions list a wide range of forms of evidence for each element. Yet, none of the Conclusions or the Commentaries expressly mentions the role of new information and communication technologies or the digital realm. The internet comes into play only indirectly, in relation to the ‘[t]eachings of the most highly qualified publicists of the various nations’, which ‘may serve as a subsidiary means for the determination of rules of customary international law’ (Draft conclusion 14) – a provision included in Part Five under the heading ‘Significance of certain materials for the identification of customary international law’.²⁶

As the Chair of the ILC Drafting Committee clarified:

‘The purpose of this draft conclusion is to address the role of teachings (in French, *doctrine*) as subsidiary means for the identification of customary international law. In following closely the language of Article 38, paragraph 1 (d), of the Statute of the International Court of Justice, it provides that such works may be resorted to as a subsidiary means for determining a rule of customary international law. The term “teachings” is to be understood in a broad sense, *including for instance audiovisual materials*.’²⁷

The ILC might have had in mind, for example, the UN Audiovisual Library of International Law, a permanent collection of lectures on virtually every subject of international law, given by leading international law scholars and practitioners from different regions, legal systems, cultures, and sectors of the legal profession.²⁸ It is a free online international law research and training tool created in 2008 by the Codification Division of the UN Office of Legal Affairs, and maintained by the latter for promoting knowledge of international law, under the UN Programme of Assistance in the Teaching, Study, Dissemination and Wider Appreciation of International Law.

Now, the express acknowledgment that the teachings of scholars may include teachings in ‘non-written’ forms such as audiovisual, is a recognition that new technologies and modern forms of communication are useful *tools*

²⁶ The other ‘materials’ singled out for their particular practical role are: ‘Treaties’ (Draft conclusion 11); ‘Resolutions of international organizations and intergovernmental conferences’ (Draft conclusion 12), and ‘Decisions of courts and tribunals’ (Draft conclusion 13).

²⁷ Statement of the Chair of the Drafting Committee, Mr. Charles Chernor Jalloh, introducing the third report of the Drafting Committee for the seventieth session of the International Law Commission, which concerns the topic ‘Identification of Customary International Law’, 25 May 2018, 15, emphasis added (UN Doc. A/CN.4/L.908, available at <<http://legal.un.org>>). Under Art. 38, para. 1 lit. d) ICJ Statute, ‘judicial decisions and the teachings of the most highly qualified publicists of the various nations [...] are] subsidiary means for the determination of rules of law.’

²⁸ The lectures – organised by subject matter and accompanied by related materials such as lecture outline, presentation slides, references, recommended readings, etc. – are available at <<http://www.un.org>>.

in explicating the law, including international law. Yet, the reference made exclusively in relation to ‘teachings of the most highly qualified publicists’ which are a subsidiary means for determining rules of customary international law, is a lacuna that needs to be addressed.

The internet offers different categories of materials that are frequently invoked in the identification of ‘a general practice’ and ‘acceptance as law’ (*opinio juris*). Even before the outbreak of COVID-19, it had become more and more frequent for international legal scholars to use the internet in lectures and power-point presentations. The pandemic emergency has only accelerated a process already underway – and dramatically so.

Moreover, it is not only academic teachings but the entire life of peoples and nations that has moved, in hitherto unimaginable proportion, from the physical space of the real world to the virtual – but not less real – virtual space of the internet. States, international organisations, non-governmental organisations (NGOs), and other non-state actors, including groups of all sorts and individuals, are on the internet: their actions and inactions, accomplishments and wrongful acts, reactions to events and failures to act; what they do right and what they do wrong; the situations that they address, and the challenges that remain standing and beg for action but are not (or not appropriately) dealt with. All of this is available through the internet, mostly open access, free of charge, worldwide: across countries, cultures, language barriers.

It is commonplace that the proliferation of legal databases and more generally the development of modern technologies have enormously increased the means and speed of communications across the globe and immensely facilitated the task of seeking information about the practices followed by other jurisdictions, governmental and non-governmental organisations, and other actors.²⁹

The recognition of the instrumental value of the internet in spreading knowledge about international law or even the attribution to modern communication and information technologies of an *explanatory* function of international rules, however, fall short of the true impact of the internet on international law. The internet offers a wide range of materials that may serve as *evidence* for the purposes of the identification of customary rules. Also in this respect, the ILC’s work presents a lacuna.³⁰

In addition to being paramount as evidence of *lex lata*, the internet offers a range of *normative materials* that global actors, in the ordinary course, may

²⁹ See Condorelli n. 5.

³⁰ On the obstacles faced by the ILC itself to conduct its own work remotely, in the absence of in-person meetings, through video-conferencing or otherwise, during the pandemic, see Sean D. Murphy, ‘Effects of the COVID-19 Pandemic on the Work of the International Law Commission’, EJIL 114 (2020), 726-728.

use and treat as customary international law *de lege ferenda*. The digital realm *originates* (at least part of the very) behaviours that contribute to the emergence of customary rules. Take, for example, the right of humanitarian intervention: internet related means and activities can be relevant to the question of whether a rule that authorises humanitarian intervention exists and, in the affirmative, under what circumstances.³¹ The first is a question about the existence of the rule, the latter relates to content determination.

The internet plays a role for the purposes of the identification and the formation of customary international law alike, for the two concepts are – as explained above – interrelated.

2. International Responsibility

Even before the advent of the internet, international law offered different examples of the use and relevance of visual technologies in various areas, the pioneering field being international criminal law.

Videos documenting war crimes and other serious human rights breaches have long been used as evidence for the prosecution for international crimes.

In 1945-1946, at the Nuremberg trial – which can be considered as the birth point of international criminal law – the chief prosecutor Justice Jackson showed to the horror of the judges and the press corps, the real footage images of the movies which the British and the American soldiers took from the concentration camp Bergen-Belsen.³²

³¹ In early December 1992, for example, when outgoing U.S. President George H. W. Bush sent the contingent of Marines to Somalia to lead a UN-sanctioned multinational force aimed at restoring order in the conflict-ridden country, as part of a mission called Operation Restore Hope, news media showed pictures and videos of the 1,800 US Marines arriving in Mogadishu. Backed by the U.S. troops, international aid workers were soon able to restore food distribution and other humanitarian aid operations – which were also broadcasted through the internet. Sporadic violence continued, however, including the murder of 24 UN soldiers from Pakistan in 1993. As a result, the UN Security Council authorised the arrest of General Mohammed Farah Aidid, leader of one of the rebel clans. On 3 October 1993, during an attempt to make the arrest, rebels shot down two of the U.S. Army's Black Hawk helicopters and killed 18 American soldiers. As horrified internet viewers watched images of the bloodshed – including footage of Aidid's supporters dragging the body of one dead soldier through the streets of Mogadishu, cheering – President Bill Clinton immediately gave the order for all American soldiers to withdraw from Somalia by 31 March 1994. Other Western nations followed suit.

³² In *Judgment at Nuremberg*, a 1961 American courtroom drama film directed by Stanley Kramer, for the first time a Hollywood director used the real footage images of the movies which the American soldiers took from Bergen-Belsen and inserted them into a feature film in the famous reconstruction of the movie showings at the real Nuremberg trials of 1946. Stanley Kramer actually shot much of the movie on site in Nuremberg, and many of the scenes were filmed in the very same building where the real trial was held. On the re-usage of visual evidence, at the time used as real evidence in the real trial, and now used to shock the movie-going spectators of the feature film, see, for example, <<https://youtu.be/zM4ZQANR0dU>>.

In recent years, digital evidence has taken an increasing role in almost all investigative activities both at the national³³ and international level.³⁴ Images were routinely presented as evidence in trials before the *ad hoc* international criminal tribunals, most notably the International Criminal Tribunal for the former Yugoslavia (ICTY),³⁵ which also undertook a major digitisation project to convert audio-visual recordings of its court proceedings to high-resolution digital video files, as part of its Legacy Strategy.³⁶ Digital evidence is now standard practice before the International Criminal Court (ICC).

The so-called ‘open-source digital evidence’ is a new type of digital evidence: information publicly available, acquired through the Internet, which may include, among others, social media content, images, videos, and audio recordings on websites.³⁷ The internet has changed the value and use of digital evidence. But new methods for information gathering and dissemination have also created significant challenges. Digital information, including from social media, can be biased and manipulated, raising issues of reliability and credibility. Digital evidence to be of use, must be not only discovered, but also verified and authenticated.³⁸

³³ On the handling of digital evidence in national proceedings, see the international standards developed in 2012 (last reviewed and confirmed in 2018) by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to harmonise practices between countries: ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, available at <<https://www.iso.org>>.

³⁴ See Lindsay Freeman, ‘Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials’, ILJ 41 (2018), 283–336; See also Rossella Pulvirenti, ‘Internet and International Criminal Accountability: Towards a Human-Centred Approach’ in: Angelo Jr Golia, Matthias Kettemann, and Raffaela Kunz (eds), *International Law and the Internet* (Baden-Baden: Nomos forthcoming), critically assessing in a human rights perspective how the use of internet has served the goals of international criminal law – retribution, deterrence and restorative justice.

³⁵ The vast archival holdings of the ICTY exceed 9.3 million entries and include photographs, diaries, maps, diagrams, exhumation records, x-rays, radio intercepts, audio recordings, and videotapes. For a sample selection of images presented as evidence in ICTY trials, see <www.icty.org>.

³⁶ The digitisation project will permanently preserve and facilitate public access to the Tribunal’s hearings. The purpose of the preservation and accessibility of the records and archives is to secure a long-lasting and positive impact of the ICTY in the former Yugoslavia and beyond.

³⁷ Nikita Mehandru and Alexa Koenig, ‘Open Source Evidence and the International Criminal Court’, HHRJ (online) 32 (2019), at <<https://harvardhrj.com>>.

³⁸ On the collection of, and reliance on, so-called user-generated evidence, that is footage that an ordinary citizen – the user – records on their smartphone, in an effort to achieve legal accountability, see Rebecca J. Hamilton, ‘New Technologies in International Criminal Investigations’, ASIL Proc. 112 (2018), 131–133; see also Beth Van Schaack, ‘Innovations in International Criminal Law Documentation Methodologies and Institutions’ (2019), at SSRN: <<https://ssrn.com/abstract=3329102>>; Rebecca J. Hamilton, ‘Social Media Platforms in International Criminal Investigations’, Case Western Reserve Journal of International Law 52 (2020), 213–223.

Another area where the role of the internet has become most prominent for the purposes of accountability is human rights. As it has been effectively put,³⁹ to say that mobile technologies, social media, and increased connectivity are having a significant impact on human rights practice would be an understatement. From videos of rights violations to eyewitness accounts disseminated on social media, human rights practitioners have access to more data today than ever before. There has been, however, no corresponding decline in human rights breaches.⁴⁰

The internet can both significantly facilitate and impede the exercise of human rights. The internet offers a powerful technology for society and individuals to express their rights, but also an environment in which such rights can be curtailed by powerful states, public and private institutions, and individuals.⁴¹ Moreover, social media platforms have been beset with hate speech, misinformation, disinformation, incitement of violence, and other content that can also cause real-world harm.

International human rights rules emerged long before the internet and social media were widespread, and were written and ratified for use by states, not for private companies. They must therefore be interpreted and adapted for this new purpose.⁴² Lack of clarity about the nature of human rights obligations of private actors such as Big Tech companies, market actors, and consumers, coupled with their growing power and influence over public

³⁹ Sam Dubberley, Alexa Koeing and Daragh Murray (eds), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (Oxford: Oxford University Press 2020), also on the types of evidentiary considerations specific to digital evidence.

⁴⁰ On the current 'twilight' or 'end-times' of human rights, where human rights are at best the 'last utopia', see Stephen Hopgood, *The Endtimes of Human Rights* (New York: Cornell University Press 2013); Samuel Moyn, *The Last Utopia: Human Rights in History* (Cambridge, MA: Belknap, for Harvard University Press 2010); Eric A. Posner, *The Twilight of Human Rights Law* (Oxford and New York: Oxford University Press 2014). See also: Emile M. Hafner-Burton, *Making Human Rights a Reality* (Princeton, NJ: Princeton University Press 2013); David P. Forsythe, 'Hard Times for Human Rights', *Journal of Human Rights* 16 (2017), 242-253.

⁴¹ Christopher T. Marsden, 'Transnational Internet Law' in: Peer Zumbansen (ed.), *Oxford Handbook of Transnational Law* (Oxford and New York: Oxford University Press 2020), available at <<https://ssrn.com/abstract=3552918>>.

⁴² See Michael Lwin, 'Applying International Human Rights Law for Use by Facebook', *Yale Journal on Regulation* (2020), available at <<https://ssrn.com/abstract=3681581>>, proposing a framework for the use of international human rights law by social media companies; Molly K. Land, 'The Problem of Platform Law: Pluralistic Legal Ordering on Social Media' (2019), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3454222>. On the basic differences between physical searches of tangible property and electronic searches of digital evidence under national law, and a normative framework for applying the Fourth Amendment to searches of computer hard drives and other storage devices, Orin S. Kerr, 'Searches and Seizures in a Digital World', *Harv. L. Rev.* 119 (2005), 531-585.

affairs, has long been one of the most pressing human rights issues in the digital age.⁴³ The term ‘cybersecurity’ was coined to refer to the protection of information and communication technologies from unauthorised access or attempted access.⁴⁴

Due to its enormous scope and global reach, the human rights implications of the internet could not be overestimated. All international law fields, however, are affected by the pervasiveness of the internet. Videos documenting war crimes and other serious human rights breaches, for example, often serve the case for or against humanitarian intervention.⁴⁵ By way of further exemplifications, the internet offers satellite images of environmental degradation. And it plays a role in national elections, which in turn affect international politics; online national election campaigns also speak of the kind of democracy that states now days consider as part of an international right to democracy.⁴⁶

At no time in history, has there been more information available to governments and the public about violations of international norms (particularly, but not exclusively human rights violations): more and more of these violations are, or can be, ascertained and documented through the internet,

⁴³ An area of internet governance with particularly important human rights implications is the Domain Name System (DNS), which matches computer addresses to human-friendly domain names and is governed by a private, multi-stakeholder body, the Internet Corporation for Assigned Names and Numbers (ICANN), which is in turn transitioning from U.S. supervision to full privatisation. ICANN has recently adopted in its organisational bylaws a ‘Core Value’ of respecting ‘internationally recognised human rights’. See Monika Zalnieriute, ‘Reinvigorating Human Rights in Internet Governance: The UDRP Procedure Through the Lens of International Human Rights Principles’, *Columbia Journal of Law and Arts* 43 (2020), 197-235, discussing in a human rights perspective the new Uniform Domain Names Disputes Resolution Policy (UDRP) procedure created by ICANN in 1998.

⁴⁴ Although definitions can vary, see Martha Finnemore and Duncan B. Hollis, ‘Constructing Norms for Global Cybersecurity’, *AJIL* 110 (2016), 425-479.

⁴⁵ See n. 31. The overflow of information generated during disasters can be as paralysing to humanitarian response as the lack of information. This flash flood of information is often referred to as Big Data, or Big Crisis Data. Patrick Philippe Meier, *Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response* (Boca Raton, FL: CRC Press 2015).

⁴⁶ The 2020 and previous US Presidential elections offer a prominent example of the role of the internet in national elections. The Internet is now a part of American democracy. A majority of Americans are online and many of them use the internet to learn political information and to follow election campaigns, while candidates invest heavily in web and e-mail campaign communication tools in order to reach prospective voters, as well as to communicate with journalists, potential donors, and political activists. Moreover, voters are influenced by what they see on the internet. On the dynamics of the US 2000 elections, see Bruce Bimber and Richard Davis, *Campaigning Online: The Internet in U.S. Elections* (Oxford: Oxford University Press 2003). See also Jens David Ohlin, ‘A Roadmap for Fighting Election Interference’, *AJIL Unbound* 115 (2021), 69-73.

beyond the specific purposes of criminal prosecutions. Increased detection of international breaches has not resulted, however, in a higher degree of effectiveness of the relevant rules of international law.

The internet allows the detection of major breaches, it does not necessarily advance the effectiveness of international law. This does *qualify*, but it does not diminish or make less significant, the relevance of the internet for the purposes of implementation of international law.

IV. Technological Power as a Leverage of Global Governance

While the guiding principle of post-1945 global governance was multilateralism,⁴⁷ post-Cold War global governance has increasingly become a multistakeholder governance.⁴⁸

States remain the primary and most powerful actors and international organisations still retain a considerable role, but civil society, corporations, social and political groups, and the like are all potential stakeholders in many areas.⁴⁹ Internet governance is the one area in which the shift to multistakeholder governance is particularly evident.⁵⁰

The internet started as a US phenomenon, ‘a niche government-academic project to allow academics and military folks to communicate together’,⁵¹

⁴⁷ Multilateralism ‘is an institutional form which coordinates relations among three or more states on the basis of “generalized” principles of conduct [...] without regard to the particularistic interests of the parties or the strategic exigencies that may exist in any specific occurrence.’ John Gerard Ruggie, ‘Multilateralism: the Anatomy of an Institution’, IO 46 (1992), 561-598 (571).

⁴⁸ *Ex multis*, Geoffrey Allen Pigman, *The World Economic Forum: A Multi-Stakeholder Approach to Global Governance* (London: Routledge 2006); Joost Pauwelyn, Ramses A. Wessel and Jan Wouters (eds), *Informal International Lawmaking* (Oxford: Oxford University Press 2012); Richard B. Stewart, ‘Remedying Disregard in Global Regulatory Governance: Accountability, Participation, and Responsiveness’, AJIL 108 (2014), 211-270; Kenneth W. Abbott, Jessica F. Green and Robert O. Keohane, ‘Organizational Ecology and Institutional Change in Global Governance’, IO 70 (2016), 247-277.

⁴⁹ In transborder environmental protection, territorial disputes, internet governance, anti-corruption, international human rights, and humanitarian law, for example, private businesses are increasingly supporting the implementation and enforcement of international law. On the role of corporations in the global legal order, see Jay Butler, ‘The Corporate Keepers of International Law’, AJIL 114 (2020), 189-220.

⁵⁰ ‘The Internet is by no means the sole example of contemporary multistakeholderism. But it is one of the most elaborate examples and one in which the drive to multistakeholderism has had special and perhaps unique causes.’ Raustiala (n. 2), 503.

⁵¹ Mark A. Lemley, ‘The Splinternet’, Duke Law Journal 70 (2021), 101-131 (102-103) (also available as Stanford Law and Economics Olin Working Paper #555, at SSRN: <<https://ssrn.com/abstract=3664027> and <http://dx.doi.org/10.2139/ssrn.3664027>>).

before commercial entities were given unrestricted access to it in the early 90's, to become the truly global phenomenon that we know today. The internet 'flattened' the world, making it more diffuse and decentralised, with individuals and corporations as actors of influence increasingly detached from states.⁵²

While many countries have dominant private internet players, they are not the same private players. Cooperation between networks at the national, regional, and international level to regulate the internet challenges our nation-state-centred universe. But there is also an ongoing nation-by-nation competition for who gets the internet.⁵³ Since the Arab spring showed in the early 2010s the power of the internet to foment a revolution, authoritarian regimes have used their power to control and to lock down the means of communication to prevent dissent from organising.⁵⁴

We posit that technological power is a fundamental leverage in global governance, akin to economic, military, and political might. Because this is going to be a technology century, countries will sink or swim based on their brainpower in the Artificial Intelligence (AI), biotech, quantum computing, nanotech future that we're going to be living in.⁵⁵

There is considerable discussion about the shape of the international system over the next 30 to 50 years. One question that has been asked is whether our Westphalian legal world, 'which rests heavily on geography, [...] is an appropriate controlling vision of international law as we move further into the 21st century'.⁵⁶

Although a number of developments are underway, geography remains central to the international system. The very concept of statehood, but also other concepts and principles of international law (such as the

⁵² See Thomas L. Friedman, *The World Is Flat: The Globalized World in the Twenty-First Century* (Further Updated and Expanded) (3rd edn, New York: Picador / Farrar, Straus and Giroux 2007), also for the thesis that the fall of the Berlin Wall in 1989 was the first in a series of events which not only meant the end of Cold War but also aided the establishment of global connectivity which flattened the world. See also Marsden (n. 41).

⁵³ For the thesis that the internet is being balkanised and that the 'splintering' of the internet is a bad thing, and we should stop it, see Lemley (n. 51). On the distinction – amongst internet actors – between providers of internet access (telecoms companies) and providers of services and content (Google, Facebook, and other websites), see Marsden (n. 41).

⁵⁴ It happened in India (in relation to Kashmir), Iran, Turkey, Malaysia, Brazil, and Pakistan. Various Arab countries have also blocked large parts of the internet at one time or another.

⁵⁵ These lines belong to Nicholas Burns, 'Why Does Good Diplomacy Matter?', Harvard Magazine (23 March 2020).

⁵⁶ Daniel Bethlehem, 'The End of Geography: The Changing Nature of the International System and the Challenge to International Law', EJIL 25 (2014), 9-24 (10-11).

principles of non-intervention or of state jurisdiction) are deeply rooted in the traditional notion of territorial geography, which depends on the extent of the territory of states.⁵⁷ Among the challenges to the traditional conceptions of an international system rooted in geography is that 'virtual space takes on dimensions and an importance that rivals physical space in the world of transactions, communications, and other engagements'.⁵⁸

It is submitted that the virtual realm brought about by the internet changes the geography of statehood, but it does not make it less important. The very notion of geography is *expanded* to include the digital, in addition to the physical, space of a state. The regulation of the internet and internet access therefore raises profound questions of sovereignty.

For centuries, more powerful states have exerted a major influence in the formation of customary international law.⁵⁹ This largely remains true today. The interface between international law and the internet affects the relationships and the power balance between the Global South and Global North, in terms of positive law and participation in processes of norm development and implementation. A particularly critical concern is for states that are highly challenged by the digital divide. In developing countries with little access to the internet or countries with strong internet censorship regimes, that censor information online, it will be difficult to effectively use the internet to participate to international law-making processes as well as to ascertain state behaviours or document the violation of international rules. Equal *participation* to international law-making processes and implementation procedures as well as equal *impact* on such processes' and procedures' outcome, are desirable but unattainable goals, surely in the next few decades to come. In so far as technological power replicates the existing power balance, the internet is likely to both deepen and make harder to cure current divides.

The internet empowers states, but it also enhances the role of all stakeholders of international society, including corporations from the public and

⁵⁷ 'Borders and title to territory continue to matter.' Bethlehem (n. 56), 14.

⁵⁸ Bethlehem (n. 56), 15.

⁵⁹ 'It has been observed that the collections of State practice give an unbalanced view, as they concern the practice of the relatively small group of the main powers. While there is some truth in this observation, it must also be stressed that the main powers engage in relations with most other States, so that the practice of almost all States is, at least in part, reflected in these collections. Moreover, in recent times a number of collections and reviews of practice of smaller and third world States have begun to appear. Important changes in the availability of manifestations of international practice have been brought about in recent times by electronic means of knowledge now widely available.' Treves (n. 4), para. 80.

the private sectors,⁶⁰ NGOs,⁶¹ academia, and civil society. Scholars working on technology and internet governance traditionally focus on the exercise and limits of power by nation-states. But more recently, they have had to confront the practices – and the limits of power – of private companies and informal actors.⁶²

Digital constitutionalism refers to efforts ‘to articulate a set of political rights, governance norms, and limitations on the exercise of power on the internet’.⁶³

The internet is global and decentralised, hence there is more communication of information from more sources. The internet has given the world access to multiple different sources of information and content, including misinformation. But it has also birthed new – virtual, digital – territories where international practice by multiple actors originates. This practice is relevant to the formation and implementation of international law, as outlined in the previous paragraphs. There is thus a nexus between internet governance and the impact of the internet on international law-making processes and the mechanisms of international responsibility.

V. Concluding Remarks

This paper has explored the impact of the internet on the practice and theory of customary international law and showed that States’ and non-state actors’ behaviour has undergone radical change. International actors operate on and through the virtual space generated by the internet, and so does the

⁶⁰ Because global electronic commerce continues to grow rapidly, for example, the most valuable public companies are now e-commerce giants not only in the US but also in China and Russia. The Internet and associated technologies such as blockchain and smart contract have transformed the supply chains of traditionally dominant industrial sectors such as automobile manufacture, petro-chemical refining, and aerospace engineering. Even in Europe, the European Commission has been driven by industry to proclaim the emergence of Industry 4.0, a new phase based on digitisation, the Internet of Things, cloud computing, AI, advanced robotics, blockchain, and smart contracts.

⁶¹ See e.g., Nina Hall, Hans Peter Schmitz and J. Michael Dedmon, ‘Transnational Advocacy and NGOs in the Digital Era: New Forms of Networked Power’, *International Studies Quarterly* 64 (2020), 159-167.

⁶² See Ramses A. Wessel, ‘Regulating Technological Innovation through Informal International Law: The Exercise of International Public Authority by Transnational Actors’ in: Michiel A. Heldeweg and Evisa Kica (eds), *Regulating Technological Innovation: A Multidisciplinary Approach* (London: Palgrave Macmillan 2011), 77-94.

⁶³ The first research paper on ‘digital constitutionalism’ is Lex Gill, Dennis Redeker and Urs Gasser, ‘Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights’, *The Berkman Center for Internet and Society Research Publication* 15 (2015), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120>.

law. The previous paragraphs described multiple ways in which states and other actors act through the internet, and showed that the internet permeates all fields of international law. This, however, has been only partially reflected in the theory of international law.

In the work of the ILC on the 'Identification of customary international law' referred to above,⁶⁴ there is but scant reference to audiovisual materials in relation to 'teachings of the most highly qualified publicists' as a subsidiary means for determining rules of customary international law (ILC Commentary to Draft conclusion 14). That the internet, let alone its power, is barely mentioned by the ILC – the subsidiary organ of the UN General Assembly entrusted with the mandate to promote the progressive development of international law and its codification⁶⁵ – does not make the digital realm less relevant or real. It merely points to a lacuna in mainstream legal scholarship, that this paper has attempted to address.

The case studies attest and demonstrate that international practice in the digital space is not only relevant to the formation of rules regulating the digital space itself ('international internet law' or 'international law of the internet'). It does also increasingly contribute to the emergence of customary rules outside the *Internetvölkerrecht*. The previous paragraphs provide support for the proposition that the digital realm has changed the traditional law-making processes, in particular for international customary law. In spite of the relevance of treaties, customary processes and rules remain an essential part of international law. Notwithstanding their widespread codification in treaties during the last century, the unwritten norms of customary law continue to play a crucial role in international relations.⁶⁶ And customary international law often forms at a much faster pace, especially but not exclusively with respect to areas of technological or other fundamental change.⁶⁷ In contrast to earlier times, in the modern era of instantaneous electronic communications and proliferation of diplomatic conferences, organisations and other forums for multinational diplomatic exchanges (including in the virtual space), international practice is being generated at an increasing pace and is becoming more and more widely disseminated over the internet.

⁶⁴ *Supra*, III.

⁶⁵ See Art. 13 UN-Charter: 'The General Assembly shall initiate studies and make recommendations for the purpose of: (a) promoting international co-operation in the political field and encouraging the progressive development of international law and its codification.'

⁶⁶ On the continuing importance of customary international law and the primary reasons for customary international law's continuing vitality, see Treves (n. 4), paras 90-92.

⁶⁷ 'While one might tend to think of customary international law as growing only slowly, in contrast to the more rapid formation of treaties, the actual practice of the world community in modern times suggests that the reverse is more often the case.' Scharf (n. 22), 309.

The internet is part of the diversity of forms in which practice and its acceptance as law may be manifested. Hence, it provides at same time *evidence* for the identification of customary rules, and *normative materials* which may amount to the emergence and consolidation (or change in content) of those very same rules. With respect to *law-making*, the internet acts as both a sounding board for, and an originator of, international practice. In contemporary international settings, modern technologies are also a means for influencing international practice in relation to treaties, over time.

The internet has not generally contributed, however, to make international law more effective. New technologies and social networks have certainly increased the availability of information to governments and the public regarding breaches of international law. Yet, they have created a new – online – environment in which internationally wrongful acts can be committed. This qualifies, does not make less significant, the relevance of the internet for the *implementation* of international law.

Because of the pervasive power of internet communications as the medium across which all other media can be conveyed and recorded, it is difficult to conceive of any branch of international law including competition law, human privacy and electronic banking, without regard to the transformations created by the online environment. The internet entails important implications for most, if not all, areas of international law.

Yet, the impact of the internet on the making, interpretation, and implementation of international law remains elusive and hard to conceptualise. Elusiveness, however, should not be confounded with reality (or lack thereof).

In addition to communicating and sharing knowledge about, as well as contributing to the making and implementation of, international rules, the use of the internet also illuminates our understanding of the *power balance* in global governance as well as the relationship between law and power and the legitimacy of international law.

The internet has expanded the very notion of geography upon which our Westphalian nation-state-centred universe is premised, to include the digital, in addition to the physical, realm. The *digital world* has birthed whole new ‘territories’ where the practice of states and other actors is recorded and displayed, but it also exists independently from the physical realm. Technology’s power is a fundamental leverage in global governance, akin to economic, military, and political might not only for states but also for a wide range of non-state actors, such as Big Tech corporations, social and political groups, and civil society.

Whether or not it has changed our life for the better,⁶⁸ the internet contributes to shape the international landscape, international relations, the international legal order (or disorder), *and* international law's structures and processes.

International legal scholarship has failed so far to comprehensively assess the power of 'the internet'. This paper has focused the camera lens on the internet as a *game changer* not in the sense of a trigger of new rules and regulations applicable in the virtual space (*Internetvölkerrecht*), but as a changer of processes and structures, most notably, but not exclusively, of international customary law. The impact of the internet on the processes and structures of international law is real and bound to become more evident in the future. This phenomenon has been going on for several decades now, although modern technologies increased incrementally over the last decade. The COVID-19 emergency precipitated it.

⁶⁸ See Lemley (n. 51), for the view that: 'What the internet did was something quite remarkable. It allowed people to connect outside those walled gardens. It allowed you to interact with someone who wasn't part of a preexisting community, who wasn't geographically near you, who wasn't in the same community of scholarship and the same community of thought with you. And that connection turned out to be extraordinarily and unexpectedly valuable' (103). 'The internet has also changed our lives for the better. Our phones improve our lives in ways we don't think about because we're not lost in a foreign country where we don't speak the language. We have a map that will get us where we want to go. We're not stuck on the highway with a flat tire and no way to communicate to anyone about that fact. We're not sitting in a restaurant waiting for a friend who cancelled or debating some arcane fact with our friends without a device in our pocket capable of accessing all of the world's information. [...] These are things that became available because we have access to this intersecting universe of information' (123).

Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development

Antonio Segura-Serrano*

University of Granada, Granada, Spain

asegura@ugr.es

Abstract	701
Keywords	702
I. Introduction	702
II. Dynamic Application and Its Limits	703
1. Legal Nature	705
2. International Responsibility	706
a) Attribution: Rules and Problems	706
b) Countermeasures	710
c) State of Necessity	713
3. Due Diligence Obligation	715
III. Cybercrime as a Test Case of Norm-Development	718
1. Jurisdictional Issues	719
a) Territorial Jurisdiction	719
b) Extraterritorial Jurisdiction	721
2. Cybercrime	722
a) Preliminary Remarks Regarding Norm-Development	722
b) The Budapest Convention on Cybercrime	724
c) Developments at the UN Level	726
IV. Final Remarks	728

Abstract

The earliest approach by international lawyers to the question of cybersecurity was focused on collective security. Regarding this issue, there is consensus on the evolutionary and dynamic application, difficult in any case, of the basic rules concerning the prohibition of the threat and the use of force that already exists in the international order. However, cybersecurity does not only concern peace and security, as it is considered a problematic issue that poses various challenges from other international legal perspectives. This paper aims to analyse cybersecurity from this more holistic approach, pointing out the shortcomings of this evolutionary application as well as the

* Associate Professor (Senior Lecturer) of Public International law and EU Law at the University of Granada.

efforts that have been carried out so far in order to promote international cooperation in this field so as to achieve norm-development.

Keywords

cybersecurity – cyberattacks – cybercrime – international responsibility – jurisdiction – norm-development

I. Introduction

The earliest approach by international lawyers to the question of cybersecurity was focused on collective security. Regarding this issue, there is consensus on the evolutionary and dynamic application, difficult in any case, of the basic rules concerning the prohibition of the threat and the use of force that already exists in the international order. However, cybersecurity does not only concern peace and security, as it is considered a problematic issue that poses various challenges from other international legal perspectives. This paper aims to analyse cybersecurity from this more holistic approach, pointing out the shortcomings of this evolutionary application as well as the efforts that have been carried out so far in order to promote international cooperation in this field so as to achieve norm-development.

The goal of this paper consists of evaluating the background norms and the legal avenues that are proposed in extant international law in order to address cyberattacks, generally speaking. The central argument posed is that those avenues have important weaknesses and, therefore fall short of what is needed if international law is to be relevant in reacting against those cyberattacks within a rule-based international order. Thus, the norm-development avenue is analysed as the alternative option and the best way forward. However, the paper will be very critical of the efforts recently made in this realm, as they have produced only limited results. The test case of cybercrime will be used to show how far international law is from solving the problems posed by cyberattacks.

This paper will start by assuming that cyberattacks are a growing and, perhaps, the most persistent problem that the international community is in need of addressing in cyberspace. For example, the ransomware virus known as WannaCry, which put half the world in check in 2017, was still one of the most aggressive viruses in late 2019.¹ Likewise, the NotPetya cyber operation

¹ Naked Security, 'WannaCry – the Worm that Just Won't Die', 18 September 2019, <<https://nakedsecurity.sophos.com>>.

has been termed as the most devastating cyber-attack in history, with at least \$10 billion in total damages.² Cyberattacks can be attributed to State or non-State actors. In the first case, they fall within the scope of the use of force, as set by the 'scale and effects' standard,³ prohibited by international law within the framework of the United Nations (UN) Charter. However, if those cyberattacks do not reach the use of force's threshold, then international responsibility and countermeasures may be invoked, but only if there is an international wrongful act. Many of the cyber operations like the two mentioned previously do not constitute a violation of international law, unless we consider that territorial sovereignty is the infringed rule.⁴ In the case of cyberattacks attributed to non-State actors, various international legal cooperation mechanisms may be used, particularly the Budapest Convention on Cybercrime.

Section II will address the background issues that need to be solved if international law is to properly fulfil its functions and govern State relations regarding cyberspace in the face of cyberattacks. After a quick reference to the legal nature of cyberspace, this section will review how adaptive application of international law fares when it comes to basic rules such as those relating to international responsibility, which are of utmost importance for the discipline to be up to the task. Section III will be devoted to the alternative route, i.e., norm-development as the way out to achieve the international regulation needed for the most pressing cybersecurity issues. The UN efforts at the global level, and the specific endeavour to introduce new rules in the cybercrime realm mainly, but not only, at the regional level, will form the bulk of this section. Section IV will conclude this assessment with some final remarks.

II. Dynamic Application and Its Limits

The option consisting of the dynamic application of extant international law rules to cyberspace has been that held by the US and its Western allies. The cybersecurity strategies of these countries are very explicit in this regard,

² Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', 22 August 2018, <<https://www.wired.com>>.

³ ICJ, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Judgment, 27 June 1986, ICJ Reports 1986, 14 (para. 195).

⁴ Przemysław Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, <<https://www.justsecurity.org>>; François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 231; *Contra*: Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber', *AJIL Unbound* 111 (2017), 207-212 (207 f.).

as are the French,⁵ German⁶ or Spanish⁷ strategies. However, few States, e. g., France and The Netherlands,⁸ have fully delved into the specifics of this difficult legal interpretation. Among the cross-cutting issues that need to be solved in order to provide stability and security in cyberspace are those relating to responsibility. Firstly, because these are principal problems from the perspective of the discipline of public international law, in order for it to properly fulfil its functions in this new environment. Second, because, although these issues have been debated for some time in their application to cyberspace, they are very hot areas on international agendas and have certainly not been definitively unravelled as of today in the face of cyberattacks.

This section seeks to reflect on the above-mentioned issues on the basis of the few existing reference documents on the subject. The aim is to comment, mainly, on the rules set out in the Tallinn Manual 2.0, published in 2017, the first edition of which was published in 2013,⁹ and which is intended to reflect the *lex lata*. In addition, the reports of the Groups of Governmental Experts (GGE) which have been prepared to date within the framework of the UN will be reported, chiefly those corresponding to 2013 and 2015.¹⁰ Also, the paper will consider the recent Open-Ended Working Group (OEWG) Report of 2021, which will be followed by the work of a new OEWG 2021-2025.¹¹ Likewise, the scarce State practice, mainly in the form of State views on the application of international law to cyberspace will be taken into account. Although this paper does not attempt to definitively elucidate the question of the legal status of these documents, the GGE reports and the

⁵ Prime Minister, French Republic, *French National Digital Security Strategy*, adopted in 2011 and updated in 2015, <<https://www.ssi.gouv.fr/>>.

⁶ Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, adopted in 2011 and updated in 2016, <<https://www.enisa.europa.eu/>>.

⁷ Prime Minister, Spanish Government, *National Cybersecurity Strategy*, adopted in 2013 and updated in 2019, <<https://www.dsn.gob.es/>>.

⁸ Government of The Netherlands, *Letter to the Parliament on the International Legal Order in Cyberspace*, 5 July 2019, <<https://www.government.nl/>>; Ministère des Armées, République Française, *Droit internationale appliqué aux opérations dans le cyberspace*, 2019.

⁹ Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press 2017), 2-3; Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press 2013).

¹⁰ UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 24 May 2013, A/68/98; UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, of 22 September 2015, A/70/174.

¹¹ UNGA, Final Substantive Report, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of 10 March 2021, A/AC.290/2021/CRP.2.

OEWG Report have obviously more legal import, as they substantiate the collective opinion of UN Member States. However, those reports do not allow for an exhaustive legal critique, as they are very general texts which embody a global consensus on the applicability of extant customary law but are devoid of detailed rules. Conversely, the Tallinn Manual is more problematic, as it elaborates on very specific rules allegedly representing the *lex lata*, even if some previous analyses have already endeavoured to assess whether this Manual is actually followed by States.¹² Although the Tallinn Manual is the result of the work of a group of experts and therefore may be considered only as a private endeavour, it is also evident that as a North Atlantic Treaty Organization (NATO) supported project it also provides the legal arguments and the mainstream position mostly held by Western governments, i. e. that extant international law rules are sufficient to govern international relations in cyberspace. This is the reason why the Tallinn Manual is analysed more extensively in this paper, although reference is also made to UN reports and State views where they offer some guidance.

1. Legal Nature

Now that the first libertarian demands¹³ have been forgotten, there is still some debate as to the legal nature of cyberspace. On the one hand, there are those who consider it to be part of the global commons, along with a varied group of international spaces.¹⁴ However, given that the Internet infrastructure is currently both public and private, and that the rules that apply to it are both national and international, some authors opt for the concept of the ‘imperfect’ or pseudo-commons.¹⁵ This type of characterisation suggests that an internationalised legal regime for the basic resources of cyberspace could

¹² Dan Efrony and Yuval Shany, ‘A Rule Book on the Shelf? Tallin Manual 2.0 on Cyber-operations and Subsequent State Practice’, *AJIL* 112 (2018), 583-657, (653), who are critical of the Tallinn Manual, as they believe that it is not being followed by States in their most recent practice, given the wait-and-see strategy that these States have adopted. However, this remark does not go as far as to conclude that the Tallinn Manual’s rules are rejected outright by States or do not represent their views at all.

¹³ John P. Barlow, ‘A Declaration of the Independence of Cyberspace’, 8. February 1996, <<https://www.eff.org>>.

¹⁴ US Department of Defense, *Strategy for Homeland Defense and Civil Support*, 2005, 12; Government of Canada, *Canada’s Cyber Security Strategy: For a Stronger and more Prosperous Canada*, 2010, 2.

¹⁵ Joseph S. Nye, *Cyber Power*, (Cambridge: Harvard Kennedy School 2010), 15; Scott J. Shackelford, ‘Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance’, *American University Law Review* 62 (2013), 1273-1364 (1292).

be achieved in the future, following the contours of the concept of the common heritage of mankind (CHM).¹⁶ Even if cyberspace is not a perfect commons, Internet governance following the contours of the CHM concept is an innovative proposal that may be added to the discussion with some success. The CHM's principles of non-appropriation, common management, peaceful use, and preservation seem to create a better legal framework to be applicable to Internet governance than the present multistakeholder approach, as represented by the Internet Corporation for Assigned Names and Numbers (ICANN), where big commercial interests linked to the United States (US) are the leading force.¹⁷

2. International Responsibility

One of the main difficulties in relation to international responsibility in cyberspace is that of attribution, due to the prevalence of anonymity on the Net. This anonymity can be achieved in various ways, through virtual private networks (VPNs), proxy servers, onion routing, etc. In fact, the 2013 and 2015 UN GGE reports have included a prohibition on the use of third parties by States to commit internationally illicit acts through (Information and Communication Technologies) ICTs. However, leaving aside the widespread practice of States consisting of the use of intermediaries to carry out clandestine acts on the web,¹⁸ the operation of attribution itself is complicated by the diversity of actors present in cyberspace.¹⁹

a) Attribution: Rules and Problems

The Tallinn Manual raises as its most immediate concern the difficulty, both technical and legal,²⁰ of the question of attribution for a State seeking to

¹⁶ Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law', Max Planck UNYB 10 (2006), 191-272 (231).

¹⁷ Antonio Segura-Serrano, 'Cyberspace and the Common Heritage of Mankind' in: Daniele Amoroso et al. (eds) *Global Public Goods, Global Commons and Fundamental Values: The Responses of International Law*, 2017 ESIL Annual Conference, (Oxford: Oxford University Press 2021), 189-208.

¹⁸ Tim Maurer, "'Proxies' and Cyberspace', Journal of Conflict & Security Law 21 (2016), 383-403.

¹⁹ Michael N. Schmitt and Liis Vihul, 'Proxy Wars in Cyber Space: The Evolving International Law of Attribution', Fletcher Security Review 1 (2014), 55-73.

²⁰ Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', Journal of Conflict & Security Law 17 (2012), 229-244 (233).

make use of unilateral reaction measures. Indeed, the *ex ante* determination of the attribution of a cyber-operation as a preliminary step to a unilateral response may be subject to considerable uncertainty in cyberspace, in the absence of sufficient information. Given the extant situation, the Tallinn Manual considers that the unilateral reaction of the State must be subject to the criterion of reasonableness, according to the context in each case, which in turn is in line with the US and United Kingdom's (UK) views²¹ on the matter.²² However, consistent with the International Court of Justice (ICJ) case-law, the Tallinn Manual adds another decisive factor to this equation, namely the seriousness of the infringement, so that the more serious the infringement committed, the more confidence must be placed in the evidence put forward by the reacting State,²³ although the seriousness of the response must also be considered.²⁴ However, when a State takes countermeasures against the cyberactivities of another State it always does so at its own risk, so that if an error in attribution is subsequently found the State will have committed an international wrongful act with its response.

Another problematic issue raised by the Tallinn Manual is that of the publicity of the evidence on which the attribution of a cyber-operation to another State is based. The Manual understands that, although it could be positive, there is currently not enough practice or *opinio juris* to affirm this obligation. The United States has argued through the State Department's Legal Adviser that there is no international obligation to disclose the evidence before taking response action,²⁵ a position also expressed by the United Kingdom through its Attorney General,²⁶ by France,²⁷ and by The Netherlands.²⁸ On the contrary, the UN GGE has stated that 'the accusations of

²¹ Brian J. Egan, 'International Law and Stability in Cyberspace', Berkeley J. Int'l L. 35 (2017), 169-180 (177); Jeremy Wright, 'Cyber and International Law in the 21st Century', 23 May 2018, <<https://www.gov.uk>>.

²² Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', The Hague Program for Cyber Norms Policy Brief, March 2020, 15, arguing that this reasonableness should be interpreted as a standard of evidence but not as a duty of care when making the attribution, as the US and UK views seem to convey.

²³ ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia-Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, ICJ Reports 2007, 129, (paras 208-209).

²⁴ Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks', AJIL Unbound 113 (2019), 202-206 (206), proposing a system of gradation in the standards of attribution, depending on the response to be adopted by the State that is the victim of a cyber-attack.

²⁵ Egan (n. 21), 177.

²⁶ Wright (n. 21).

²⁷ Ministère des Armées (n. 8), 11.

²⁸ Government of The Netherlands (n. 8).

organising and implementing wrongful acts brought against States should be substantiated',²⁹ in accordance with ICJ case law on evidence.³⁰ A recent analysis of practice has shown that difficulties relating to attribution are leading States to a strategy of caution in which, because of this impossibility of establishing attribution with certainty,³¹ it is preferred not to invoke the illegality of certain cyber-activities, which in turn promotes impunity.³² If we take the example of the Wannacry cyber-attack in 2017, where attribution to North Korea was readily made by private firms within few days,³³ it took several months for the US and the UK to publicly attribute this cyber-attack to North Korea,³⁴ and no public sanction followed. Likewise, the 2019 Georgia cyber-attack attributed to Russia four months after its occurrence is interesting in that an increased number of States publicly made an official attribution of the cyber incident to Russia (more than 20), but failed to indicate the specific international law rules that were breached by this cyber-attack, in what has been termed as a missed opportunity to strengthen the international rules-based order.³⁵ Therefore, there is much to be done in the field of public attribution of cyber-attacks from the point of view of State practice, as States are still balancing from the application of international law to strategic and political considerations.

A particular difficulty arises in relation to the taking of control and use of the cyber infrastructure, governmental or private, of another State to carry out malicious operations. The UN GGE has specifically addressed the situation regarding the illegal use of another State's cyber infrastructure. Thus, the 2015 Report states that a determination that a cyber activity has originated in the territory or infrastructure of a State is not sufficient to attribute that activity to that State.³⁶ However, for the Tallinn Manual this use could be an indication that the State is associated with the operation, although this presumption would be less convincing if the cyber infrastructure used was

²⁹ UNGA, 2015 GGE Report (n. 10), para. 28 f.

³⁰ Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations', *Tex. Int'l L.J.* 50 (2015), 233-275 (243).

³¹ Yuval Shany and Michael N. Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations', *International Law Studies* 96 (2020), 196-222 (217), arguing that major States have the capacity to make attribution, but are sceptical about the very push for legal accountability in the face of those States that do not share the commitment to the 'rule of law'.

³² Efrony and Shany (n. 12), 633-634.

³³ Alex L. Johnson, 'WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group', 22 May 2017, <<https://community.broadcom.com>>.

³⁴ BBC News, 'Cyber-Attack: US and UK Blame North Korea for WannaCry', 19 December 2017, <<https://www.bbc.com>>.

³⁵ Roguski (n. 4).

³⁶ UNGA, 2015 GGE Report (n. 10), para. 28 f.

private, rather than governmental. Cases of spoofing, through techniques such as impersonating other organisations, or through the use of their IP addresses, are very difficult to resolve, and the Manual proposes a case-by-case assessment, depending on the context of each case. Therefore, also on this point, legal certainty is difficult to be affirmed beforehand, and end-result that is not desirable from a legal point of view.

With regard to the attribution of international responsibility in the case of cyber operations carried out by non-State actors, the Tallinn Manual as well as the OEWG Chair's Summary³⁷ endorses the criterion of 'effective control' that the ICJ has expressed in the *Nicaragua* and *Genocide* cases.³⁸ As is well known, 'global control' or indirect control would not be sufficient to produce such attribution to the State.³⁹ However, some authors have already asserted the criterion of global control as more appropriate for cyberspace,⁴⁰ basically because it makes the operation of attribution easier.⁴¹ Moreover, in the case of cyber-attacks that reach the threshold of armed attacks, some literature does not hesitate to reject the criterion of effective control out of hand and accept the much more lax criterion of tolerance or reluctance to act against such non-State actors, and end up attributing the act in question to the State from which the attacks originate.⁴² Some authors, in a scarcely reasoned argument, have even put forward a criterion of 'virtual' control through which the burden of proof would be reversed.⁴³

A final issue that connects with the question of attribution is that envisaged in the UN GGE 2013 and 2015 Reports. According to these reports, States must ensure that their territories are not used by non-State actors to commit internationally wrongful acts. On this basis, an intense debate has

³⁷ UNGA Chair's Summary, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 10 March 2021, A/AC.290/2021/CPR.3, para. 14.

³⁸ ICJ, *Nicaragua* (n. 3), para. 115; ICJ, *Genocide* (n. 23), para. 400.

³⁹ ILC, 'Articles on the Responsibility of States for Internationally Wrongful Acts with Commentaries', ILCYB, Vol. II, Part Two, (2001), 31, Art. 8, para. 5.

⁴⁰ Kubo Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors', *Journal of Conflict & Security Law* 21 (2016), 405-428 (423).

⁴¹ Scott J. Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' in: Christian Czosseck and Karli Podins (eds), *Conference on Cyber Conflict Proceedings 2010* (Tallinn: CCD COE 2010), 197-208.

⁴² Tsagourias (n. 20), 242.

⁴³ Peter Margulies, 'Sovereignty and Cyberattacks: Technology's Challenge to the Law of State Responsibility', *Melbourne Journal of International Law* 14 (2013), 496-519 (514), arguing that a State that has previously funded or assisted non-State actors who are perpetrators of malicious online activities should demonstrate its innocence in relation to such activities.

taken place around the due diligence obligation of States. This obligation is set out in Rules 6 and 7 of the Tallinn Manual and will be assessed later on.

Therefore, this paper is of the view that attribution is a crucial cybersecurity issue which extant international law is incapable of clarifying. To overcome this problem, part of the literature promotes attribution by non-State actors,⁴⁴ while other commentators support the setting up of a centralised international attribution mechanism,⁴⁵ though difficult to implement in the short run,⁴⁶ or propose a revision of the attribution determinants as stated by Article 8 of the International Law Commission (ILC) Draft Articles.⁴⁷ This kind of solution is in line with other proposals to internationalise the process of attribution, as those made by Microsoft⁴⁸ and RAND.⁴⁹ Hence, any of the mentioned ways forward entail the development of new rules of international law on this topic.

b) Countermeasures

The emphasis in the Tallinn Manual on countermeasures, to which a very extensive analysis is devoted, must be stressed. Perhaps this emphasis can be explained by the Tallinn Manual's undisguised interest in finding a formula for States to respond when self-defence against cyber-attacks is not legally justified in the specific case. This view is shared by those Western States that have expressed their opinion on the matter, e.g. the US, UK, France, and The Netherlands,⁵⁰ although the UN Reports by the GGE/OEWG do not refer to this possibility. However, a recent analysis of practice shows the States'

⁴⁴ Kristen E. Eichensehr, 'Decentralized Cyberattack Attribution', *AJIL Unbound* 113 (2019), 213-217 (217).

⁴⁵ Henning Lahmann, *Unilateral Remedies to Cyber Operations – Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, (Cambridge: Cambridge University Press 2020), 279.

⁴⁶ Shany and Schmitt (n. 31), 196 f., arguing that this mechanism would be of help in three contexts: for States facing capacity issues, for those interested in collective attribution, and in case of extant cyber-related sanctions regimes.

⁴⁷ Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *EJIL* 31 (2020), 941-967, (941 f.)

⁴⁸ Shaun Waterman, 'Microsoft Calls for UN-type Body to Attribute Big Cyberattacks', 23 June 2016, <<https://www.fedscoop.com>>.

⁴⁹ Benjamin Boudreaux, Jonathan W. Welburn, John S. Davis (II) and Cordaye Ogletree, 'Stateless Attribution, Toward International Accountability in Cyberspace', *RAND* (2017), 25 ff., calling for a Global Consortium for Cyber Attribution.

⁵⁰ Egan (n. 21), 169, 178; Wright (n. 21); Ministère des Armées (n. 8), 8; Government of The Netherlands (n. 8), 7.

reluctance to publicly claim their right to apply countermeasures for the time being regarding specific cyber-attacks.⁵¹ The reason why countermeasures as active defences against a cyberattack (hack-back) have not been widely used yet is related to the difficulty of timely attribution, which in turn gives countermeasures a more prominent *ex post facto* role in the near future.⁵² Indeed, the literature that is less inclined to make extensive use of self-defence, and therefore the use of force, in cyberspace considers that countermeasures have been given little consideration regarding this role, when in fact they may be the best recourse to be used, particularly since claims of malicious activity will ultimately have to be redirected to requests for financial compensation.⁵³

As for the object of a countermeasure, it must always be a State. Therefore, it is not possible to take countermeasures against non-State actors, unless the State has failed to fulfil its due diligence obligation, as will be seen later. In other words, non-State actors are not subject to States' own international legal obligations and, for that reason, cannot be the object of countermeasures against a previous wrongful act. For the Tallinn Manual, the alternative response to actions by non-State actors would be two measures that preclude wrongfulness, namely self-defence and state of necessity. However, with respect to self-defence, the problem is that this alternative response presupposes that non-State actors may violate the principle of prohibition of the use of force, and that the State against which the defensive action is directed is not the object of an international wrong when its consent is not present.⁵⁴ In this sense, some literature asserts that it is currently possible for non-State actors to infringe the principle of prohibition of the use of force, thus allowing self-defence against them. In turn, self-defence as a ground for precluding wrongfulness provided for in Article 21 of the ILC Draft Articles would justify the violation of the territorial sovereignty of the State where these non-State actors, who are the object of self-defence, are located.⁵⁵ However, this position does not reflect customary international law, nor is it supported by ICJ jurisprudence.⁵⁶ With respect to state of necessity, as

⁵¹ Efrony and Shany (n. 12), 646.

⁵² Lahmann (n. 45), 200.

⁵³ Mary E. O'Connell, 'Cyber Security without Cyber War', *Journal of Conflict & Security Law* 17 (2012), 187-209 (204-205).

⁵⁴ Federica I. Paddeau, 'Use of Force against Non-state Actors and the Circumstance Precluding Wrongfulness of Self-Defence', *LJIL* 30 (2017), 93-115 (106-107).

⁵⁵ Nicholas Tsagourias, 'Self-Defence against Non-state Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule', *LJIL* 29 (2016), 801-825 (801 f.).

⁵⁶ Monika Hakimi, 'Defensive Force against Non-State Actors: The State of Play', *International Law Studies* 91 (2015), 1-31 (1 f.).

opposed to countermeasures, its application does not require a prior international wrongful act, but the existence of a grave and imminent peril to an essential interest of the State, which makes the state of necessity very interesting so as to be applied to non-State actors. Yet, this situation is unusual in practice.⁵⁷

In any case, and despite the difficulty of the attribution referred to above, the Tallinn Manual agrees with the ILC in considering that States adopting countermeasures do so at their own risk and must answer for the legality of such measures. Therefore, a State which adopts a countermeasure which subsequently does not pass the legitimacy test will be liable for the unlawfulness involved. This conclusion in the context of the adoption of countermeasures has a restrictive function, since otherwise there could be a certain risk of escalation which must be avoided,⁵⁸ particularly in cyberspace, the intrinsic speed of which may run counter to a careful consideration of the situation at hand. However, the Tallinn Manual understands that this risk of escalation is mitigated by the requirement of prior notification, although, surprisingly, the effectiveness of this requirement is negated by the considerations later made in the Manual, as will be seen.

As regards the aim of countermeasures, namely to induce the offending State to comply with its international obligations, the Tallinn Manual considers that countermeasures in cyberspace are of a reactive, not prospective, nature, as a consequence of the first requirement called for by the ICJ in the *Gabčíkovo-Nagymaros* case,⁵⁹ namely the existence of a previous international wrongful act. The Tallinn Manual therefore maintains that there can be no countermeasures equivalent to anticipatory self-defence against imminent armed attack, nor is there room for preventive countermeasures. However, the requirement of reversibility of countermeasures, which was confirmed by the ILC, is understood by the Tallinn Manual as a requirement in the broad sense, it should not be absolute, nor should the State be required to choose the option that is most easily reversible. The Tallinn Manual gives as an example a denial of service attack (DDoS) which, when used as a countermeasure, has very limited reversibility, since the cyber-activities that are prevented can no longer be carried out.

A particularly difficult issue in the context of countermeasures arises in relation to the obligation of prior notification, as it is said this requirement

⁵⁷ ILC, ARSIWA (n. 39), Art. 25, para. 2.

⁵⁸ Michael N. Schmitt, "Below" the Threshold Cyber Operations: The Countermeasures Response Option and International Law', Va. J. Int'l L. 54 (2014), 697-732 (715).

⁵⁹ ICJ, *Gabčíkovo-Nagymaros Project* (Hungary v. Slovakia), ICJ Reports 1997, Judgment of 25 September 1997, 7 (83).

could make countermeasures ‘unrealistic’ in cyberspace.⁶⁰ This is also the position taken by Western States, e.g. the US, UK, France, and the Netherlands, although it is not clear whether the absence of prior notification is limited to those cases of covert cyber intrusion (UK and France), or it is to be based on urgency of the action (The Netherlands).⁶¹ Because of this unrealistic reason, the Tallinn Manual considers this requirement as non-categorical, in what has been called a pragmatic approach.⁶² Firstly, because the perpetrator of a malicious online operation may be masked. Secondly, because of the speed present in that medium, the reaction may be considered urgent,⁶³ in which case the requirement for prior notification should lapse. Lastly, prior notification may mean that the countermeasure to be taken is rendered ineffective and it would therefore be pointless to require compliance. However, this paper considers that the unveiled intention to dispense with this prerequisite of notification is worrying because it makes the approach of the Tallinn Manual and the mentioned States’ views clearly punitive.

Furthermore, the Tallinn Manual opts for the absence of an obligation to negotiate prior to the adoption of countermeasures, which departs from the rule reflected in the Commentary to the ILC Draft Articles on International Responsibility.⁶⁴ Indeed, the Tallinn Manual, in line with the position expressed by the United States on the Draft Articles, understands that a State may take countermeasures in cyberspace before entering into negotiations and even during negotiations, as otherwise the offending State would have control over the duration and impact of its breach.

c) State of Necessity

Rule 26 of the Tallinn Manual is devoted to state of necessity, which the Manual considers to be a controversial circumstance, even if it does attribute a customary character to it.⁶⁵ Although the Manual acknowledges that the threshold for invoking the plea of necessity is extremely high, the positive

⁶⁰ William Banks, ‘State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0*’, *Tex. L. Rev.* 95 (2017), 1487–1513 (1502).

⁶¹ Egan (n. 21), 178; Wright (n. 21); Ministère des Armées (n. 8), 8; Government of The Netherlands (n. 8), 7.

⁶² Eric T. Jensen, ‘The Tallinn Manual 2.0: Highlights and Insights’, *Geo. J. Int’l L.* 48 (2017), 735–778 (754).

⁶³ ILC, ARSIWA (n. 39), Art. 52, para. 6.

⁶⁴ ILC, ARSIWA (n. 39), Art. 52, para. 5.

⁶⁵ *Contra*: Sarah Heathcote, ‘Est-ce que l’État de nécessité est un principe de droit international coutumier?’, *RBDI* 40 (2007), 53–89.

approach to this circumstance is surprising, given that the ILC had framed it in negative terms.⁶⁶ This circumstance precluding wrongfulness can therefore be invoked only in exceptional cases, that is, where the essential interests of the State are seriously compromised.

Although the consideration of what is essential depends very much on each State and is therefore basically contextual, the Tallinn Manual endorses the tendency of some States to classify certain State infrastructures as critical, including cyber-infrastructure, which may highlight their essential nature. Examples of critical infrastructure could be the national banking system, the air navigation system, etc.,⁶⁷ as The Netherlands has stated.⁶⁸ An unresolved issue in the Manual is whether an essential interest of the international community can be used by a State to take unlawful but legitimate action on the basis of the plea of necessity. Besides, as the ILC's Draft Articles points out, the existence of an essential interest is not sufficient and the danger generated by a cyber operation must be grave and imminent, which basically means the destruction of a certain essential interest or its fundamental impairment, so that it becomes dysfunctional. This would be the case of the aforementioned basic infrastructure and its destruction or alteration with severe negative consequences for the State's security, economy, health system, or environment.⁶⁹

For the Tallinn Manual, the state of necessity can be used even if the response to the grave danger involves the infringement of the rights of other, non-responsible third States, as follows *a contrario* from Article 25(1)(b) of the ILC Draft Articles. Indeed, an objective limit is found in this provision, as a State could adopt a cyber-operation on the basis of necessity if it violates an international obligation, but could not do so if it seriously affects the essential interest of another State or the international community.⁷⁰ The Tallinn Manual chooses an example, which does not seem accidental, to explain this situation. In the case of cyber operations by non-State actors, where no State is responsible, the victim State can respond on the basis of state of necessity if this protects its essential interests, even if it thereby causes a breach in a non-responsible third State. However, if the response affects an essential interest of the third State, then the plea of necessity would not cover the response.

⁶⁶ Karine Bannelier and Théodore Christakis, *Cyber-Attacks. Prevention-Reactions: The Role of States and Private Actors* (Paris: Les Cahiers de la Revue Défense National 2017), 38-39.

⁶⁷ Antonio Segura Serrano, 'Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructure', *European Journal of Law and Technology* 6 (2015), 1-24 (1 f.).

⁶⁸ Government of The Netherlands (n. 8), 8.

⁶⁹ Schmitt, 2017 (n. 9) 136-137.

⁷⁰ James Crawford, *State Responsibility – The General Part* (Cambridge: Cambridge University Press 2013), 312.

Another problematic issue is whether the state of necessity also provides justification for reactions in cyber operations of unknown origin. The Tallinn Manual is inclined to consider that the state of necessity could cover responses that can take the form, for example, of a computer shutdown of another's infrastructure, or even counter-hacking. Furthermore, this type of response can be anticipated, as it is sufficient that the danger is imminent, as stipulated in Article 25(1)(a) of the ILC Draft Articles, without having to wait until it has actually taken place. The Netherlands concurs with the Tallinn Manual on both points.⁷¹

In short, the state of necessity offers a series of advantages, from the legal point of view, which have attracted a certain part of the literature and particular countries, e.g. The Netherlands, especially at the present time when the normative process has made little progress in relation to cyberspace, as we will see. First, the application of the plea of necessity does not depend on the prior attribution to a State of a wrongful act, so it is particularly interesting when acting against non-State actors. Furthermore, the plea of necessity can be activated even in the absolute absence of a previous international wrongful act. For these two reasons, the state of necessity has been considered the most appropriate instrument for reacting to the cyber-activities of non-State actors. However, this is a theoretical possibility rather than a legal certainty, since the very restrictive conditions for invoking the plea of necessity, in particular the fact that it is the 'only way for the State to safeguard an essential interest', make it very difficult to apply this plea in practice.⁷² In addition, if the state of necessity was to be used by States on a regular basis, the normalisation of this exception would lead to a 'slow erosion of the rule of law'.⁷³ Therefore, this paper considers the state of necessity an option that will not be available to States in their day-to-day cyberspace business, as it entails an evolutionary interpretation of the international law customary rules that runs counter the limited scope this plea of necessity received by the ILC.

3. Due Diligence Obligation

One way for overcoming the problems of attribution in international responsibility is that proposed by the Tallinn Manual in Rules 6 and 7 on the

⁷¹ Government of The Netherlands (n. 8), 8.

⁷² Bannelier and Christakis (n. 66), 36-39; Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', *The Yale Law Journal Forum* 125 (2015-2016), 68-81 (78).

⁷³ Lahmann (n. 45), 265.

obligation of due diligence. It is understood that this obligation is based on the *Corfu Channel* case,⁷⁴ in particular on the principle of avoidance of damage, which is often applied in international environmental law.⁷⁵ Such due diligence would obviate the question of attribution, holding the State from which the cyber activities originated responsible on the basis of its inaction to prevent or avoid such harmful activities. The core elements of the due diligence obligation are not perfectly outlined in international law.⁷⁶ However, this obligation comprises at least two elements, the duty of prevention and the duty of knowledge,⁷⁷ whose more or less wide interpretation determines a more or less demanding obligation in relation to the State to which it applies.

Some authors argue that due diligence is required not only for cyber activities that the State is aware of, but also for those that it should have been aware of. This criterion is called constructive knowledge and the Tallinn Manual concedes that it is controversial in international law. There are certain factors that help determine whether the State should have known, such as whether the State's governmental cyber infrastructure was used, or whether the malicious activities consisted of denial of service (DDoS) attacks, which imply extensive use of bandwidth, etc.

With regard to the damage, the Manual understands that this rule applies to all cyber operations that are 'contrary to the rights' of the States concerned (to use the wording of the *Corfu Channel* case) under international law, and that involve serious adverse consequences. However, the threshold to be reached by the damage is an unresolved issue, although the Manual is inclined to consider that damage to things or injury to persons is not essential⁷⁸ as, for example, interference with critical infrastructure or a serious impact on the economy would be sufficient.

With regard to the element of prevention, some literature advocates that it includes the rule of reasonableness together with the duty of the State to adopt the necessary legislation to prevent.⁷⁹ However, the Tallinn Manual is

⁷⁴ ICJ, *Corfu Channel* case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ Reports 1949, 22.

⁷⁵ Jovan Kurbalija, 'State Responsibility in Digital Space', *Swiss Review of International and European Law* 26 (2016), 307-326.

⁷⁶ International Law Association, Study Group on Due Diligence in International Law, Second Report, 2016, 7.

⁷⁷ Russel Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Trans-boundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429-453, framing these elements in the form of an obligation of result (to have sufficient legislation and administrative apparatus) and an obligation of conduct (to use that capacity diligently).

⁷⁸ Government of The Netherlands (n. 8), 5.

⁷⁹ Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low Intensity Cyber Operations?', *Baltic Yearbook of International Law* 14 (2014), 23-39.

more conservative and upholds that the duty of care, first, requires States to effectively stop malicious cyber operations, both those that are occurring and those that are in preparation and are warned. Secondly, however, the Manual considers that there is no general obligation of prevention in cyberspace beyond the best efforts test, since this is an obligation of conduct, not result. In this sense, the State is not obliged to monitor activity in networks, which can lead to the violation of internationally protected human rights,⁸⁰ nor is it obliged to adopt institutional or legal measures to comply with this obligation.

As can be seen, the Tallinn Manual has analysed in detail the ins and outs of the due diligence obligation, and the editor himself, Prof. Schmitt, has endeavoured to highlight the advantages of its application in cyberspace. The main advantage of due diligence is that it can be invoked against malicious activities by non-State actors. In the case of activities of non-State origin, no countermeasures can be applied, as countermeasures can only be taken if the unlawful acts can be attributed to a State. Nor is it easy to invoke a plea of necessity, whose threshold for application is high because, as is well known, an essential interest and a grave peril must be present. On the contrary, due diligence would allow the attacked State to respond with a cyber-countermeasure against non-State actors. This response, which would initially infringe the sovereignty of the State targeted by the countermeasure, would nevertheless find legitimacy in the unlawfulness consisting of the prior breach of due diligence. Yet, the proportionality of the countermeasure in this case would have to be determined, not in relation to the seriousness of the malicious acts committed by the non-State actors, but in relation to the seriousness of the omission committed by the State which infringed the due diligence.

However, some authors have criticised the formulation of the due diligence obligation in the Tallinn Manual. Indeed, firstly, it has been pointed out that due diligence can lead to a destabilisation of international relations as a result of a proliferation of cybernetic countermeasures.⁸¹ Likewise, as France has warned, there is a certain risk that the due diligence obligation be used as an excuse to legally resort to the use of force.⁸² Secondly, and to the contrary, another part of the literature has stressed that the Tallinn Manual sets an

⁸⁰ Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', *Harv. Int'l L.J.* 56 (2015), 81-146.

⁸¹ Eric T. Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', *Tex. L.Rev.* 95 (2017), 1555 -1577. These authors are members of the international group of experts of the Tallinn Manual 2.0.

⁸² Ministère des Armées (n. 8), 10, where France is cautioning that «(L)e non-respect de l'obligation de diligence requise par un État tiers ne suffit pas à fonder le droit de recourir à la force à son encontre dans le cadre de cyberattaques perpétrées depuis son territoire».

unclear standard, the application of which is uncertain, as States that are victims of a cyberattack carried out by non-State actors from the territory of a third State are going to encounter many legal difficulties in articulating a right of response.⁸³ Despite this, the latter literature also stresses that recent practice seems to be moving towards a less demanding standard of due diligence.

In this vein, some States have expressed their opposition to this due diligence, or have remained silent, such as the US and the UK,⁸⁴ because of the scope of obligations it may create to them, especially for these States which are more connected to the network and which could bear the heaviest burden.⁸⁵ According to this, the 2013 and 2015 GGE Reports simply note that 'States [...] should seek to ensure that their territory is not used by non-State actors to commit [internationally wrongful acts]'.⁸⁶ Indeed, this formulation has been included in the UN GGE Report 2015 not as rule of international law, but as a voluntary and non-binding norm, which in turn anticipates the legal weight UN Member States are willing to attribute to it. The OEWG Report 2021 has not even mentioned the due diligence obligation.

As can be seen, the current customary formulation of the due diligence obligation is much less demanding than the one adopted in the Tallinn Manual. In other words, the Tallinn Manual has set up a standard of due diligence that States are unwilling to assume at this time, as demonstrated by the practice of using proxies,⁸⁷ as well as by the widespread refusal to conduct ongoing monitoring of activities taking place in cyberspace.⁸⁸ Therefore, the due diligence obligation must not be taken as panacea, as there are important limitations to its dynamic applicability in this field of cyberspace. The challenge of cybersecurity needs to be met but this kind of wide formulation of international law rules may be counterproductive compared to other avenues, even if in the long run, like norm-development.

III. Cybercrime as a Test Case of Norm-Development

From a holistic approach, international cooperation to tackle cybercrime should be a priority for international lawyers, thereby going beyond the

⁸³ Efrony and Shany (n. 12), 592-593.

⁸⁴ Egan (n. 21), 169; Wright (n. 21).

⁸⁵ Schmitt (n. 72), 78.

⁸⁶ UNGA, 2013 GGE Report (n. 10), para. 23; UNGA, 2015 GGE Report (n. 10), para. 28 (e).

⁸⁷ Maurer (n. 18), 383 f.

⁸⁸ Eric T. Jensen, 'Cyber Sovereignty: The Way Ahead', *Tex. Int'l L.J.* 50 (2015), 275 (299).

traditional contours of peace and security with the aim of globally addressing the issue of cyberattacks. In this vein, it is true that cyber-attacks attributable to non-State actors are to be dealt by State authorities through the application of domestic law. Yet, international law's jurisdictional rules may be insufficient in order to solve the new issues posed by cyberspace. Therefore, norm-development efforts have been crucial in this field, with the Budapest Convention on Cybercrime as the main test case to be analysed.

1. Jurisdictional Issues

States can exercise their jurisdiction, and in fact are doing so, over cybernetic activity that is oriented towards a specific territory and has a local effect, bypassing the instrument used (Internet).⁸⁹ Yet, this paper claims that the exercise of State jurisdiction should be improved so as to allow for more coordination in this field. Indeed, State jurisdiction may be facilitated in the future if there is international consensus, as the example of the Budapest Convention on Cybercrime shows, even if in turn this Convention should be upgraded to achieve its goals.

Certainly, the bases of territory and nationality are being used normally in the exercise of State jurisdiction over cyberspace, as derived from Article 22 (1) of the 2001 Budapest Convention on Cybercrime, drawn up in the framework of the Council of Europe. These bases are sufficient to ensure the connection between acts of cybercrime and at least one State.

a) Territorial Jurisdiction

The exercise of territorial competence is full in relation to persons and objects located in the State territory, as warned in the Reports of the Groups of Governmental Experts of 2013 and 2015, which expressly refer to ICT infrastructures.⁹⁰ However, the Tallinn Manual also extends this territorial competence to data located on State territory. In addition, the Tallinn Manual considers that States that are intermediaries in a transnational cyber activity can also exercise their territorial jurisdiction if their infrastructure is used in

⁸⁹ Édouard Treppoz, 'Jurisdiction in the Cyberspace', *Swiss Review of International and European Law* 26 (2016), 273 (275).

⁹⁰ UNGA, 2013 GGE Report (n. 10), para. 20; UNGA, 2015 GGE Report (n. 10), paras 27 and 28.a.

that activity. In contrast, the experts who have prepared this Manual have not reached agreement on whether the States used for data transit can exercise the same territorial jurisdiction, given that in this case the connection with this infrastructure is minimal.⁹¹

The Tallinn Manual also reflects the *Lotus*⁹² doctrine of subjective and objective territorial jurisdiction, i. e. cyber-activities that respectively originate or are completed on the territory of the State are subject to its jurisdiction. In other words, it is the jurisdiction that may be exercised by a State which happens to be the place of distribution or the place of reception of information circulating in cyberspace.⁹³ Subjective territorial jurisdiction is not appropriate in cyberspace because of the limitation it implies for the protection of the values and public policy options of the territorial State, making forum shopping by online operators very easy.⁹⁴ On the contrary, objective territorial jurisdiction, which is defined as that exercised by the State when none of the constituent elements of the crime occurs on the territory of the State exercising jurisdiction, tends to be too inclusive, which creates problems of overlap between jurisdictions.

Finally, the Tallinn Manual also echoes the effects doctrine, to which it attributes the status of customary law. This type of exercise of territorial jurisdiction is prevalent in cyberspace, since the latter allows the implementation of activities that cause effects in States in whose territory they do not originate or are not completed. In fact, malicious activities in cyberspace often seek precisely to affect a multitude of States simultaneously. However, this effects doctrine is problematic because it creates legal uncertainty by allowing a large number of States to claim the exercise of jurisdiction simultaneously. On the basis of the *Lotus* case, the effects doctrine has been applied in cyberspace with great laxity by States. Thus, mere accessibility has been used as a criterion to subject an activity to the jurisdiction of the territorial State from which a content is accessible, as happened in the *Yahoo!* case.⁹⁵ There have been efforts to refine the effects doctrine through the targeting principle. In the framework of this new rule of reason, an activity that has effects on and is oriented towards a specific territory is subject to State jurisdiction, as was the case in the *Google Spain* judgment decided by the

⁹¹ Schmitt, 2017 (n. 9), 55.

⁹² PCIJ, *S.S. Lotus* (France v. Turkey.), 7 September 1927 P. C. I. J. (ser. A) No. 10, 23.

⁹³ Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law', *Tex L. Rev.* 88 (2010), 1571 (1573).

⁹⁴ Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface', *EJIL* 19 (2008), 799 (811).

⁹⁵ Segura-Serrano (n. 16), 202, analysing the procedural path followed by this case in France and the United States.

Court of Justice of the European Union (CJEU).⁹⁶ This targeting principle appears to be the best balance between, on the one hand, *de facto* universal jurisdiction, to which the broad version of the effects principle (and, also, objective territoriality⁹⁷) leads, and, on the other hand, the approach based on the principle of origin (or exclusive subjective territoriality), which would prevent States from exercising their regulatory autonomy over their territories in relation to the online activities to which they are subject.

b) Extraterritorial Jurisdiction

The previous analysis serves us to evaluate the risks posed by the rules proposed to be applied extraterritorially. Regarding extraterritorial jurisdiction, enforcement is the most pressing issue in the field of cyberspace. Rule 11 of the Tallinn Manual is framed as meaning that extraterritorial enforcement jurisdiction is justified only where there is a specific international law qualification, or there is consent by the territorial State, as in the *Lotus* case, a rule which is considered too rigid for cyberspace. In other words, the extraterritorial executive competence of the State is much more limited than legislative or judicial competence, which in cyberspace generates an obvious result of an executive or enforcement gap that has, however, been filled through measures such as voluntary compliance or local blocking of online content.⁹⁸ As a result, one State, for example, cannot hack into servers located in another State to obtain evidence. However, the Manual's assertion that evidence may well be obtained without violating international law when it cannot be determined with certainty in advance in which particular country such digital evidence is located is highly problematic. Similarly, the Manual states that it would be lawful to obtain data, now in the exercise of territorial jurisdiction, when accessing public content, although it is available on servers located in another country. Even if this content is not publicly available, but protected by passwords or otherwise, but ultimately intended to be available. This extensive reading of extant international law rules should be criticised, as it would offer technological powerful States an advantage to overreach

⁹⁶ ECJ, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgement of 13 May 2014, Case no. C-131/12, ECLI: EU:C:2014:317.

⁹⁷ Uta Kohl, 'Who Has the Right to Govern Online Activity? A Criminal and Civil Point of View, International Review of Law', *Computers & Technology* 18 (2004), 387 (401).

⁹⁸ Uta Kohl, 'Jurisdiction in Cyberspace' in: Nicholas Tsagourias and Russel Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar 2015), 30, 53.

from a jurisdictional point of view. Finally, the Manual's group of specialists could not agree on whether contacting private storage service providers, located abroad, to request the voluntary provision of information is contrary to the exclusive executive jurisdiction of the territorial State.⁹⁹ As we will see, normative efforts are being developed nowadays in order to achieve this result, as the US Cloud Act and the proposed E-evidence Directive show.¹⁰⁰ However, this is an issue that is in need of elucidation from a legal point of view, as it may create uncertainties and potential conflicts between States in favour and against such a rule. Therefore, norm-development efforts to improve international cooperation in the cybercrime realm are much needed, at the regional and global level alike.

2. Cybercrime

a) Preliminary Remarks Regarding Norm-Development

The UN's activity has been very prolific in terms of cybersecurity and has to a large extent endorsed the option consisting of the application of international law rules to this field of cyberspace. It is the Groups of Governmental Experts established within the framework of the United Nations General Assembly (UNGA) First Committee that have attracted the most attention. If the first Group in 2004 was unable to prepare a final report due to a lack of consensus¹⁰¹ (Russia wanted to advance in setting new rules and the United States objected that the current ones are sufficient), the second Group did reach in 2010 the consensus necessary to establish areas of cooperation in responsible State behaviour, as well as capacity-building and confidence-building measures (reiterated in subsequent reports).¹⁰²

In the 2013 GGE Report, an agreement was reached regarding the applicability to cyberspace of existing international law, specifically, the UN Charter, human rights, as well as the basic rules on international responsibility.¹⁰³ Similarly, the 2015 GGE Report insisted on the applicability in cyberspace of

⁹⁹ Schmitt, 2017 (n. 9), 68-70.

¹⁰⁰ See Section III.2. on cybercrime.

¹⁰¹ UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 5 August 2005, A/60/202, 2.

¹⁰² UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 30 July 2010, A/65/201, 2-9.

¹⁰³ UNGA, 2013 GGE Report (n. 10).

some principles of international humanitarian law (such as proportionality or distinction), as well as of the obligation of due diligence.¹⁰⁴ Some important private initiatives have supported this option, such as the Tallinn Manual, promoted by NATO, and which makes an exhaustive analysis of this evolutionary application as *lex lata*,¹⁰⁵ as we have seen.

By contrast, the second option, consisting of the elaboration of new international rules, has been championed by Russia, China, and other countries, which have made several proposals over the years such as the 2011 Code of Conduct for Information Security, updated in 2015.¹⁰⁶

The contrast between these two options has been highlighted in the 2017 GGE Report, which has been deemed a failure.¹⁰⁷ Indeed, issues such as the recourse to self-defence, countermeasures, or the explicit recognition of certain norms of international humanitarian law have been rejected by countries such as Russia, China, or Cuba, on the grounds that Western countries are pursuing the militarisation of cyberspace. This failure may lead to think that the multilateral route is closed and that States are going to resort to the unilateral or regional route.

However, at the end of 2018, two working groups have been created within the framework of UNGA.¹⁰⁸ On the one hand, a new GGE sponsored by the US, with 25 government representatives, has been launched (UNGA Resolution 73/266) and, on the other hand, an Open-ended Working Group promoted by Russia has been created (UNGA Resolution 73/27). The latest group is not incompatible with the former and purportedly more inclusive, as it may incorporate all members of the UN. These two parallel tracks have been recently confirmed,¹⁰⁹ despite the efforts made in order to merge both

¹⁰⁴ UNGA, 2015 GGE Report (n. 10).

¹⁰⁵ Schmitt, 2017 (n. 9), 2-3.

¹⁰⁶ UNGA, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General of 14 September 2011, A/66/359; UNGA, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General of 13 January 2015, A/69/723.

¹⁰⁷ Stefan Soesanto and Fosca D’Incau, ‘The UN GGE is dead: Time to Fall forward’, 15 August 2017, <<https://www.ecfr.eu>>.

¹⁰⁸ UNODA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, <<https://www.un.org/>>, introducing a good account of both processes.

¹⁰⁹ UNGA, First Committee, Resolution on Advancing responsible State behaviour in cyberspace in the context of international security, 5 October 2020, A/C.1/75/L.4 (sponsored by the U.S.); UNGA, First Committee, Resolution on Developments in the field of information and telecommunications in the context of international security, 26 October 2020, A/C.1/75/L.8/Rev.1 (sponsored by Russia).

initiatives, e. g. through the Programme of Action.¹¹⁰ The OEWG has already produced its first Report,¹¹¹ though its work will continue with the setting up of a 2021-2025 OEWG (UNGA Resolution 75/240). The most recent development in this field has been the adoption of a GGE Report on 28 May 2021 (not officially published yet), which insists on the applicability of IHL to cyber operations during an armed conflict, together with the due diligence as a voluntary norm. This outcome shows a new, more pro-normative attitude among the UN member States, although it may be at the cost of a slower and more complex process. This pro-normative activity may also be a kind of government reaction to the various private efforts that are taking place recently. Indeed, in addition to the so-called Hague process, in which the 2017 Tallinn II Manual is to be placed, the initiative regarding the Digital Geneva Convention, promoted by Microsoft since 2017,¹¹² has a prominent role.

b) The Budapest Convention on Cybercrime

If this is what happens at the level of general international regulation regarding cybersecurity, in the most limited area of cybercrime there has been a particular evolution worth of analysis. From the holistic approach towards cybersecurity taken in this paper, we consider cybercrime as a test case where some progress has been achieved regarding the fight against cyber-attacks. This advancement in the cybercrime realm has also been encouraged by the pervasiveness of cyberattacks of private origin, which creates an increasing cost, above \$800 billion annually, according to a 2018 report.¹¹³ Therefore, the advanced international cooperation achieved in this field makes it appropriate to focus our attention on this process.

In the field of cybercrime, the Budapest Convention was already adopted in 2001 within the framework of the Council of Europe. It is a convention that very early exemplified the possibilities of successful international cooperation. This convention involves a minimum harmonisation in jurisdictional matters and, specifically, on issues regarding access to digital evidence. Unilateral transborder searches are provided in very limited cases: where the data is publicly available (Art. 32(a)) or disclosed on a voluntary basis (Art. 32

¹¹⁰ <<https://front.un-arm.org>>.

¹¹¹ UNGA, 2021 OEWG Report (n. 11).

¹¹² Brad Smith, 'The Need for a Digital Geneva Convention', 14 February 2017, <<https://blogs.microsoft.com>>.

¹¹³ Paul Dreyer *et al.*, 'Estimating the Global Cost of Cyber Risk, Methodology and Examples', RAND, (2018), <<https://www.rand.org>>.

(b)). However, as in other instances of international legal cooperation, this convention is weighed down by a significant slowness in assistance between Party States (requests take months to be answered), which leads many States to alternatively resort to bilateral instruments known as Mutual Legal Assistance Treaties (MLATs).¹¹⁴ From a different perspective, it has also been pointed out by NGOs that this Convention allows States to circumvent national safeguards protecting human rights.¹¹⁵

As a consequence of the limited effectiveness of the international legal cooperation implemented through the Budapest Convention,¹¹⁶ States have begun to resort to unilateral mechanisms to deal with the phenomenon of cybercrime of a transnational nature. One of those unilateral avenues is through cross-border hacking. So far, no State has formally charged other States of this type of practice. However, the certainty about the existence of this sort of capabilities indicates that their use has already been carried out in particular situations.¹¹⁷ On the other hand, there is another unilateral way to access digital evidence, such as the one that involves obtaining direct collaboration from foreign service providers. The advantage of this option is that it makes the intervention of the authorities from the destination or territorial State unnecessary for the requesting State to have access to electronic evidence. This possibility is provided by the 2018 US Cloud Act¹¹⁸ and it is also envisaged in the proposed E-evidence Directive, which includes a European Production Order.¹¹⁹

Precisely, the Council of Europe is trying to address the current under-utilisation of the Budapest Convention, so it has started the negotiations leading to the adoption of a new Protocol to the 2001 Convention. This new Protocol aims to introduce simplification in the process of legal assistance between Party States, thus improving the cooperation obtained to date in this regard. The end-result that the Protocol intends to reach would allow the

¹¹⁴ Miriam F. Miquelson-Weismann, 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?', *John Marshall Journal of Computer & Information Law* 23 (2005), 329 ff.

¹¹⁵ Anne Peters, 'Russia and China Are Trying to Set the UN's Rules on Cybercrime', 16 September 2019, <<https://foreignpolicy.com>>.

¹¹⁶ UNODC, *Comprehensive Study on Cybercrime*, 2013, 201 <<https://www.unodc.org/>>, according to which, in transnational cybercrime cases, 'only in 25 per cent of cases were international and regional instruments cited as the legal basis'.

¹¹⁷ Philippe Jougoux, Tatiana E. Synodinou and Lilian Mitrou, 'Criminalization of Attacks against Information Systems' in: Ioannis Iglezakis (ed.), *The Legal Regulation of Cyber Attacks* (Alphen aan den Rijn: Kluwer Law International 2020), 116.

¹¹⁸ EPIC, 'The Cloud Act', <<https://epic.org>>.

¹¹⁹ European Council, 'E-evidence Package: Council Agrees its Position on Rules to Appoint Legal Representatives for the Gathering of Evidence', 8 March 2019, <<https://www.consilium.europa.eu>>.

State of origin to make prevail its applicable rules on the matter as a consequence of the exercise of its jurisdiction to prosecute the cybercrime in question. In the meantime, the Council of Europe (CoE) Cybercrime Convention Committee has produced a 2017 Guidance Note on Production Orders, with the aim to address the issue of the storage of data outside the investigating State's territory. Yet, this Guidance has been criticised as a unilateralist transborder access to electronic evidence promoted via soft law.¹²⁰

However, several NGOs have condemned this attempt to elaborate a new Protocol, since they consider that it will surely entail an erosion of the applicable legal standards in the destination State.¹²¹ Taking into account that not only is there no harmonisation of criminal laws among the States of the Council of Europe, but that the national legal systems are very diverse, the areas that could be most affected would be those related to human rights protected in the territorial State, among which must be highlighted the right to privacy and the protection of personal data, as well as the procedural safeguards applicable in that destination State.

c) Developments at the UN Level

Within the United Nations, a proposal by Russia for a Convention on Cybercrime was rejected as early as 2010.¹²² In 2011, the Commission on Crime Prevention and Criminal Justice (CCPCJ) created an Expert Group, at the request of the General Assembly, to carry out an exhaustive study on cybercrime, in order to prepare legal or otherwise, national or international responses, to confront this phenomenon.¹²³

This comprehensive study on cybercrime was commissioned from the UN Office on Drugs and Crime (UNODC) and completed in 2013.¹²⁴ The work of the Group of Experts will continue until 2021 when it is scheduled to complete its task. However, there is disagreement within the UN on how to tackle the scourge of cybercrime. On the one hand, the US and its allies

¹²⁰ Paul de Hert, Cihan Parlar and Juraj Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law', *Computer Law & Security Review* 34 (2018), 327 ff.

¹²¹ EDRI, 'New Protocol on Cybercrime: a Recipe for Human Rights Abuse?', 25 July 2018, <<https://edri.org/>>; Katitza Rodríguez, 'The Cybercrime Convention's New Protocol Needs to Uphold Human Rights', 18 September 2017, <<https://www.eff.org/>>.

¹²² ITProPortal, 'UN Rejects Russian Cyber-Crime Treaty', 21 April 2010, <<https://www.itproportal.com/>>.

¹²³ UNODC, 'Global Program on Cybercrime', <<https://www.unodc.org/>>.

¹²⁴ UNODC (n. 116).

understand that the Budapest Convention is the most adequate ongoing effort to fight cybercrime. Furthermore, the work of the Group of Experts is nearing completion, so that at present it is most convenient to wait to evaluate the results of that work, according to them. On the other hand, Russia and other States have stated that they prefer the elaboration of a new universal text that conveys a global consensus, therefore, a consensus that is not limited to the States party to the Council of Europe. Furthermore, in their opinion, certain mechanisms of the Budapest Convention, such as Article 32(b), constitute an attack on the sovereignty and the jurisdictional authority of the territorial State, since it implies the possibility of evading the prior authorisation of said State on the occasion of obtaining electronic evidence.¹²⁵

In this context, some Western countries were shocked as a Proposal for a Convention on Cybercrime has been recently approved by the UNGA at the end of 2019. Indeed, the majority reached to adopt Resolution 74/247 has shown a divisive vote (79-60-30), but this time in favour of the normative proposal. The projected convention is based on a draft submitted by Russia in 2017.¹²⁶ This draft comprised a list of prosecutable cybercrimes (including hacking), the various options for legal cooperation between States, as well as the setting-up of an International Technical Commission. In order to move forward the proposal approved by the UN in 2019, the creation of an open-ended ad hoc intergovernmental committee of experts has been envisaged.

However, this UN proposal has been criticised by Non-Governmental Organizations (NGOs). In an open letter to the UNGA,¹²⁷ 36 human rights groups consider that, Russia being its main promoter, the proposal can only lead to greater criminalisation of conduct on the Internet, in line with the larger State control that nations such as Russia or China promote on the Internet. In their opinion, this proposal seeks to go beyond the provisions set forth in the Budapest Convention, so that the possibility of rejecting requests for assistance by the host State is diminished. Furthermore, according to them, the CCPCJ's Group of Experts should be allowed to finish its work in 2021.

¹²⁵ Summer Walker, 'Cyber-Insecurities? A Guide to the UN Cybercrime Debate', *The Global Initiative against Transnational Organized Crime*, (2019), 5-6.

¹²⁶ UNGA, Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General of 16 October 2017, A/C.3/72/12.

¹²⁷ APC, 'Open letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online', 6 November 2019, <<https://www.apc.org/>>.

The proposal for a new UN Convention on Cybercrime is an example of the new, more pro-normative attitude that seems to be consolidating today. Indeed, on the one hand, the Budapest Convention gathers an experience of two decades, with ample approval among States, as there are 65 Party States and many of them have integrated it into their national legislation. In particular, it has been the subject of a Statement in Support from the EU, which, together with the US, rejects the UN proposal.¹²⁸

On the other hand, Russia, China and many developing countries argue that the Budapest Convention represents a limited club of States, far from the global consensus that can be reached at the UN.¹²⁹ In fact, this option for a new convention has been gaining weight among UN Member States, either because the foreign policy balances have been changing (there are State Parties to the Budapest Convention, including the Council of Europe, who have voted in favour of the proposal), or because there is a growing appeal around a new Global Treaty on this matter and the resulting reinforcement of State sovereignty that it may entail.

From a legal point of view, it should be borne in mind the consequences derived from the adoption of a new Convention on Cybercrime, which, like the Budapest Convention, seeks to attain global implementation. If there were two conventions on the same subject, it will be necessary to resort to Article 30 of the Vienna Convention on the Law of Treaties in the event of a concrete application. Regardless of the solution to be adopted in each case, by way of a sort of bilateralisation, the truth is that the existence of two general legal frameworks on the same subject is not going to help simplify legal assistance between States. However, as in the case of Human Rights, it may very well be the case that the existence of various self-contained regimes on this subject-matter do not run counter the objective sought, but to the contrary make it more probable the occurrence of international cooperation being achieved in the instance.

IV. Final Remarks

From the point of view of international law, there remain many issues to be solved regarding cybersecurity, either through evolutionary application or norm-development processes.

¹²⁸ EEAS, 'EU Statement in Support of the Council of Europe Convention on Cybercrime', 15 January 2020, <<http://eeas.europa.eu>>.

¹²⁹ UNGA, Official Records, 52nd Meeting of 19 December 2019, A/74/PV.52 (36).

As we have seen, dynamic application of international law in cyberspace is not panacea,¹³⁰ specifically when relating to the enforcement of international responsibility rules for wrongful acts committed in cyberspace. The UN GGE Reports of 2013 and 2015, as well as the Tallinn Manual, generally take a conservative position on the rules of international law applicable in cyberspace. Not surprisingly, both documents claim to reflect customary law as it applies in this area, although the Tallinn Manual goes much further in its ambition to provide detailed regulation on the subject.

However, it can also be inferred from the analysis above that the Tallinn Manual and some States are inclined to flexibly interpret very particular legal issues, specifically regarding a strong unilateral State's right of reply in case of infringement of international obligations. In particular, it is to be highlighted the main role ascribed to countermeasures and the due diligence obligation, until now very limited to certain special regimes, as a way of ensuring a State's ability to respond to malicious actions carried out on the Net by non-State actors, an aim which, considered in itself, is obviously laudable.

Nevertheless, this kind of reformulation of the due diligence obligation and its use as a means of justifying the implementation of legitimate countermeasures could alter contemporary international relations if States entered into a dynamic of normalisation around their adoption. Indeed, the risk of escalation in such an event exists and should not be underestimated. Fortunately, however, as mentioned earlier, this practice is not being generally observed as States follow an overall strategy of 'wait and see'. Even so, this proposal, which encourages the somewhat exponential use of perfectly legitimate international legal instruments, is preferable to other proposals that seek precisely the opposite, that is, to undermine international legal rules to make way for the law of the strongest. Indeed, some authors seek to lighten the normative 'burden' arising from the existence of certain international legal norms, for example, that relating to State sovereignty, which would enable States to take a more proactive action in cyberspace, on the basis of the greater technological capacity that some enjoy.¹³¹

Likewise, norm-development is nowadays a very complex and slow process regarding cybersecurity. There is an absence of normative consensus in the international arena, which in turn reveals the confrontation between the position of the US and Western countries, on the one hand, and that of Russia, China, and many DCs, on the other hand. The former countries

¹³⁰ *Contra*, François Delerue, 'The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?', *ESIL Reflections* (2018), 4.

¹³¹ Corn and Taylor (n. 4).

advocate an evolutionary application of existing standards to cyberspace, while the latter prefer the development of new international rules, as expressed by the OEWG Chair's Summary.¹³² The root causes of this lack of consensus are both political, in terms of an open Internet and protection of human rights versus a closed Internet, together with greater State control; and strategic, in terms of the protection of the current technological advantage some enjoy versus the modification of the *status quo*.

This absence of consensus is dangerous for the stability of international relations, as well as for the ability to stop cyberattacks, in addition to the abandonment of State functions that it implies and that explains the proliferation of private regulatory initiatives. Moreover, in the most specific area of cybercrime, a certain paradox is emerging. Perceptions about the defence of State sovereignty at all costs, for whatever reason, prevent progress in terms of norm-development. However, greater cooperation in this field would lead to more effective protection of State interests since, in the current situation, unilateral whims remain frequent.

Even if there are objective reasons to call for either specific primary norms or specific norms of attribution,¹³³ the lack of agreement among big powers is hindering in the short to medium term any norm-development effort, undertaken by the United Nations or otherwise. Only regional initiatives (European Union [EU], CoE) seem to have success, if geographically limited, which in turn may make it more difficult to achieve any advancement from the point of view of general international law. Yet, this outcome is not the only possible one, as witnessed in the Human Rights realm, where self-contained regimes and general international law have evolved on parallel with positive results.

Truly, there is an impasse situation regarding cybersecurity. On the one hand, evolutionary application has been useful to a certain extent until now, but some proposals have important limits when flexibility in interpreting international law rules may lead to destabilising international relations. On the other hand, norm-development which is much wanted to complete the gaps left by interpretation of existing international law is nowadays very slow and very difficult to achieve. However, improving cybersecurity is a public good that is in need of a solid fostering effort. Therefore, the central argument advanced in this paper was that international cooperation needs to be enhanced if we want international law to be relevant in the near future in addressing cyberattacks, both attributable and non-attributable to States.

¹³² UNGA, 2021 OEWG Chair's Summary (n. 37), para. 16.

¹³³ Andreas Zimmermann, 'International Law and "Cyber Space"', ESIL Reflections (2014), 3.

Hence this paper serves as a legal critique of the mainstream position expressed by many Western governments and scholars.

Firstly, this paper supports as a way forward the enhancement of the international cooperation needed to set up a centralised mechanism for attribution, through the establishment of an international council or otherwise, that helps in the task of making public attributions of wrongful cyber operations through a process of impartial fact-finding. This way, the allocation of international responsibility would achieve the legitimacy needed in this field, where we find very advanced technological States together with other States that do not have the same technological capabilities. This improvement would open the door to the adoption of more legitimate countermeasures, or even public sanctions (e. g., the EU Cyber Diplomacy Toolbox), diminishing the need to resort to bilateral countermeasures where attribution is not well proved, countermeasures instrumented through the due diligence obligation, or the difficult-to-justify state of necessity. The application of existing international law rules would be facilitated, instead of unnecessarily stretched, this way reinforcing the rules-based international order.

Second, the OEWG seems to be gaining ground as the central forum to accomplish the cybersecurity goal and the most convenient avenue to foster legal engagement among the main players. This is not to say that the GGE will not help to finally reach a much-needed agreement. However, even if the interests at stake are very much in opposition from the start, the OEWG deserves to be considered as a convenient setting where cybersecurity must be built up from a legal point of view. Likewise, in the more limited realm of cybercrime, a new majority within the UNGA points towards a growing consensus on a UN Convention on this topic. As we have seen, the issue of access to digital evidence is crucial in order to fight against cybercrime but it is a particularly delicate problem when jurisdictional overreach is perceived as infringing State sovereignty. The UN legal avenue is worth of exploring, as the work developed regarding jurisdictional cooperation in this field may also help advance the task of developing norms in other cybersecurity-related areas.

Internet and eDiplomacy: ‘Traditional’ Diplomatic Law in the Digital Era

Stefano Dominelli*

University of Genoa, Genoa, Italy

stefano.dominelli@unige.it

Abstract	733
Keywords	734
I. Introduction	734
II. ‘Diplomatic Communications’ Through Social Media	737
III. Diplomatic Premises, and ‘Virtual’ Embassies and Consular Posts	741
IV. Diplomatic Emails and Private ‘Inter-Net-Ferences’	744
1. Relevant Provisions Under the VCDR	745
2. Host State’s Obligations Under Arts 24 and 27(2) VCDR in <i>Bancoult</i>	745
3. ‘Inviolability’ Under the VCDR: Publicly Disseminated Cables and Open Issues	749
V. Online Crimes, and Diplomatic and Consular Privileges	750
VI. Closing Remarks	752

Abstract

The rise of internet and social media has changed, amongst others, international politics and international relations, putting the rules of the 1961 Vienna Convention on Diplomatic Relations under a stress test. The present work wishes to contribute to the current scholarly debate on whether already existing traditional rules of diplomatic law can easily be adapted to a post-modern world.

More in detail, it will be dwelled if and to what extent diplomatic privileges and immunities conceived for an ‘in person’ diplomacy can be applied to ‘eDiplomacy’ as well. The proper identification of notions such as ‘premises’, ‘archives’, or ‘correspondence’ are currently under debate, as is the regime of protection of diplomatic premises in cases of cyber-crimes. Additionally, at current times, it seems the most prominent issue relates to the possibility to use in court diplomatic protected documents illegally obtained. Under the 1961 Vienna Convention, it remains unclear whether an unlawfully obtained diplomatic cable is always inadmissible. More straightforward seem to be other issues of eDiplomacy, either because the existing legal framework appears sufficiently flexible to be interpreted in such a way as to cope with eDiplomacy, or because international diplomatic law is not applicable to such new scenarios, leaving the door open for States to elaborate original solutions, if they deem it opportune.

* Researcher in International Law, University of Genoa.

Keywords

Diplomatic Law – VCDR – diplomatic online communications – online diplomatic privileges

I. Introduction

The ‘digital revolution’ has brought significant societal changes in many countries of the world.¹ Legal narratives have evolved accordingly over time, exploring and unravelling topical issues² as there appear to be few areas of

¹ On the internet as one of the tools for social change, see *ex multis* Miriyam Aouragh and Anne Alexander, ‘The Egyptian Experience: Sense and Nonsense of the Internet Revolution’, *International Journal of Communication* 5 (2011), 1344-1358; on the efforts by States to ‘control’ the internet and limit its impact amongst the masses, see Kal Raustiala, ‘Governing the Internet’, *AJIL* 110 (2016), 491-503. Specifically on the control over the internet in China, see Katherine Tsai, ‘How to Create International Law: The Case of Internet Freedom in China’, *Duke J. Comp. & Int’l L.* 21 (2011), 401-430.

² On territorial sovereignty in the digital era, see Martti Koskenniemi, ‘What Use for Sovereignty Today?’, *Asian Journal of International Law* 1 (2011), 61-70; Henry H. Jr. Perritt, ‘The Internet as a Threat to Sovereignty? Thoughts on the Internet’s Role in Strengthening National and Global Governance’, *Ind. J. Global Legal Stud.* 6 (1998), 423-442 (425 ff.); Patrick W. Franzese, ‘Sovereignty in Cyberspace: Can it Exist?’, *A. F. L. Rev.* 64 (2009), 1-42; Benedikt Pirker, ‘Territorial Sovereignty and Integrity and the Challenges of Cyberspace’ in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallin: NATO CCD COE Publication 2013), 189-216; Wolff Heintschel von Heinegg, ‘Territorial Sovereignty and Neutrality in Cyberspace’, *International Law Studies* 89 (2013), 123-156; and Nicholas Tsagourias, ‘The Legal Status of Cyberspace’ in: Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar 2015), 13-29 (17 ff.); on warfare approaches and artificial intelligence see Michael W. Lewis and Emily Crawford, ‘Drones and Distinction: How IHL Encouraged the Rise of Drones’, *Geo. J. Int’l L.* 44 (2013), 1127-1166; Chantal Grut, ‘The Challenge of Autonomous Lethal Robotics to International Humanitarian Law’, *Journal of Conflict and Security Law* 18 (2013), 5-23; Marco Sassòli, ‘Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified’, *International Law Studies* 90 (2014), 308-340; Markus Wagner, ‘The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems’, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2541628>; Kjølv Egeland, ‘Lethal Autonomous Weapon Systems under International Humanitarian Law’, *Nord. J. Int’l L.* 85 (2016), 89-118; Alan L. Schuller, ‘At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law’, *Harvard National Security Journal* 8 (2017), 379-425; on online hate speech see Joseph Rikhof, ‘Hate Speech and International Criminal Law: The Mugesera Decision by the Supreme Court of Canada’, *JICJ* 3 (2005), 1121-1133; Antonio Segura-Serrano, ‘Internet Regulation and the Role of International Law’, *Max Planck UNYB* 10 (2006), 191-272; James Banks, ‘European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation’, *European Journal of Crime, Criminal Law and Criminal Justice* 19 (2011), 1-13; Federica Falconi, ‘Addressing Disability Hate Speech: The Case for Restricting Freedom of Expression in the Light of

human activities – and, consequently, branches of law – that are left unaffected by the development of information technology.

International diplomatic (and consular) law is no exception. A greater possibility to make recourse to computer-based resources in diplomacy³ changes the way foreign politics is expressed and international diplomacy is conducted. Recourse to social media by (some) Heads of States and politicians can increase the level of public participation in the decision-making

the ECtHR's Case Law' in: Carola Ricci (ed.), *Building an Inclusive Digital Society for Persons with Disabilities New Challenges and Future Potentials* (Pavia: Pavia University Press 2019), 69-81; on access to internet as a fundamental right see Steven Hick, Edward F. Halpin and Eric Hoskins (eds), *Human Rights and the Internet* (New York: Palgrave 2000); and Stephen Tully, 'A Human Right to Access the Internet? Problems and Prospects', HRLR 14 (2014), 175-195; and on private international law in the digital world see Anna Gardella, 'Diffamazione a mezzo stampa e Convenzione di Bruxelles del 27 settembre 1968', Rivista di diritto internazionale privato e processuale 3 (1997), 657-680; Manlio Frigo, 'Recognition and Enforcement of Judgments on Matters Relating to Personality Rights and the Recast of the Brussels I Regulation' in: Fausto Pocar, Ilaria Viarengo and Francesca C. Villata (eds), *Recasting Brussels I* (Milan: CEDAM 2012), 341-352; Susanne L. Gössel, *Internetspezifisches Kollisionsrecht? – Anwendbares Recht bei der Veräußerung virtueller Gegenstände* (Baden-Baden: Nomos 2014); Alex Mills, 'The Law Applicable to Cross-Border Defamation on Social Media: Whose Law Governs Free Speech in "Facebookistan"?', Journal of Media Law 7 (2015), 1-35; Giovanni Zarra, 'Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo Internet', Riv. Dir. Int. 98 (2015), 1234-1262; Dan Jerker B. Svantesson, *Private International Law and the Internet* (Alphen aan den Rijn: Wolters 2016); Simone Carrea, 'L'individuazione del forum commissi delicti in caso di illeciti cibernetici: alcune riflessioni a margine della sentenza Conurrence Sàrl', Diritto del commercio internazionale 31 (2017), 543-571; and Tobias Lutzi, *Private International Law Online* (Oxford: Oxford University Press 2020).

³ For example, for the purposes of increased capacities of direct communication between States without the necessity of the intermediation of diplomatic staff; enhanced capacity to collect relevant information over the internet with smaller sized permanent missions abroad; direct communication between nationals and (long distant) consular posts over email; to update communication channels between the sending State and its missions abroad; to organise pre-negotiations phases in bilateral or multilateral conferences or to possibly establish 'virtual diplomatic missions abroad' (as in the case of the US virtual Embassy in Iran in 2011, whose website was blocked for several hours by local authorities), see The White House, Office of the Press Secretary, Statement by the Press Secretary on Iran's Blockage of Virtual Embassy Tehran, 7 December 2011, available at <<https://obamawhitehouse.archives.gov>>; Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, Cambridge University Press 2017), 216; and Eytan Gilboa, 'Digital Diplomacy', in Costas M. Constantinou, Pauline Kerr and Paul Sharp (eds), *The SAGE Handbook of Diplomacy* (London: Sage 2016), 540-551 (544); on the greater recourse to IT in diplomacy, see *ex multis* Won-Mog Choi, 'Diplomatic and Consular Law in the Internet Age', Singapore Yearbook of International Law 10 (2006), 117-132 (118 ff.); Holger P. Hestermeyer, 'Vienna Convention on Diplomatic Relations (1961)' in Rüdiger Wolfrum (ed.), *MPEPIL* (Oxford: Oxford University Press 2009), 697-709, paras 28 and 43; Jovan Kurbalija, 'The Impact of the Internet and ICT on Contemporary Diplomacy' in: Pauline Kerr and Geoffrey Wiseman (eds), *Diplomacy in a Globalizing World. Theories and Practices* (Oxford: Oxford University Press 2013), 141-150; and Jovan Kurbalija, 'E-Diplomacy and Diplomatic Law in the Internet Era' in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallinn: NATO CCD COE Publication 2013), 393-424.

process with potentially positive effects on the democratic legitimacy of diplomacy and online negotiations may turn out less adversarial than *de visu* meetings.⁴ Of course, for ‘eDiplomacy’ to remain and flourish in the field of international relations and diplomacy, the legal framework should be as clear and predictable as possible. As it will be argued, this is not necessarily the case. Commenting some events that have taken place in recent years,⁵ the aim of this paper is to explore the persistent relevance of the main international treaties in the field of diplomatic relations contextualised in the framework of eDiplomacy. In other words, the paper aims to put the current international diplomatic law to a ‘stress-test’ and analyse if and to what extent emerging practices may be regulated by one of the most traditional branches of international law. By combining positivism and a policy-oriented approach, the present work will seek to reconstruct what is the law mainly under the 1961 Vienna Convention on Diplomatic Relations (VCDR)⁶ and the 1963 Vienna Convention on Consular Relations (VCCR)⁷ where electronic tools and resources have already been employed in the field of diplomatic law, to understand if and to what extent ‘traditional’ international diplomatic law is flexible enough to cope with the main current digital challenges. The overall argument will be that, despite some difficulties in terms of qualification of new ‘scenarios’ for the purposes of the applicability of the Vienna Conventions, such treaties remain a valid text. However, this does not mean that the conventions remain a good-for-all legal framework. Some questions may be

⁴ Stressing the consequences of ‘secrecy’ connected to e-negotiations, as ‘A negotiation process made in through such tools would become less visible to the public and thus the decision-making would be done without much pressure’, see Paula Sullaj, ‘Digitalization of Diplomacy: A New Way of Making Diplomacy?’, *Rivista elettronica del Centro di Documentazione Europea dell’Università Kore di Enna*, available at <<http://unikore.it>>. From a practical side, whereas this might pave the way to more ‘behaved’ discussions in bilateral meetings (and in meetings in general), in multilateral fora, a full online negotiation does not necessarily appear fully suited to ensure the best outcome and substantive equality in terms of participation to the negotiation. Moreover, in more general terms, the less ‘publicity’ to the event following the online nature could run counter the idea of democratic participation to foreign policy and international diplomacy as well. In the scholarship, cf also Choi (n. 3), 119.

⁵ Amongst the most ‘incumbent’ issues of eDiplomacy, the use of social media for diplomatic purposes and the applicability of relevant rules of diplomatic law; the establishment of virtual embassies and the applicability of rules on inviolability of premises; the possibility to use in court diplomatic cables unlawfully extracted from diplomatic archives and made freely available online (on which see UK Supreme Court, *R (on the application of Bancoult No 3) (Appellant) v. Secretary of State for Foreign and Commonwealth Affairs (Respondent)*, judgment of 8 February 2018, [2018] UKSC 3), and the possibility to overrule the principle of inviolability of diplomatic premises where cyber-crimes are either emanating from or attacking an Embassy.

⁶ UNTS, Vol. 500, 95.

⁷ UNTS, Vol. 596, 261.

too far away from the ‘traditional’ rules and their scope of application⁸, whilst other practical issues that have already emerged do not appear apt to be regulated by the Vienna Conventions because they exceed the reconstructed scope of application of the treaties.⁹

II. ‘Diplomatic Communications’ Through Social Media

Due to the lack of replies, the Swedish Minister for Foreign Affairs, in 2012, tweeted the Ministry of Foreign Affairs of Bahrain who – after answering to the Twitter shout-out – apparently made recourse to traditional channels for an official response.¹⁰ High ranking officials, and some Heads of States in particular,¹¹ make increasing recourse to instruments such as Twitter or Facebook in their domestic and international politics. This raises the issue of the legal status of such communications. However, two different scenarios should be separately considered and addressed; on the one side, social media communications from the diplomatic corps accredited within a State, and – on the other side – social media communications made from Heads of States or Governments, and from Ministers of Foreign Affairs.

As to the first case, under international diplomatic law, ‘All official business [...] entrusted to the mission by the sending State shall be conducted with or through the Ministry for Foreign Affairs of the receiving State [...]’.¹² At the same time, there is a principle of freedom of forms

⁸ For example, one of the fields where in the near future necessities for specific new rules may become urgent, is that of secrecy and data protection when diplomatic agents use third private parties applications for their reserved or secret communications (such as, e.g. Zoom or similar apps that have taken full potential out of the pandemic crisis). In this sense, it has become quite normal to see European Union videolink meetings where representative of States negotiate the content of a piece of legislation to be.

⁹ As may be the case for ‘diplomatic communications’ through social media, on which see *amplius infra*.

¹⁰ As reported by Andreas Sandre, *Twitter for Diplomats* (Lausanne: DiploFoundation and Istituto Diplomatico 2013), 28.

¹¹ One of the most notable examples probably being Donald Trump during his terms of office as President of the United States of America, on whose recourse to Twitter and ‘Twitter Diplomacy’, see Constance Duncombe, ‘Twitter and the Challenges of Digital Diplomacy’, *SAIS Review of International Affairs* 38 (2018), 91-100; and Maja Šimunjak and Alessandro Caliendo, ‘Twiplomacy in the Age of Donald Trump: Is the Diplomatic Code Changing?’, *The Information Society* 35 (2019), 13-25.

¹² Art. 41(2) VCDR. On which see Eileen Denza, *Diplomatic Law* (Oxford: Oxford University Press 2016), 382; and Niklas Wagner, Holger Raasch and Thomas Pröbstl, *Wiener Übereinkommen über diplomatische Beziehungen vom 18. April 1961: Kommentar für die Praxis* (Berlin: BWV Berliner Wissenschafts-Verlag 2007), 365.

for communications between the sending State and its missions abroad,¹³ and the convention is generally silent on the form of communication between the Embassy and the receiving State. Diplomatic practice has in this last regard developed a wide range of forms, such as the ones explicitly regulated within given legal systems, of First-Person Notes; Note Verbale; Memorandum; Aide-Memoire; Pro Memoria; Note Diplomatique; Note Collective; and Circular Diplomatic Notes.¹⁴ Yet, domestic laws of the receiving State may impose limitations as per the means of communication for specific acts, requiring for example a note verbale rather than other forms.

'Twitter diplomacy' from Ambassadors hardly fits established categories, and 'tweets' *may* fall within the scope of application of the VCDR only if i) communications are conducted through the Ministry of Foreign Affairs of the receiving State (Art. 42(2) VCDR); ii) if the latter does not at least prohibit 'Twitter diplomacy'; and iii) if a principle of freedom of forms can be transposed from the rules on communication between the Embassy and its State to the communication between the Embassy and the receiving State. From an historical perspective, States appear quite bound to a formalistic (and ritualistic) approach to international diplomacy, and a public tweet might be deemed to be in violation of the requirement to carry out official business 'through' the Ministry of Foreign Affairs of the receiving State. In other words, if 'tweets' *might* be acceptable under *formal* aspects, they can violate the rules concerning the *channel of communication*,¹⁵ with the consequence that diplomatic accredited corps should refrain from using it for official purposes (unless otherwise agreed between the States). Similar issues could rise for blogs used by diplomats to inform the public of the situation within their Host State – after the authorisation of their home countries.¹⁶ Such activity might not only breach the duty to communicate through the Ministry of Foreign Affairs of the receiving State, but it might also amount to an unduly interference with the national (domestic and international) affairs.

Perhaps more common and widespread is the recourse to social media in the last years by Heads of States or other top-ranking officials. In general

¹³ Art. 27(1) VCDR. See Ivor Roberts (ed.), *Statow's Diplomatic Practice* (Oxford: Oxford University Press 2009), 114.

¹⁴ On which see US Department of State, Foreign Affairs Manual and Handbook, 5 FAH-1 H-610 ff., Using Diplomatic Note, available online.

¹⁵ See Kurbalija, E-Diplomacy (n. 3), 423. See Art. 41(2) VCDR, according to which 'All official business with the receiving State entrusted to the mission by the sending State shall be conducted with or through the Ministry for Foreign Affairs of the receiving State or such other ministry as may be agreed'.

¹⁶ Denza (n. 12), 381.

terms, it can preliminary be noted that, despite the many legal doubts surrounding the use of social media in international law, these have been significantly used.¹⁷ However, the relevance of social media by Heads of States can be approached from different perspectives.

From the specific point of view of diplomatic law, the VCDR does not apply to the communication of Heads of States, regardless of the type of the communication. The treaty might nonetheless constitute a reference point at the interpretative level.¹⁸

For those unilateral acts which might fall within the material scope of application of diplomatic law, thus be characterised as unilateral diplomatic communications directed at other international actors, it has to be noted that State practice has developed a principle of freedom of forms. ‘Recognition’ of new States, and the intention to start diplomatic relationships have been communicated by various means, such as conference presses or phone calls.¹⁹

¹⁷ Whilst the constitutive elements of domestic practices can be drawn from a wide array of elements, caution is generally followed; see Second Report on the Identification of Customary International Law, by Michael Wood, Special Rapporteur, International Law Commission. Sixty-sixth session, 22 May 2014, A/CN.4/672, para. 29: ‘All evidence must be considered in light of its context. In assessing the existence or otherwise of the two constituent elements, be it by reviewing primary evidence or by looking to subsidiary means, great care is required. While “evidence can be taken [from a variety of sources] [...] the greatest caution is always necessary.” Much depends on the particular circumstances in determining what the relevant practice actually is and to what extent it is indeed accepted as law, and different weight may be given to different evidence. For example, “[p]articularly significant are manifestations of practice that go against the interest of the State from which they come, or that entail for them significant costs in political, military, economic, or other terms, as it is less likely that they reflect reasons of political opportunity, courtesy, etc.” In a similar manner, the care with which a statement is made is a relevant factor; less significance may be given to off-the-cuff remarks made in the heat of the moment’. See also International Law Commission, seventieth session, 2018, A/73/10, Draft conclusions on identification of customary international law, Conclusion 6(1) (‘Practice may take a wide range of forms. It includes both physical and verbal acts [...]’), whose commentary reads that ‘While some have argued that it is only what States “do” rather than what they “say” that may count as practice for purposes of identifying customary international law, it is now generally accepted that verbal conduct (whether written or oral) may also count as practice [...]’.

¹⁸ ICJ, *Arrest Warrant of 11 April 2000* (Democratic Republic of the Congo v. Belgium), Judgment of 14 February 2002, I. C. J. Reports 2002, 3 (para. 52).

¹⁹ On which see Carlo Curti Gialdino, *Lineamenti di diritto diplomatico e consolare* (Torino: Giappichelli 2015), 10 ff., and 68. The beginning of diplomatic relationships between the United States of America and the Holy See were announced by the respective press conferences in 1984, and in 1960 Cuba announced the establishment of diplomatic relationships with China – who was unaware of this intention but accepted and conformed accordingly. In December 2017, US President Donald Trump tweeted that ‘I have determined that it is time to officially recognize Jerusalem as the capital of Israel. I am also directing the State Department to begin preparation to move the American Embassy from Tel Aviv to Jerusalem’, thus showing how social media ‘declarations’ are followed by traditional diplomatic channels of communication, being more an ‘anticipation’ of subsequent possible official State positions.

If such an approach of freedom of forms for unilateral acts might have any value in the context of official social media unilateral communication, it would have to mean that, from the very specific focal lenses of diplomatic law, the nature of social media as a communication tool does not negatively affect the communication as ‘diplomatic communication’. Of course – the question, whose answer is everything but straightforward – is under which conditions expressions made through social media can amount to ‘unilateral declarations’ under international law and are for these purposes attributable to the State and exert effects on the plane of the international community generating obligations.²⁰

For bilateral acts, if the VCDR is again to offer any guidance, its underlying principle of mutual consent between States should at least suggest that State-to-State communication between Heads of States by way of social media, to be acknowledge or legally binding, should expressly be accepted as ‘diplomatic means of communication’. A solution that, from a practical perspective and taken into consideration the ritualistic approach that generally permeates the field, appears unlikely at least.

Outside these boundaries, social media should not be considered as means of diplomatic communication and diplomatic law should not be considered applicable. If a social media post is not considered a legitimate means of diplomatic communication, either because international diplomatic law is not applicable or because the ‘post’ tweeted by the politician is destined to a domestic audience (making the act ‘non-international’ in nature, even though with relevance on the field of foreign policy), possible consequences of course remain open if one adopts different focal lenses of international law, such as for example the rules on the use of force.²¹ The circumstance that a ‘tweet’ or a ‘post’ falls outside the scope of application of international diplomatic law does not necessarily and automatically mean that the very same social media post does not bear any relevance at all for other branches of international law.

²⁰ Extensively, see Erlend Serendahl, ‘Unilateral Acts in the Age of Social Media’, *Oslo Law Review* 5 (2018), 126-146.

²¹ Serendahl (n. 20), 138-139, referring to the diplomatic ramifications of social media activity, more specifically referring to posts of President Trump directed at the US population conveying messages to North Korea, raising questions of a potential unlawful threat of the use of force in violation of Art. 2(4) UN Charter.

III. Diplomatic Premises, and ‘Virtual’ Embassies and Consular Posts

Some States have already established either ‘virtual’ Embassies or consular posts abroad. In 2007 the Maldives and Sweden opened respectively a ‘full’ virtual embassy and a cultural office.²² Such embassies were ‘created’ within a specific webpage, *secondlife.com* – an open 3D virtual world developed by a private US company.

Other States have proceeded differently, establishing virtual embassies using governmental tools, namely official webpages of the State – such as the United States of America who did set up a virtual Embassy in Tehran in 2011. Similarly, to have some contacts with States (and their people) with whom it had no formal diplomatic relationship, Israel opened a ‘Twitter Embassy account’ in 2013 for the Gulf States²³, which closed soon after in 2014 and was re-launched in 2019.²⁴

The advantages of virtual establishments are apparent, both in terms of economics and public administration management²⁵ (especially for small size States unable to establish representations in all foreign countries), and in terms of possibility to unilaterally reach foreign people and institutions where diplomatic relationships are broken. Yet, the relevant *legal* question is whether such digital tools do amount to Embassies or consular post, thus entitled to any specific protection.

From an historical perspective, the VCDR strongly rests upon a physical conceptualisation of diplomatic missions. According to its Art. 1(i), ‘premises of the missions’ are buildings and land.²⁶ The receiving State must assist the sending State in the search for necessary premises.²⁷ These buildings and

²² Gilboa (n. 3), 544.

²³ Ilan Manor, *The Digitalization of Public Diplomacy* (Cham: Palgrave 2019), 228.

²⁴ ‘Israel Re-launches “Virtual Embassy” on Twitter for Gulf Dialogue’, 7 February 2019, <<https://www.middleeastmonitor.com>>.

²⁵ See Dietrich Klapper, ‘New Diplomatic Tools and the Broadening Access of Developing Counties’ in: Justin Robertson and Maurice A. East (eds), *Diplomacy and Developing Nations: Post-Cold War Foreign Policy-making Structures and Processes* (Oxon: Routledge 2005), 80-93 (85 ff.); and Justyna Arendarska, ‘Foreign Ministries in the Perspective of Information Revolution’ in: Monika Szkarłat and Katarzyna Mojska (eds), *New Technologies as a Factor of International Relations* (Newcastle upon Tyne: Cambridge Scholars Publishing 2016), 91-105 (92).

²⁶ ‘The “premises of the mission” are the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission including the residence of the head of the mission.’ See Jean d’Aspremont, ‘Diplomatic Premises’ in: Rüdiger Wolfrum (ed.), *MPEIL* (online ed., Oxford: Oxford University Press 2009), 1 ff.; Denza (n. 12), 16; and Wagner, Raasch and Pröbstl (n. 12), 53.

²⁷ ‘The receiving State shall either facilitate the acquisition on its territory, in accordance with its laws, by the sending State of premises necessary for its mission or assist the latter in obtaining accommodation in some other way’ (Art. 21(1) VCDR).

lands, their furnishings and other property thereon are protected from foreign intrusions, as they enjoy inviolability under Art. 22 VCDR. Even though the convention seeks an extensive definition of ‘premises’ – by including buildings not in property of the foreign State²⁸ or by including short-term rent of immovable properties destined to the diplomatic function²⁹ – a literal interpretation, historically contextualized, seems to point towards the idea that virtual ‘Embassies’ are not such in legal terms. Subsequent practice seems of little help to argue that a clear and settled customary law rule extending the definition of ‘Embassies’ has already emerged. Practice appears quantitatively not sufficient, as this comprises that of some Insular or Micro-States, Israel, Sweden, and the United States (US) only.

Moreover, some of these practices either show resistances in recourse to virtual posts, or theoretical inconsistencies which militate against an evolutionary interpretation in international law.

Some States, such as Sweden, have closed their ‘missions’,³⁰ whilst others – such as Israel – have had a practice inconsistent in time, intermittent, and for limited and specific purposes.

Iran did block the US virtual Embassy in Tehran, by obscuring the website.³¹ The United States of America themselves disqualified their own tool by clearly stating: ‘This website is not a formal diplomatic mission, nor does it represent or describe a real U.S. Embassy accredited to the Iranian Government. But, in the absence of direct contact, we hope it can serve as a bridge between the American and Iranian people’.³²

It seems however that the question at hand cannot be given a single and unitary answer, as different scenarios require different evaluations.

The first case to be dwelled upon is that of virtual missions opened and running on privately-owned websites, such as Second Life or Twitter. It is true that under the VCDR, ‘premises’ are not necessarily property of the foreign State; yet, once in their possession, the foreign State acquires a significant control over the *res*, which becomes inviolable to public and private entities (with well-known issues in cases of evictions if rent is not paid). The use of private websites and social media seems inconsistent with the idea of control of the premises, as States using such accounts have no

²⁸ D’Aspremont (n. 26), 2; Denza (n. 12), 16; and Wagner, Raasch and Pröbstl (n. 12), 54. However property alone, also if given, does not suffice to ensure application of diplomatic privileges to the building (see Roberts (n. 13), 107).

²⁹ Wagner, Raasch and Pröbstl (n. 12), 54 f.

³⁰ Gilboa (n. 3), 544.

³¹ The White House, Office of the Press Secretary, 7 December 2011, Statement by the Press Secretary on Iran’s Blockage of Virtual Embassy Tehran (n. 3).

³² On the website, <<https://ir.usembassy.gov>>. Cfr in the scholarship, Yolanda Kemp Spies, *Global South Perspectives on Diplomacy* (Cham: Palgrave 2019), 25.

different treatment than the public. The very existence of the ‘virtual mission’ will depend on the policies of both the ‘receiving State’, who might obscure single accounts or the social media at large, and of the private company, as this could retain the faculty to ‘block’ the account in accordance with the terms and conditions of the contract – a ‘self-enforcement’ measure that is not given to tenants of the building of the mission. In this sense, due to the lack of control over the *res* inherently required by the VCDR, privately-owned websites should not be classified as ‘diplomatic premises’ for the purposes of diplomatic law. Consequently, no diplomatic law protection should be granted, until at least an eventual subsequent State practice to the contrary can successfully be reconstructed.

The second case which deserves some thought is that of a virtual mission running on a governmental website. Such scenario would not meet the critiques of missions relying on private systems, yet the leading principle should remain that of consent,³³ as this strongly characterizes diplomatic relations. Under the VCDR, ‘The establishment of diplomatic relations between States, and of permanent diplomatic missions, takes place by mutual consent.’³⁴ In this sense, a ‘unilateral diplomatic mission’ is no diplomatic mission under diplomatic law. Hence, actions such as blocking the website of the foreign State should not constitute a violation of diplomatic law, nor a violation of the foreign State’s right to enter into contact (and influence) a given population with its website (as such a right to contact and influence other populations could hardly be reconstructed).

If the concerned States do not agree anything specific on the inviolability of the website, provided that this does not amount to ‘premises of the mission’ under the VCDR, some of its rules might nonetheless still be applicable.³⁵ If the governmental website runs on servers placed at a ‘physic’ diplomatic mission, accredited to the receiving State, such servers should enjoy both physical and ‘virtual’ inviolability. The first deriving from its location inside the premises of the Embassy; the second, from the principle of avoiding unduly interferences that is embedded in the convention³⁶ and in general principles of public international law. However, if there is no physical reality of the website attached to diplomatic premises in the host State, i. e. where there is no diplomatic premise and the server hosting the website is in

³³ See also Schmitt (n. 3), 216.

³⁴ Art. 2 VCDR.

³⁵ See also Schmitt (n. 3), 216.

³⁶ Cf. Art. 37(4) VCDR, according to which the jurisdiction of the receiving State over private servants of the mission shall be exercised to the extent immunity is not granted, and provided that jurisdiction is exercised in such a manner ‘as not to interfere unduly with the performance of the functions of the mission’.

its State of origin (or in a third State), as ‘virtual embassies’ do not fall within the scope of application of the VCDR,³⁷ a subsequent blockage by the State to whom it is directed would still not constitute a breach of general diplomatic law.

IV. Diplomatic Emails and Private ‘Inter-Net-Ferences’

In the context of online communication and online storage systems used for diplomatic purposes,³⁸ the *Bancoult* 3³⁹ judgment of the United Kingdom Supreme Court (UKSC) is one of the most recent cases⁴⁰ showing the complexities and limits surrounding the VCDR in relation to ‘internet cases’. The issue concerned ‘The leaking of governmental documents and their widespread distribution through the internet’, which ‘is a phenomenon of our time. The status of leaked documents in the public domain is an issue which is likely to recur’.⁴¹ In *Bancoult*, diplomatic cables from the US mission in London were sent to its home government, and to other non-specified third parties. Leaked documents were published on journals following an alleged illegitimate extraction by Wikileaks. Journal articles and diplomatic cables published were thus produced in court by private parties – who had no role in the taking of diplomatic cables.⁴²

³⁷ Schmitt (n. 3), 216.

³⁸ Other than the already quoted literature, see Carlo Curti Gialdino, *Lineamenti di diritto diplomatico e consolare* (Torino: Giappichelli 2018, 33 ff. and 302 ff.; Naomi Burke, ‘The Protection of Diplomatic Correspondence in the Digital Age: Time to Revise the Vienna Convention?’ in: Paul Behrens (ed.), *Diplomatic Law in the New Millennium* (Oxford: Oxford University Press 2017), 204 ff.; Elena Carpanelli, ‘On the Inviolability of Diplomatic Archives and Documents: The 1961 Vienna Convention on Diplomatic Relations to the Test of WikiLeaks’, *Riv. Dir. Int.* 98 (2015), 834-851; and Karen Kaiser, ‘Does the Inviolability of Archives Lead to a Catch-22 Situation?’, *Revista IUS* 11 (2017), 183-200.

³⁹ UKSC, *Bancoult No 3* (n. 5).

⁴⁰ See also Tribunal Supremo (Spain), 9 May 2016, STS 1029/2016, ECLI:ES:TS:2016:1029, arguing that ‘La mera información reflejada en un diario de gran tirada, que dice hacerse eco de los cables hechos públicos por Wikileaks, no puede ser tomada en consideración. No solo ignoramos la autenticidad de esa información, sino que la revelación de los cables procedentes de la Embajada americana no es sino una prueba obtenida de forma ilícita cuya consideración resulta vedada, de acuerdo con el artículo 11 de la LOPJ, conforme ha puesto de relieve en múltiples ocasiones el Tribunal Constitucional. El Tribunal ha reiterado que no se compecece con el derecho a la tutela judicial efectiva y con el derecho a un juicio justo (artículo 24 CE) el hecho de valerse de pruebas obtenidas mediante la vulneración de derechos fundamentales, secreto [...] Por lo tanto, el motivo no puede prosperar’. See also ECJ (General Court), *Bank Mellat v. Council of the European Union*, judgment of 29 January 2013, case no. T-496/10, paras 98 ff.

⁴¹ UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 64.

⁴² UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

1. Relevant Provisions Under the VCDR

According to Art. 24 VCDR, ‘The archives and documents of the mission shall be inviolable at any time and wherever they may be’.

Under Art. 27(2), ‘The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions’.⁴³

Whereas both Art. 24 and Art. 27(2) VCDR establish a duty upon the receiving State, none of them tackles the issue of use in court of unlawfully obtained evidence. In other words, it is not clearly regulated whether an unlawful conduct makes the evidence inadmissible in court (so called fruit of poisonous tree doctrine). The scope of application of the two provisions can of course overlap when the correspondence becomes part of the archives.⁴⁴ Both Arts 24 and 27(2) appear to have a quite extended scope of application as neither the correspondence nor the archives must bear external marks identifying them as ‘diplomatic’ post or archive (as opposed to Art. 27(3)(4) VCDR on courier bag).⁴⁵

2. Host State’s Obligations Under Arts 24 and 27(2) VCDR in *Bancoult*

The first issue dealt with by the British courts concerns the possibility for domestic courts to rely upon diplomatic documents extracted by a private party (not by the host State) who made them available online. The Court of Appeal,⁴⁶ relying upon Mann’s arguments,⁴⁷ concluded that Arts 24 and 27(2)

⁴³ The provision, contrary to Art. 24, does not specify that protection is afforded to correspondence ‘wherever this may be’. Yet, due to the ancillary nature of correspondence to archives, part of the scholarship advocates for the extension of the protection also to correspondence where this does not reach the recipient for intrinsic problems in delivery (Denza (n. 12), 189); a circumstance, this last one, that encourages delivery by way of diplomatic courier (Stanisław E. Nahlik, ‘Development of Diplomatic Law: Selected Problems’, RdC 222 (1990), 187-346 (288) and Roberts (n. 13), 117). See also Carlo Curti Gialdino, ‘Alcuni nuovi profili in tema di immunità diplomatiche’, Ordine internazionale e diritti umani (2018), 428-434 (429), and Michael Richtsteig, *Wiener Übereinkommen über diplomatische und konsularische Beziehungen* (Baden-Baden: Nomos Verlag 2010), 55.

⁴⁴ Denza (n. 12), 190.

⁴⁵ VCDR, Art. 27(4): ‘The packages constituting the diplomatic bag must bear visible external marks of their character and may contain only diplomatic documents or articles intended for official use.’

⁴⁶ *Bancoult*, R (on the application of) v. Secretary of State for Foreign & Commonwealth Affairs, judgment of 23 May 2014, [2014] EWCA Civ 708. Supporting the line of reasoning, Carpanelli (n. 38), 839.

⁴⁷ Frederick A. Mann, *Further Studies in International Law* (Oxford: Clarendon Press 1990), 327, and 337 (‘“Inviolability”, let it be stated once more, simply means freedom from official interferences. Official correspondence of the mission over the removal of which the receiving state has had no control can, as has been submitted above, be freely used in judicial proceedings.’).

VCDR only protect the foreign State from an active intervention of the receiving State. Consequently, diplomatic cables can be used in court by private parties if the unlawful extraction is not attributed to the host State.⁴⁸ This is a formalistic interpretation that⁴⁹ admittedly appears functional to the protection of State sovereignty, as the VCDR would not limit the powers of domestic courts.

The Supreme Court did not agree with such a view.⁵⁰ According to the Supreme Court, the use in court of documents extracted by private parties would be inconsistent with the principle of support and protection of foreign diplomatic missions.⁵¹ Hence, a solution again for the protection of sovereignty – this time of the State of origin of the mission.

⁴⁸ EWCA, *Bancoult No 3* (n. 46), 708, para. 58 f. ('We see considerable force in the argument that was advanced by Mr Kentridge and rejected in Shearson Lehman. Inviolability involves the placing of a protective ring around the ambassador, the embassy and its archives and documents which neither the receiving state nor the courts of the receiving state may lawfully penetrate. If, however, a relevant document has found its way into the hands of a third party, even in consequence of a breach of inviolability, it is prima facie admissible in evidence. The concept of inviolability has no relevance where no attempt is being made to exercise compulsion against the embassy. Inviolability, like other diplomatic immunities, is a defence against an attempt to exercise state power and nothing more. In Shearson Lehman, the Court of Appeal was reluctant to hold that a document, originally obtained in violation of the archives of the ITC, should be admissible in a court of the receiving state. It felt that a court, as an arm of the receiving state, should play its part in protecting the archives of the ITC. But Mr Kentridge submitted that, in view of the existence of an adequate range of remedies available to the ITC if a relevant document was originally obtained in violation of its archives, there was no reason to give an extended meaning to the term "inviolable". This submission reflects the views expressed by Dr Mann in the publications to which we have already referred.').

⁴⁹ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 18, quoting Jean Salmon, *Manuel de Droit Diplomatique* (Brussels: Bruylant 1994), 244.

⁵⁰ Cf. Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon Press 1995), 88; Nahlik (n. 43), 292, and Denza (n. 12), 167.

⁵¹ UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 71. See also International Tin Council (Intervener) (No 2) [1988] 1, WLR 16, *Shearson Lehman Bros Inc v. Maclaine, Watson and Co Ltd*; per Lord Bridge ('Mr Kentridge presented a forceful argument for the defendants based on the proposition that the only protection which the status of inviolability conferred by Article 24 of the Vienna Convention and Article 7(1) of the Order of 1972 affords is against executive or judicial action by the host state. Hence, it was submitted, even if a document was stolen, or otherwise obtained by improper means, from a diplomatic mission, inviolability could not be relied on to prevent the thief or other violator from putting it in evidence, but the mission would be driven to invoke some other ground of objection to its admissibility. I need not examine this argument at length. I reject it substantially for the reasons given by the Court of Appeal. The underlying purpose of the inviolability conferred is to protect the privacy of diplomatic communications. If that privacy is violated by a citizen, it would be wholly inimical to the underlying purpose that the judicial authorities of the host state should countenance the violation by permitting the violator, or anyone who receives the document from the violator, to make use of the document in judicial proceedings.').

The solution adopted by the Supreme Court seems consistent with international case law suggesting that diplomatic archives must be protected – thus not only free from State seizures.⁵²

Provided that Arts 24 and 27(2) VCDR are also applicable if the alleged unlawful conduct is not attributed to the receiving State, the Supreme Court dwells on the extent of the ‘inviolability’ therein provided for.

The Court specifies a number of circumstances in which ‘inviolability’ to correspondence and archives is not to be granted despite the applicability of the relevant rules of international law. In the first place, this privilege can be denied if this is necessary to ensure the survival of the host State itself.⁵³

In the second place, ‘inviolability’ is denied if the relevant document was not part of the archives or of the official correspondence at the time of the extraction. Here the Supreme Court shifts its attention to the notions of ‘archive’ and ‘correspondence’ in order to determine their scope of application (thus the scope of the protection afforded).

The Supreme Court understands ‘archives’ broadly, so as to encompass means of electronic storage.⁵⁴ Nonetheless, it has refused to decide on whether the documents were part of diplomatic archives because the cable was sent to the US State Department *and* ‘elsewhere’. With a ‘procedural eye’, the Court concluded that there was ‘no indication from where the Wikileaks document emanate[d]’⁵⁵ at the time of the unlawful extraction. Furthermore, to argue that the document was not part of the archives of the US Embassy in London, the court stressed that ‘once the document reached the State Department or any other addressee, it was, so far as appears and in the form in which it was there held, a document in the custody of the Federal Government of the United States of that other authority, and not part of the

⁵² I.C.J. Reports 1980, 36, Judgment, United States Diplomatic and Consular Staff in Tehran, para. 77 ([...] the Iranian authorities are without doubt in continuing breach of the provisions of Articles 25, 26 and 27 of the 1961 Vienna Convention and of pertinent provisions of the 1963 Vienna Convention concerning facilities for the performance of functions, freedom of movement and communications for diplomatic and consular staff, as well as of Article 24 of the former Convention and Article 33 of the latter, which provide for the absolute inviolability of the archives and documents of diplomatic missions and consulates. This particular violation has been made manifest to the world by repeated statements by the militants occupying the Embassy, who claim to be in possession of documents from the archives, and by various government authorities, purporting to specify the contents thereof.).

⁵³ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 17. See Quebec Court of King’s Bench, Appeal Side, *Rose v. The King* [1947] 3 D.L.R. 618.

⁵⁴ Vienna Convention on Consular Relations, Vienna, 24 April 1963, United Nations, Treaty Series, Vol. 596, 261, Art. 1(a)(k). See UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 11. In the scholarship, see Roberts (n. 13), 113.

⁵⁵ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

London Embassy archive'.⁵⁶ No role plays, in the court's eye, the *intention* of the diplomatic mission not to make a document public nor the unlawfulness of the extraction⁵⁷ from the archives under the authority⁵⁸ of the mission. An effective 'control theory' approach that however seems inconsistent with the *ratio* of the VCDR, which has the aim to protect archives 'wherever they may be'.

After having excluded that the diplomatic cable was part of the US diplomatic archives in London at the time of the extraction, the Supreme Court also excluded the applicability of the inviolability granted to diplomatic correspondence. In the Court's eye, Art. 27(2) VCDR is only applicable for the communication between the mission and the Ministry of Foreign Affairs (or other diplomatic missions),⁵⁹ namely the US State Department. The provision is not applicable for communications with third parties or 'unprotected organ[s] of the government'.⁶⁰ For the Supreme Court, the sending of 'confidential' (rather than top secret) cables also to third parties excludes the applicability of Art. 27 VCDR,⁶¹ unless it is proven that the extraction did take place *en route* from the mail destined to the Ministry of Foreign Affairs of the sending State.

Critiques to the positions of the Supreme Court have been expressed already within the bench. According to Lady Hale, the simple extraction of the document '[...] not [...] from the mission, but from elsewhere in the United States',⁶² does not necessarily mean that inviolability should be denied. The theory of control over documents should rather be integrated with a scrutiny of the will of the diplomatic mission to make the document available to subjects that are not the intended protected recipients of communication.⁶³

⁵⁶ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

⁵⁷ See UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 71.

⁵⁸ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20 ('There is no indication that the United States Embassy in London attached any reservation to or placed any limitation on the use or distribution of the cable by the State Department or any other authority to whom the cable went.').

⁵⁹ See Roberts (n. 13), 115. See also *Questions relating to the Seizure and Detention of Certain Documents and Data* (Timor Leste v. Australia), Provisional Measures, Order of 3 March 2014, I. C. J. Reports 2014, 147.

⁶⁰ UKSC, *Bancoult No 3* (n. 5), Lord Sumption: '[...] the Secretary of State is unable to establish that it was obtained by Wikileaks, and through them by The Guardian and The Telegraph, from the archives of the US embassy in London as opposed to some other unprotected organ of the US government. He has not therefore established the essential factual foundation for reliance on article 24 of the Vienna Convention.', para. 76.

⁶¹ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

⁶² UKSC, *Bancoult No 3* (n. 5), Lady Hale, para. 125.

⁶³ UKSC, *Bancoult No 3* (n. 5), Lady Hale, para. 126 f.

3. 'Inviolability' Under the VCDR: Publicly Disseminated Cables and Open Issues

The third exception developed by the Supreme Court is strictly related to the internet-world, even though it is dealt with only out of caution, as the applicability of both relevant rules has already been excluded. This last exception appears to be a first in the case law.⁶⁴

In the Court's eye, inviolability is not to be granted where the information at hand has become of public domain and is freely accessible.⁶⁵ Free access to information is incompatible with the need of confidentiality grounding the rules on inviolability – up to the point that the last one is ousted. However, the Court is silent on whether an unlawful extraction by the receiving State (which was not the case in the judgment) might have any consequences for private entities seeking to use in courts the documents extracted. A lack of transmission of procedural invalidity would help circumvent the protection afforded by the VCDR: States might commit an international wrongdoing by extracting diplomatic cables and making them available online to the general public, whilst private lawsuits may be decided based on such documents.

What appears relevant in the decision of the Supreme Court on this point is not the conclusion per se, but the methodological approach followed to advocate in favour of this additional exclusion to inviolability. The interpretation of the Court⁶⁶ is not founded on treaty-law, but on parallelisms with the domestic rules on confidential materials.⁶⁷ Although the solution does not necessarily seem inconsistent with the VCDR, as this could be interpreted to imply confidentiality as a necessary element of inviolability, the fact that it is grounded on domestic law seems to reduce the potential of the decision as a future international law leading case.

⁶⁴ UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 74.

⁶⁵ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 21, and UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 74 ('There is, however, a reservation of some importance which follows from the nature of the protection accorded by Article 24 of the Convention, as I have analysed it. It concerns documents which, although indirectly obtained without authority from the archives and documents of a mission, have entered the public domain. By that I mean that they have been disclosed not simply to a few people or in circumstances where it would take some significant effort on the part of others to discover their contents, but that they are freely available to anyone who cares to know.').

⁶⁶ On which see Robert McCorquodale, 'Wikileaks Documents are Admissible in a Domestic Court', EJIL: Talk!, 21 February 2018.

⁶⁷ UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 21. Generally referring to principles of confidentiality where secrecy has already been prejudiced, Lord Sumption, para. 74 ff.

What remains open is the burden of proof, unregulated in the VCDR. Some previous judgments have developed a presumption *iuris tantum* in whose light diplomatic documents should be presumed to be part of diplomatic archives or correspondence.⁶⁸ A solution that is certainly consistent with the VCDR framework. In *Bancoult 3*, only Lord Sumption, in a concurring opinion, stresses that the US State Department has not offered proof of the unlawful extraction from the diplomatic mission⁶⁹, thus failing to give proof of the ‘essential factual foundation for reliance on article 24 of the Vienna Convention’.

All these critical elements, the transmission of procedural invalidity, the domestic interpretation of ‘treaty relevant matters’, and the question of the burden of proof, will have to be clearly determined in the future, possibly by States rather than courts – so as to ensure uniform application of the VCDR to online accessible reserved information.

V. Online Crimes, and Diplomatic and Consular Privileges

The relationship between online (or cyber) crimes and diplomatic privileges should be analysed from different perspectives.⁷⁰

The first scenario concerns the inviolability of the premises of the mission (rather than immunities of staff), either when these are subject to cyber attacks, or when the crime is committed from the Embassy or consular post itself. If the mission is the victim of online crimes, the receiving State should do as much as possible to ‘prevent any disturbance of the peace of the mission or impairment of its dignity’ (Art. 22(2) VCDR). Should the forces of the receiving State need to enter the premises to fulfil such obligation, two different regimes are applicable. For diplomatic premises, the VCDR sets an absolute inviolability, meaning that the public forces of the receiving State need pre-emptive authorisation to enter.⁷¹ In Contrast for consular posts, inviolability is granted only to that part of the consular premises used exclusively for the purpose of the work of the consular post, and consent for

⁶⁸ Quebec Court of King’s Bench, *Rose* (n. 53), 646 (‘International law creates a presumption of law that documents coming from an Embassy have a diplomatic character and that every Court of Justice must refuse to acknowledge jurisdiction or competence in regard to them.’).

⁶⁹ UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 76.

⁷⁰ On which, in general see Choi (n. 3), 120 ff.

⁷¹ VCDR, Art. 22(1). See Denza (n. 12), 118 f.; Wagner, Raasch and Pröbstl (n. 12), 182; d’Aspremont (n. 26), 5 f., Curti Gialdino (n. 19), 212.

entrance is presumed in case of ‘fire or other disaster requiring prompt protective action’.⁷²

The scholarship has debated whether the ‘disaster exception’ can be extended from consular to diplomatic premises as well, or if there exists an implied presumed consent of the diplomatic mission where the action of the receiving State is necessary to save human lives.

Even if one should adhere to the (not unanimous) idea that also diplomatic premises are subject to an implied authorisation if an action is necessary to save human lives, it could scarcely be argued that cyber-attacks against the diplomatic mission amount to a threat of life.⁷³ In this sense, it appears that – at least as a general principle – authorisation from the head of the mission or the State of origin will be necessary.

As for consular posts, the question for those premises that do fall within the scope of application of inviolability is whether the term ‘disaster’ might also include cyber-crimes. Even though ‘disasters’ might not necessarily only be natural (as fires might also derive from the action of men), it should be stressed that such a provision is an exception to the general rule – hence it should be subject to a restrictive interpretation. Moreover, the *ratio* of the rule is to protect both the sovereignty of the foreign State, and the safety and security of the receiving State in whose territory a fire might expand from the consular post. In this sense, it appears that an unauthorised entrance into consular posts in cases of cyber-attacks could be deemed possible only to the extent such intervention is necessary to protect the host State itself, rather than only the post whose head does not grant access to.

The additional issue of eavesdropping or cyber-espionage may also be scrutinised through the lenses of the inviolability of the premises. If any device is ‘implanted’ in the mission for the purposes of cyber-espionage, this would amount to a violation of the inviolability of the premises. On the contrary, if information from the mission to the State of origin is ‘intercepted’ by other means, this could constitute a breach of the freedom of communication of the mission with its State enjoyed under Art. 27(1) VCDR.⁷⁴

⁷² VCCR, Art. 31(2). See also Convention on special missions, New York, 8 December 1969, UNTS, Vol. 1400, 231, Art. 25(1) (‘The premises where the special mission is established in accordance with the present Convention shall be inviolable. The agents of the receiving State may not enter the said premises, except with the consent of the head of the special mission or, if appropriate, of the head of the permanent diplomatic mission of the sending State accredited to the receiving State. Such consent may be assumed in case of fire or other disaster that seriously endangers public safety, and only in the event that it has not been possible to obtain the express consent of the head of the special mission or, where appropriate, of the head of the permanent mission.’).

⁷³ See Choi (n. 3), 123.

⁷⁴ See in particular d’Aspremont (n. 26), 10 f., and Curti Gialdino (n. 38), 211.

The second scenario, on the other side, sees premises not as victims, but as the origin of cyber-attacks. The rules on inviolability remain the same; however, if the victim of the attack is the receiving State itself, this might advocate the necessity to overrule inviolability to ensure its own survival. If it is true that some courts have rejected inviolability of diplomatic communication to ensure self-preservation, the same should hold true also in the case of inviolability of premises.

Stronger, and potentially more difficult to be overruled, is the immunity from jurisdiction of diplomatic and consular staff where these are responsible for the cyber-attack against the receiving State. Personal and functional immunity of diplomatic agents is extended under Art. 31 VCDR, and the most common accepted reaction of the receiving State would generally be a declaration of *persona non grata*,⁷⁵ so as to rip immunities off after the expiration of the warning to leave the country.

The receiving State could have stronger reaction powers, namely the possibility to arrest and trial the responsible persons, if these are non-diplomatic staff at the Embassy and their acts are performed outside their duties (or, as a general rule, if they are nationals or habitual residents in the host State). A similar limitation to the possibility for the State to proceed to trial is given for consular staff members, whose immunity is also limited to official acts.⁷⁶

VI. Closing Remarks

The paper has examined four questions that have already emerged into practice, i. e. social media and diplomatic communications; digital embassies; online archives and diplomatic cables, and cyber-crimes involving diplomatic premises.

From the above case studies, it seems possible to identify scenarios that can be subsumed within the scope of application of ‘traditional’ rules of diplomatic law. Here, a certain flexibility and adaptability of the Vienna Conventions to the digital world emerges (despite the substantive adequacy of the solution). As the *Bancoult* judgment or the questions revolving around cyber-crimes involving diplomatic or consular premises suggest, many issues posed by the internet era to diplomatic law appear essentially to be hermetic in nature. Nonetheless, domestic jurisprudence also proves that interpretation and qualification matters are still open, as neither a significant and

⁷⁵ Choi (n. 3), 121.

⁷⁶ VCCR, Art. 43(1).

consistent State practice subsequent to the Vienna Conventions, nor a specific interpretation of those treaties on ‘internet-related issues’, has been developed yet.

At the same time, the Vienna Conventions do not seem suited to other scenarios – such as the use of social media for official communication purposes by diplomats or Head of States, and the possibility to establish ‘online posts’. Despite a reasonable flexibility in the interpretation of the rules of the Vienna Conventions, these appear unsuited to be applied to these new situations, leaving legal uncertainty as per their treatment under international law.

If legal certainty, as mentioned, is one of the preconditions for eDiplomacy to flourish, it seems that no clear prediction can be drawn in current times. Where for some delicate issues the codified rules of diplomatic law, one of the oldest fields of international law, appear inherently flexible enough to ‘cope’ with the most urgent challenges posed by the digital divide, the Vienna Conventions and international diplomatic law at large appear non-applicable in other circumstances.⁷⁷ As the basic approaches and the most fundamental legal assumptions of diplomatic law still rest upon a ritualistic conceptualisation of diplomatic functions and the treatment of diplomatic premises as ‘sanctuaries’, for the array of ‘new challenges’ States will need to develop ‘new rules’. It seems however difficult to foresee if these new rules will be developed. This is because, on the one side, a specific legal framework would increase legal certainty and, to some extent, contribute in promoting eDiplomacy. At the same time, on the other side, such development might be to the detriment of traditional in person diplomacy.

⁷⁷ Amongst the legal questions that have not been emerged with strength as case-studies, the existence of a ‘right’ of diplomatic or consular missions to access an adequate internet connection; international cooperation to ensure the establishment of proper internet-infrastructures in all States; privacy, secrecy, and data protection at large where eDiplomacy is carried out through third parties applications could be thought of.

Microsoft Corp. v. United States and the ‘Hot Pursuit’: A Case Study Against the Application of the Law of the Sea into the Cyberspace

Patricia A. Vargas-León*

The Fletcher School at Tufts University, Medford, United States of America
patriciaavl@gmail.com

Abstract	755
Keywords	756
Introduction: The Cyberspace as a Challenge for the Traditional International Order	757
I. Application of International Law and Law of the Sea	759
1. Hot Pursuit: A Policy Beyond Territorial Sovereignty	761
2. Selection of the Hot Pursuit Principle	764
II. Case Study: <i>Microsoft Corp. v. United States</i>	765
1. Facts	766
2. Arguments of the Parties	768
a) The US Government	769
b) Microsoft	770
III. Application of the Hot Pursuit: Negative Repercussions	772
1. A Call for Nation-States: Bits under Nation-States’ Sovereignty	773
2. Direct Access v. MLATs: Private Actors Using Arguments of International Law	774
3. A ‘Virtual Fragmentation’ with ‘Practical Consequences’: A Call for the Nation-States Westphalian Model	776
4. More Centralised Government Control and Less of a Governance Model	778

Abstract

In today’s world, no treaty regulates the cyberspace or the Internet. To some extent, the multi-stakeholder model has successfully kept the Internet free of a unique point of control, yet some nation-states advocate for a government-based-model. Amid the Internet Corporation for Assigned Names and Numbers (ICANN) transition debate, some governments favoured a cyberspace regulation in the hands of an inter-governmental organi-

* Postdoctoral Scholar, The Fletcher School, Tufts University; Visiting Fellow Information Society Project, Yale Law School, PhD (Syracuse University), Law Degree (Pontifical Catholica University from Peru).

The work described in the paper was partially supported by NSF grant CNS 1923528, grant Hewlett 2018-7277 and grant Hewlett 2020-1484.

sation. Additionally, western democracies have advocated to declare the cyberspace a fifth domain.

Reasons for these different perceptions are related to the different conceptions nation-states have what should be the governance model for a resource beyond their traditional borders. Considering this dichotomy, this paper analyses the negative implications of applying the law of the sea into cyberspace. For this purpose, this paper will explore the concept of the ‘*right of hot pursuit*’, one of the provisions of the United Nations Convention on the Law of the Sea (UNCLOS).

The research methodology includes as a case-study *Microsoft Corp. v. United States*, also known as the ‘*Microsoft Ireland*’ case. This case was selected because it exemplified how government administrations attempt to use the principles of international law to protect their sovereignty over the Internet infrastructure located in their territory, even when the access to that infrastructure is ‘virtual’ and there is no need to access such infrastructure physically.

Facing this scenario, where governments try to exercise their sovereignty beyond their territorial borders, this paper will:

1. Provide an overview of the International Court of Justice (ICJ) and the International Tribunal for the Law of the Sea (ITLOS) interpretations of the hot pursuit to determine the international legal conception over this principle.
2. Analyse the arguments of the parties involved in the *Microsoft Ireland* case about why one nation-state’s sovereignty should be applied or not beyond the borders of its territory.
3. Analyse the negative repercussions of including the hot pursuit and the fictional fragmentation of the ocean into the cyberspace.

Findings expect to enrich the discussion within the Internet governance debate and understand the consequences of (1) applying the international law over the Internet infrastructure and (2) clarify the traditional legal approach that spaces without nation-states’ sovereignty should not exist.

Keywords

Hot Pursuit – Cyberspace – UNCLOS – *Microsoft Corp. v. United States*

Introduction: The Cyberspace as a Challenge for the Traditional International Order

The cyberspace is defined as a global space, the virtual world, for interactions among Internet users, where nation-states' territorial borders are irrelevant. The concept has been considered a sort of 'third force', different from governments and businesses. The cyberspace also has a 'global connotation' because it is considered a worldwide domain consisting of an interdependent network of information technology infrastructures, including the Internet, telecommunications networks, and computer systems.¹

Unlike the traditional territorial borders, the cyberspace is 'aterritorial',² invisible, unidentifiable, cannot be felt, or identified in any way and does not have natural or physical characteristics. It is also characterised by anonymity and ubiquity.³ For some academics, the law cannot control the cyberspace, it only can control the use that human beings put to it.⁴

The current international landscape witnesses a growing state power over the Internet infrastructure, which has created a definition of cyberspace as a military domain or fifth domain. As consequence, nation-states see fit that the traditional 'Westphalian model' should be the role for the cyberspace as well. Therefore, if nation-states are the sovereign authority within their territories, they also should be the supreme sovereign authority within the cyberspace and the Internet infrastructure located in their territories.⁵

Claims of sovereignty come from all types of regimes and in different circumstances.

The North Atlantic Treaty Organization (NATO) declared the cyber as the fifth domain, alongside water, fire, land, and space.⁶ During the ICANN transition debate, some governments (Russia, India, Iran, and Saudi Arabia) argued in favour of a cyberspace regulation in the hands of an inter-govern-

¹ Milton Mueller, *Ruling the Root Internet Governance and the Taming of Cyberspace* (Cambridge, Mass.: MIT Press 2002); Shabtai Rosenne and The Hague Academy of International Law, *The Perplexities of Modern International Law* (Leiden: Martinus Nijhoff 2004).

² 'Aterritoriality' refers to the lack of applicability of the territorial criteria that exists in nation-states.

³ Stephen C. Jacques, 'Comment Reno v. ACLU: Insulating the Internet, the First Amendment, and the Market Place of Ideas', *The American University Law Review* 46 (1998), 1945-1992; Joanna Kulesza, *International Internet Law* (London: Routledge 2012); Rosenne and Hague Academy of International Law (n. 1).

⁴ Kulesza (n. 3).

⁵ Robert Jackson, 'Sovereignty in World Politics: A Glance at the Conceptual and Historical Landscape', *Pol. Stud.* 47 (1999), 431-456; Milton Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 (2020), 779-801.

⁶ Steve Ranger, 'Cyberwarfare Comes of Age: The Internet Is now Officially a Battlefield' (2016), <<https://www.zdnet.com/>>.

mental organisation.⁷ Additionally, in 2011, former President Obama pointed out that the creation of rules and norms for state behaviour in cyberspace does not require re-inventing customary international law or rendering existing international norms. For the United States' (US) government, long-standing international norms guiding state behaviour (in times of peace and conflict) also apply in cyberspace.⁸

In view of the constant sovereignty claims over the cyberspace, a group of academics⁹ and non-academics¹⁰ have called to apply similar policies to the ones contained in the Convention on the Law of the Sea to this domain. In the US, the military called to move from 'sea power' to 'cyber power' and, in June 2016, NATO announced that the 28-member alliance agreed to declare cyber an operational domain, like sea, air, and land.¹¹ Furthermore, the Tallinn Manual 2.0 contains clear provisions of UNCLOS that should be included in case of a cyberwarfare.

In the real world, this conception framed according to the views of the national sovereignty refers to an international order based on mutually recognised territorial borders and in the absence of overlapping jurisdictions.¹² Nevertheless, no nation-state in the world may claim sovereignty over the cyberspace. In the same way, although no nation-state can control the cyberspace, nation-states understand the conception of the cyberspace as a 'whole thing', which explains the comparison with the oceans and the outer space, instead of continental land.¹³

For those who claim that the rules of UNCLOS should be applied into the cyberspace, the comparison between the cyberspace and the sea is adequate because, in the past, the sea was considered a space for communications, economic production, transportation, and war, many of the characteristics

⁷ Edward Moyer, *US Hands Internet Control to ICANN* (2016), <<https://www.cnet.com/>>.

⁸ White House, 'International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World', White House (2011), <<https://obamawhitehouse.archives.gov>>.

⁹ Julija Kalpokienė and Ignas Kalpokas, 'Hostes Humani Generis: Cyberspace, the Sea, and Sovereign Control', *Baltic Journal of Law & Politics* 5 (2012), 132-163; Michael Sechrist, 'Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public-Private Partnership', *Harvard – Belfer Center for Science and International Affairs* (2010), <<http://belfercenter.ksg.harvard.edu>>.

¹⁰ Kris E. Barcomb, 'From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future', *National Defense Unit*, <<https://ndupress.ndu.edu>>; Steven M. Barney, 'Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace', *Nav. L. Rev.* 48 (2001), 56-83.

¹¹ Barcomb (n. 10); Colin Clark, 'NATO Declares Cyber A Domain' *Breaking Defense*, (2016), <<http://breakingdefense.com/>>.

¹² Robert Jackson, 'Sovereignty in World Politics: A Glance at the Conceptual and Historical Landscape', *Pol. Stud.* 47 (1999), 431-456; Mueller (n. 5).

¹³ Mueller (n. 5).

attributed to cyber-space today.¹⁴ The ocean has been a subject of a global governance regime,¹⁵ in many ways similar to what nation-states attempt to do with the cyberspace today.

For others, the comparison between the sea and cyberspace is linked to the concepts of war and state-practice. This though can be summarised in two points: (1) wars are traditionally fought over territory, but the concept of territory has evolved to incorporate cyberspace,¹⁶ and (2) the existence of UNCLOS (and similar treaties) proofs the existence of a state practice of claiming any space beyond nation-states' territorial borders.¹⁷

This contribution discusses the consequences of applying the provisions of UNCLOS into the cyberspace and the Internet infrastructure as nation-states claim. For this purpose, this paper has selected one of the principles of UNCLOS to be subject to analysis, the 'hot pursuit'. As it will be explained in this paper, this principle has been selected because it represents the unrestricted respect to a nation-state's sovereignty even when another nation-state has a legitimate legal claim to pursue beyond its own zones of national sovereignty.

A first part will define the role of international law in the attempts to create a legal framework for the cyberspace, legal conceptualisation of the hot pursuit according to UNCLOS and the rulings of international courts. The second part will analyse the hot pursuit principle, from a theoretical and practical point of view, as this is one of the core elements for analysis. The following parts will explain the reasons why this principle was selected and the arguments of the selected case study. Finally, this paper will address the arguments against the creation of an international legal regime based on UNCLOS for the cyberspace.

I. Application of International Law and Law of the Sea

It is quite complicated to apply old principles of international law, linked to human history from its beginning, to new circumstances and technologies that do not recognise the basic principles on which the current international order was built.

The cyberspace and the Internet represent a new opportunity for mutual interactions among individuals and entities subject to different sovereignties.

¹⁴ Philip E. Steinberg, *The Social Construction of the Ocean* (Cambridge: Cambridge University Press 2001); Barney (n. 10).

¹⁵ Dire Tladi, 'Ocean Governance: A Fragmented Regulatory Framework', *A Planet for Life* (2011), <<http://regardssurlaterre.com/>>.

¹⁶ Andrew Sheng, 'The Coming CLASS War', *Project Syndicate* (2014), <<https://www.project-syndicate.org/>>.

¹⁷ Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in: Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict* (Tallin: NATO CCD COE Publications 2012), 7-19.

In this regard, lawmakers of each territory involved in a particular interaction claim the right to regulate a specific behaviour or to sanction a harmful conduct. Therefore, nation-states have taken action to exercise their coercive capacity over online activities. This situation directly affects Internet users as they may not be sure, and therefore they may not take informed decisions about what the legislation is applicable to their activities.¹⁸

For some international law scholars, such as Shabtai Rossene¹⁹ and Ian Brownlie,²⁰ the law of the sea is an inherent part of the theory of international law, therefore, they should not be considered as separated disciplines. In any case, it cannot be denied that there are similarities between the cyberspace (as a whole), which is shared by all the networks that formed the Internet, and the ocean, a space that is shared by the humankind.

This could lead to conclude that any regulation over the cyberspace should be an international one, based on the rules of international law. The achievement of international regulation is also essential for those who desire the achievement of concrete standards especially when human rights are involved, such as data privacy and freedom of expression.²¹

Nevertheless, the particular characteristics of the cyberspace, which do not make it possible for a nation-state to control it, but make it difficult to achieve rules based on international law to regulate it. Moreover, nation-states behind every potential attempt to regulate the cyberspace, have completely different visions about the regime that should set the rules of interaction within the cyberspace. For this particular characteristic, many legal scholars consider the cyberspace a 'perplexity' for the classic theory of international law.²²

One of the clearest attempts to concretise this tendency to apply the rules of international law into the cyberspace and cyber operations was the Tallinn Manual from 2013,²³ a comprehensive intellectual attempt to include the concept of sovereignty into the cyberspace. Elaborated under the sponsorship of the NATO Cooperative Cyber Defence Centre of Excellence, the Tallinn Manual created considering State practice and statements on the applicability of international law to cyber operations.

¹⁸ Kulesza (n. 3).

¹⁹ Rosenne and Hague Academy of International Law (n. 1).

²⁰ James R. Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford: Oxford University Press 2012).

²¹ Molly Land, 'Toward an International Law of the Internet', *Harv. Int'l L.J.* 54 (2013), 393-458.

²² Rosenne and Hague Academy of International Law (n. 1).

²³ Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (Cambridge: Cambridge University Press 2013). CCDCOE, 'The Tallinn Manual', (2021) <<https://ccdcoe.org/>>.

According to the Tallinn Manual from 2013 a government can exercise control over the national cyberinfrastructure and any activity within the borders of the nation-state territory.²⁴ A subsequent project, the Tallinn Manual 2.0 from 2017²⁵ focuses on the physical capacity around Internet access. This perspective is crucial because, although the cyberspace may be aterritorial, every piece of the Internet infrastructure that exists in a geographic location is owned, operated, and maintained by a specific entity subject to the local legislation.²⁶ Following this logic, local governments have created national statutes that have created international controversies, as it will be explained in the next paragraphs.

1. Hot Pursuit: A Policy Beyond Territorial Sovereignty

UNCLOS is a multilateral treaty that covers multiple aspects of the regulation of the spaces and activities in the ocean and sets out the framework for legal governance within which all activities in the oceans must be conducted and the institutions that must oversee those activities.²⁷ However, UNCLOS's main and most controversial characteristic is the creation of fictional spaces or legal areas where coastal nation-states sovereignty decreases with increasing distance of the coast. UNCLOS defines nation-states' rights and obligations from coast to coast and from the surface to the deep sea in these zones. This policy is known as 'maritime jurisdiction'²⁸ or a 'fragmented governance'²⁹ model. This paper will use the term a 'virtual fragmentation' of the ocean.

The hot pursuit is a classic principle of the doctrine of international law, the law of the sea, and is part of modern nation-states' practices. The doctrine related to the hot pursuit evolved through history and developed as customary international law. In 1982, the principle obtained international legal recognition by being included in UNCLOS.³⁰

²⁴ Schmitt (n. 23).

²⁵ Michael Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn manual 2.0 on the international law applicable to cyber operations*, (2nd edn, Cambridge: Cambridge University Press 2017).

²⁶ Kris Barcomb, Dennis Krill, Robert Mills and Michael Saville, 'Establishing Cyberspace Sovereignty', *International Journal of Cyber Warfare and Terrorism* 2 (2012), 26-38.

²⁷ World Ocean Review, 'A Constitution for the Seas' (2010), <<https://worldoceanreview.com/>>.

²⁸ Alfonso Arias-Schreiber Pezet, *El Derecho del Mar [Law of the Sea]*, (Lima: Academia Diplomática del Perú 1984).

²⁹ Tladi (n. 15), para. 4; Julia A. Ekstrom, Oran R. Young, Steve D. Gaines, Maria Gordon and Bonnie J. McCay, 'A Tool to Navigate Overlaps in Fragmented Ocean Governance', *Marine Policy* 33 (2009), 532-535.

³⁰ Vasilios Tasikas, 'Unmanned Aerial Vehicles and the Doctrine of Hot Pursuit: A New Era of Coast Guard Maritime Law Enforcement Operations', *Tul. Mar. L.J.* 29 (2004), 59-80.

UNCLOS defines the hot pursuit principle as the right of a nation-state to pursue and seize a non-national vessel suspected of having committed a crime within the nation-state's internal waters and territorial sea (where the nation-state has sovereign rights) and arrest it. Such a right remains, even if the vessel moves onto the high sea (where the coastal nation-state has no sovereign rights).³¹

The territorial sea is the extension of seawaters adjacent to coastal states until the distance of 12 miles. According to UNCLOS provisions, nation-states are sovereign in the territorial sea and the internal waters, as if they were in their territory.³²

The hot pursuit principle of a foreign ship may be undertaken when there are reasons for the coastal nation-state's competent authorities to believe that a foreign ship violated its laws and regulations. The main characteristics of the pursuit are:³³

1. The pursuit must start when the foreign ship or one of its boats is within the internal waters, the territorial sea or the contiguous zone of the pursuing nation-state.
2. The pursuit must be continuous and only can continue outside the territorial sea if there were no interruptions and there was a warning, visual or auditory signal for the crew of the prosecuted ship.
3. The pursuit must end as soon as the chased ship enters into the territorial sea of its nation-state or a third nation-state's territorial sea (entering into other nation's state territorial sea is the equivalent to enter into that nation-state's territory).

According to the rules of UNCLOS, the hot pursuit purpose is 'to bring escaping wrongdoers before the jurisdiction of the injured State'.³⁴ The hot

³¹ Eugene Kontorovich, 'Law of the Sea – Visit and Seizure of Vessels at Sea – Definition of Piracy – Right of Hot Pursuit – Enforcement Jurisdiction at Sea – Compliance with Provisional Measures', *AJIL* 110 (2016), 96-102.

³² United Nations Convention on the Law of the Sea of 1982

Part II. – Territorial Sea and Contiguous Zone

Article 2: Legal status of the territorial sea, of the air space over the territorial sea and of its bed and subsoil

1. The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea.

2. This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.

3. The sovereignty over the territorial sea is exercised subject to this Convention and to other rules of international law.

Jose Luis Messeguer Sanchez, 'Los Espacios Maritimos en el Nuevo Derecho del Mar [Sea Spaces in the New Law of the Sea]' (Madrid: Marcial Pons 1999).

³³ Robin Rolf Churchill and Alan Vaughan Lowe, *The Law of the Sea* (Manchester: Manchester University Press 1999).

³⁴ Nicholas M. Poulantzas, *The Right of Hot Pursuit in International Law*, (Leiden: Martinus Nijhoff Publishers, 2002), 2.

pursuit is an exception to the principle and freedom of the high seas and to the exclusive jurisdiction of the flag-state that rules the vessels in the high seas.³⁵

As established by ITLOS³⁶ in the case of the merchant vessel *M/V Saiga*,³⁷ conditions to exercise the hot pursuit are set out in Article 111 of UNCLOS.³⁸ Such conditions must be accumulative; each one must be satis-

³⁵ Poullantz (n. 34), 239.

³⁶ The International Tribunal for the Law of the Sea (ITLOS) is an independent judicial body created by UNCLOS to solve disputes related to the interpretation and application of the Convention. The Tribunal is composed of 21 independent members and, according to article 21 of its statute, ITLOS has jurisdiction over any dispute concerning the interpretation or application of the Convention, and over all matters specifically provided for in any other agreement which confers jurisdiction on the Tribunal. In practical terms, ITLOS is a parallel jurisdiction to the ICJ, and the final venue to solve a controversy is a matter of decision for the involved parties.

³⁷ ITLOS, *The M/V 'SAIGA' Case No. 2* (Saint and Vincent The Grenadines v. Guinea), judgment of 1 July 1999, para. 146.

³⁸ United Nations Convention on the Law of the Sea of 1982

Part VII. – High Seas

Article 111: Right of Hot Pursuit

1. The hot pursuit of a foreign ship may be undertaken when the competent authorities of the coastal State have good reason to believe that the ship has violated the laws and regulations of that State. Such pursuit must be commenced when the foreign ship or one of its boats is within the internal waters, the archipelagic waters, the territorial sea or the contiguous zone of the pursuing State, and may only be continued outside the territorial sea or the contiguous zone if the pursuit has not been interrupted. It is not necessary that, at the time when the foreign ship within the territorial sea or the contiguous zone receives the order to stop, the ship giving the order should likewise be within the territorial sea or the contiguous zone. If the foreign ship is within a contiguous zone, as defined in article 33, the pursuit may only be undertaken if there has been a violation of the rights for the protection of which the zone was established.

2. The right of hot pursuit shall apply mutatis mutandis to violations in the exclusive economic zone or on the continental shelf, including safety zones around continental shelf installations, of the laws and regulations of the coastal State applicable in accordance with this Convention to the exclusive economic zone or the continental shelf, including such safety zones.

3. The right of hot pursuit ceases as soon as the ship pursued enters the territorial sea of its own State or of a third State.

4. Hot pursuit is not deemed to have begun unless the pursuing ship has satisfied itself by such practicable means as may be available that the ship pursued or one of its boats or other craft working as a team and using the ship pursued as a mother ship is within the limits of the territorial sea, or, as the case may be, within the contiguous zone or the exclusive economic zone or above the continental shelf. The pursuit may only be commenced after a visual or auditory signal to stop has been given at a distance, which enables it to be seen or heard by the foreign ship.

5. The right of hot pursuit may be exercised only by warships or military aircraft, or other ships or aircraft clearly marked and identifiable as being on government service and authorised to that effect. [...]

fied to claim the principle.³⁹ In the *Corfu Channel* case,⁴⁰ the ICJ recognised that the use of force is allowed when the pursued vessel subject to arrest refuses to stop. The idea of using necessary force is authorised even though that it is a severe infringement on freedom in the high seas.⁴¹

In 2013, in the case of the *Arctic Sunrise*⁴² ITLOS established new clarifications surrounding the claim of the hot pursuit principle. As established by ITLOS, signals of the coastal nation-state ship for the vessel suspected of having committed a crime must be clear and ratified that boarding must be urgent. Additionally, in 2015 and about the same case, the Permanent Court of Arbitration (PCA Tribunal)⁴³ also established that boarding must be immediate; the coastal nation-state boat must not be shadowing the vessel suspected of committing a crime. If those requirements are not met, the chance to claim the hot pursuit may disappear.

2. Selection of the Hot Pursuit Principle

The principle of hot pursuit can be exercised to act in circumstances of necessity or criminal activity. Main critiques against the hot pursuit claim that it is a principle that allows a nation-state to enforce its domestic laws extra-territorially against non-national ships that flee onto the high seas where nation-states lack jurisdiction.⁴⁴ Defenders of the principle claim that, if the hot pursuit empowers a coastal nation-state to pursue a vessel that has violated its laws onto the high seas, this occurs in order to deny to the offending vessel the opportunity of escape punishment by claiming the free navigation designed to protect innocent vessels.⁴⁵

This critique resembles the one related to the cyberspace, where governments (acting on behalf of their nation-states) have acted in two different ways: a) by attempting to expand their sovereignty accessing data stored

³⁹ Saiful Karim, 'Conflicts over Protection of Marine Living Resources: The "Volga Case" Revisited' *GoJIL* 3 (2011), 101-127.

⁴⁰ ICJ, *Corfu Channel* Case (UK v. Albania), merits, ICJ Reports 1949, 4 (1949).

⁴¹ Craig H. Allen, 'Doctrine of Hot Pursuit: A Functional Interpretation Adaptable to Emerging Maritime Law Enforcement Technologies and Practices', *ODILA* 20 (1989), 309-341 (20).

⁴² ITLOS, *Arctic Sunrise* (Kingdom of the Netherlands v. Russian Federation), Provisional Measures, ITLOS Case No. 22, Order of 22 November 2013.

⁴³ In *re Arctic Sunrise* (Netherlands v. Russian Federation), PCA Case No. 2014-02, Merits, PCA Case No. 2014-02, UNCLOS Annex VII Arb. Trib. 14 August 2014.

⁴⁴ Robert C. Reuland, 'The Customary Right of Hot Pursuit onto the High Seas: Annotations to Article 111 of the Law of the Sea Convention', *Va. J. Int'l L.* 33 (1993), 557-589; Tasikas (n. 30).

⁴⁵ Allen (n. 41).

beyond the borders of their territory⁴⁶ and b) by attempting to keep data within the borders of its territory.⁴⁷

In this regard, a nation-state's territory consists of all the land within its frontiers, together with a belt of sea adjacent to its coast known as the territorial sea, and the airspace above its land territory and territorial sea. National sovereignty is framed by a nation-state's territorial borders and does not extend to the outer space.⁴⁸ The hot pursuit is one of the few exceptions that allow governments to go beyond the spaces where they can exercise jurisdiction and yet, the pursuit must stop the moment a space of national sovereignty of a third nation-state gets involved.

Following the nation-states' logic of applying UNCLOS into the cyberspace, the sovereignty claim of one nation-state must stop when another nation-state sovereignty claim starts. The hot pursuit is the best principle to concretise this premise because the hot pursuit is the outcome of the unrestricted respect to the recognition of the fictional borders international law has created in the ocean.

Nevertheless, because the cyberspace lacks traditional territorial borders, nation-states demand respect to the Internet infrastructure located in their own territories, under the assumption that the Internet is the main component of the cyberspace. Following this claim, any access to the physical Internet infrastructure located in a nation-state cannot be accessed from another nation-state. The same logic is the one with the hot pursuit principle, as any international legal persecution must stop as soon as the borders (and anything inside of them) of a third nation-state are affected.

II. Case Study: *Microsoft Corp. v. United States*

The case *Microsoft Corp. v. United States*, or *United States v. Microsoft Corp.*, was a case involving the extraterritoriality of law enforcement seeking electronic data under the 1986 Stored Communications Act, which involved Internet data centres and cloud storage.

This case was selected for the following reasons:

1. It exemplifies the claims to respect sovereignty over anything included within a nation-state territory, including an Internet server.
2. From the facts of the case, it is known that the retrieval of the data did not require physical access to the server. It could be done virtually from US territory, this is through the networks of the cyberspace.

⁴⁶ David Goldman, 'Microsoft Is Fighting the DOJ Too' 2016, <<http://money.cnn.com/>>.

⁴⁷ The Economist, 'Should Governments Be Able to Look at Your Data When It Is Abroad?', 2011, <<https://obamawhitehouse.archives.gov>>.

⁴⁸ Rosenne and Hague Academy of International Law (n. 1).

3. This case is an example of the potential application of the extraterritoriality of law enforcement seeking electronic data in an attempt to solve a criminal investigation of illegal activities occurred within US territory.
4. The case also clarifies how private corporations are willing to use or support principles of international law when it sues to their business model.

The purpose of this section is describing the facts of the case and the arguments of the involved parties, which included: (1) the authority in charge of the criminal investigation, (2) the interpretation of the law, (3) conflict of jurisdictions, (4) extraterritoriality, and (5) economic argumentation. This paper will focus on the controversy related to the extraterritorial application of the US legislation into Irish territory. Although this became the central issue of discussion, it is also a fact that in order to access the data, Microsoft Corp. did not have to send anyone physically to Ireland to collect it, since the data was under its control to be collected from US territory.

1. Facts

In December 2013, a New York District Court judge issued a warrant requesting Microsoft Corp. to produce emails and private information associated with particular accounts hosted by the company. The data was stored on a Hotmail server located in Dublin, Ireland, and was related to a drug trafficking investigation.^{49 50} To get the data, the U.S. government applied for a warrant according to section 2703(a)⁵¹ of the Stored Communications

⁴⁹ 'In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.', Harv. L. Rev. 128 (2015), 1019-1026.

⁵⁰ Mark Scott, 'Ireland Lends Support to Microsoft in Email Privacy Case', The New York Times <<http://bits.blogs.nytimes.com/>>.

⁵¹ Stored Communications Act

18 U. S. C.

Title 18 – Crimes and Criminal Procedure

Part I. – Crimes

Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access

§ 2703. Required disclosure of customer communications or records

(a) Contents of Wire or Electronic Communications in Electronic Storage.

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

Act (SCA), enacted as part of the 1986 Electronic Communications Privacy Act (ECPA).⁵² According to the U.S. Department of Justice (DoJ), the government has the right to demand the emails of anyone in the world as long as the electronic email (e-mail) provider has headquarters within borders.⁵³

Microsoft sued the US government and refused to deliver the names and accounts contained in the server stored in Ireland, arguing that a US Court has no jurisdiction over information stored out of US territory. Microsoft also argued that the US government should pursue traditional bilateral law enforcement and diplomatic channels in order to work with the Irish government to get the data they required. Such channels are referred as the 'Mutual Legal Assistant Treaties' (MLATs), general agreements signed between two or more nation-states to gather and exchange information to enforce public and criminal laws.⁵⁴ Similarly, the Irish government supported Microsoft's opinion and claimed that US Courts do not have the sovereignty to issue search warrants to be executed abroad. The US District Court for the Southern District of New York denied Microsoft's motion, and the company appealed.⁵⁵

Microsoft refused to turn over the e-mails and tried to quash the US government's warrant under the argument that the US government's warrant authority cannot extend extraterritorially and, therefore, the warrant was invalid.

The US government, along with the magistrate judge and district court, disagreed. They concluded that the relevant reference point for warrant jurisdiction purposes was the location of the provider (in this case Microsoft), not the location of the data. In practical terms, the data located in Ireland can be accessed and retrieved by Microsoft employees within US territory.⁵⁶

On 7 July 2016, the 2nd US Circuit Court of Appeals in Manhattan resolved that the US government is not entitled to force Microsoft to turn over customer e-mails stored on servers outside of US territory. According to the appealing Court, US service providers that own servers outside the US are beyond the reach of domestic US laws, and therefore, search warrants

⁵² Alex Ely, 'Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview', Lawfare 2015, <<https://www.lawfareblog.com/>>.

⁵³ Sam Thielman, 'Microsoft Case: DoJ Says It Can Demand Every Email from any US-based Provider', The Guardian 2015, <<http://www.theguardian.com/>>.

⁵⁴ United States Department of State, 'Treaties and Agreements' 2016, <<http://www.state.gov>>.

⁵⁵ Goldman (n. 46).

⁵⁶ Jennifer Daskal, 'Case To Watch: Microsoft v. US on the Extraterritorial Reach of the Electronic Communications Privacy Act | Just Security', Just Security 2016, <<https://www.just-security.org/>>.

issued under SCA are not applicable.⁵⁷ The 2nd US Circuit Court concluded that the US Congress legislation is meant to be applied only within US territory. The court did not mention anything about the extraterritorial application of the SCA.⁵⁸

In October 2016, the US government filed a petition for an ‘en banc session’ rehearing by the Second Circuit. In January 2017, the Court voted 4 to 4 to rehear the case. The judgment in favour of Microsoft remains in place. Differently from this case, in February 2017, the District Court within the Third Circuit ruled that Google must comply with a warrant of the US government to retrieve data from foreign servers. According to the Third Circuit, the scope of privacy invasion for the case was entirely within US territory, not where the electronic transfer occurs.⁵⁹

2. Arguments of the Parties

The context of the *Microsoft Ireland* case refers to the rise of an electronic medium that cannot be governed by any current territorially based sovereign. In this regard, this case puts on the table an ‘international’ problem: current national statutes were written before the concept of the cyberspace was created and before the Internet was privatised and open to the public. In this way, US Courts have to guess or interpret what Congress would have written into legislation if the Internet had been available at the time. In this scenario, law enforcement agencies find themselves trying to access data stored abroad, and sometimes facing multiple jurisdictions.

It is a fact that it must be remembered that Microsoft and other companies invested billions in building data centres abroad, especially in Europe. If US authorities and intelligence agencies can access that data, European firms may be reluctant to trust US companies. On the other hand, depending upon the result, this case may encourage other governments to request Microsoft or other companies to hand data stored abroad. This situation could generate a forever conflict of jurisdictions.⁶⁰ In any case, the actions of the US government will have significant implications in terms of international law. Just to set an example, in the middle of the *Microsoft* case, the former European

⁵⁷ Jonathan Stempel, ‘Microsoft Wins Landmark Appeal Over Seizure of Foreign Emails’, Reuters 2016, <<http://www.reuters.com/>>.

⁵⁸ ‘Cooperation or Resistance? The Role of Tech Companies in Government Surveillance’, Harv. L. Rev. 131 (2018), 1722-1741.

⁵⁹ Cooperation or Resistance? (n. 58).

⁶⁰ The Economist, ‘Should Governments Be Able to Look at Your Data When It Is Aroad?’, 2015, <<http://www.economist.com/>>.

Union Justice Commissioner warned that the US warrant's final execution might constitute a breach of international law.⁶¹ This was a clear call to respect the sovereignty of a member of the union.

Here there is a quick note to make. The words of the former European Union Justice Commissioner referring to a breach of the rules of international law, could be read, among lines, as the figure of the 'non-intervention principle', so many times featured by the international law and the United Nations. However, the term must be correctly understood and not confused with political rhetoric. First, there must be an 'intervention' by one state in the affairs of another and second, the intervention must be about issues in which each nation-state has a right to decide freely according to the rules of international law.⁶²

The discussion surrounds when nation-states face an issue of their sovereignty. In order to better understand the legal controversy, the next section will describe the main arguments outlined by both parties, Microsoft and the US government, during the trial.⁶³

a) The US Government

For the US government, the Federal Bureau of Intelligence (FBI) and US Courts are the authorities in charge of the criminal investigation. Upon their request, private companies (like Microsoft) must disclose customer information or records following the Stored Communications Act (SCA). The exercise of authority is not an issue of international law, but one of the domestic laws that establish a citizen's duty concerning its government request. While the Congress's legislation (unless the contrary intention appears) seems to be applicable only within US territory, the question of its application requires a debate, at least until there is a legislative change. According to the US government, nationality, as a principle, supports the legal requirement that an

⁶¹ Viviane Reding, 'Viviane Reding Letter European Commission', European Commission 2015, <<http://www.nu.nl>>.

⁶² Mazier Jamnejad and Michael Wood, The Principle of Non-Intervention, LJIL 22 (2009), 345-381.

⁶³ AT&T, 'District Court Amicus Brief in Support of Microsoft', Electronic Frontier Foundation 2014 <<https://www.eff.org/>>; Preet Bharara, 'Government's Brief in Support of Magistrate's Decision', Electronic Frontier Foundation 2014, <<https://www.eff.org/>>; 'EFF District Court Amicus Brief in Support of Microsoft', Electronic Frontier Foundation 2014, <<https://www.eff.org/>>; 'Judge Francis. Magistrate's Opinion Denying Microsoft's Motion to Quash', Electronic Frontier Foundation, 2014, <<https://www.eff.org/>>; Microsoft, 'Microsoft's Objection to the Magistrate's Opinion', 2014, <<https://www.eff.org/>>; U.S. District Court, 'Microsoft's District Court Reply Brief', Electronic Frontier Foundation 2014, <<https://www.eff.org/>>; Verizon, 'Verizon District Court Amicus Brief in Support of Microsoft', Electronic Frontier Foundation, 2014, <<https://www.eff.org/>>.

entity subject to jurisdiction within US territory (like Microsoft) is required to get evidence stored abroad.

According to the SCA provisions, the government can request information through a subpoena, court order, or warrant. On this matter, the SCA was enacted in recognition that the fourth amendment protections that apply in the physical world might not apply to information communicated through the cyberspace. This is why SCA authorises the Court with jurisdiction over the investigation of a criminal act to issue a warrant directly, despite the intervention of its counterpart in the district where the Internet service provider is located.

Additionally, according to the US government, the warrant required in section 2703 of SCA demands the government to show probable cause, but it does not change the duty an entity has to produce information regardless of where the data is located. In this case, the US Congress anticipated that an ISP located within US territory would be obligated to respond to a warrant issued according to section 2703(a) by producing information within its control. Therefore, the warrant triggers a US company's statutory obligation to disclose records within its possession and control to law enforcement within US territory. The purposes of the warrant are: (1) to require Microsoft to disclose the content of any electronic communication under Section 2703, and (2) to authorise a review of that data by law enforcement agents within US territory after the data has been disclosed. Moreover, for purposes to deliver the requested data, Microsoft was not in need of sending anyone physically to Irish soil to retrieve it. The company had the capacity of accessing the data electronically from US territory.

On the other hand, Microsoft argues that it is not required to produce the records demanded by the warrant because those records were stored abroad. According to the US government, that argument finds no support under SCA's rules because any 'court of competent jurisdiction' is authorised to issue a warrant. Those courts include those that have jurisdiction over (1) the offence under investigation, (2) the physical location of the service provider, or (3) the storage site of the relevant records.

b) Microsoft

In 1986, the US Congress enacted ECPA, a statute intended to protect individuals' privacy expectations in electronic communications. To protect these privacy interests, ECPA requires federal, state, and local officers to use forms of process within their own powers and limitations. In terms of privacy, the Sixth Circuit's leading decision ruled that the Fourth Amendment requires the US Government to obtain a warrant to access the contents of e-mail communications. ECPA never meant to allow the government to

obtain e-mails without a warrant at all. This practice would be unconstitutional under US law.

However, the extraterritorial application of warrants issued under ECPA represents a violation of international law and reduces privacy expectations at a global level. No provision in the statute ever suggests that this was the intention of the US Congress. If the Congress intended to give the warrant provision from ECPA extraterritorial effects, then the Congress should have been clear indications about it. The legislative history of ECPA confirms that warrants executed according to section 2703 (a) are limited to the US territory.

About the competent jurisdiction, Microsoft also acknowledges that a court of competent jurisdiction is the only one who can issue a warrant, but for the company, this principle is vital. According to section 18, 2703(a) of ECPA, a state or federal entity may compel a provider of electronic communications services to disclose the content of a wire or electronic communication, but only when a warrant is issued by a Court of competent jurisdiction. According to a related SCA provision contained in section 2703(b)⁶⁴ compels

⁶⁴ Stored Communications Act

18 U. S. C.

Title 18 – Crimes and Criminal Procedure

Part I – Crimes

Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access

§ 2703. Required disclosure of customer communications or records

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

the disclosure of content information maintained by a remote computing service provider as long as the government obtains a warrant issued by an appropriate state or federal court. To this end, and according to Irish law, in order to obtain the content of electronic mails from an electronic service provider, it is required authorisation from an Irish District Court Judge.

The use of 'cloud' computing services makes it easier for US companies to store data abroad. On this matter, each nation-state may have its data protection law to protect data and impose more strict protection standards than the US law. Regarding the interpretation of the extension of the US legislation's application, courts of justice are not free to re-write national statutes to achieve what they believe the Congress intended to say.

Microsoft does not refuse to provide the information requested by the US Court; however, the company argues that the US authorities should request it through the regular MLAT procedures. MLATs convert a foreign law request for information into a request that conforms to the domestic law requirements. In this particular case, the US government ratified a MLAT applicable to Ireland, the nation-state where the requested information is stored.

Finally, Microsoft mentions an economic argument because the company has encountered concerns in consumers abroad about the US Government extraterritorial pretensions to access their information. Potential customers have decided to hire the services of a provider based out of US territory and therefore, out of US jurisdiction.

III. Application of the Hot Pursuit: Negative Repercussions

Although no nation-state in the world can exercise sovereignty over the cyberspace, some academics argue that the principle of territorial sovereignty protects the Internet infrastructure (which is at the same time, part of the cyber infrastructure) located within a nation-state's territory. Therefore, following the rules of international law, nation-states are prohibited to interfere with the cyber infrastructure located in the territory of another State. States have a right to exercise their territorial jurisdiction over cyber activities within their territories, but not beyond.⁶⁵

The hot pursuit principle clearly serves this principle. Although the Internet infrastructure is part of the cyberspace, a space that everyone shares, the Internet infrastructure is local and can be regulated. Accordingly, nation-states are entitled to enforce their domestic law. The pursue of any legal claim

⁶⁵ von Heinegg (n. 17), 7-19.

cannot access the Internet infrastructure in another nation-state, without its consent. This is also the maximum of the hot pursuit.

Regarding the case, the main legal issues can be summarised as (1) what legislation is applicable, (2) what jurisdiction is the competent one, (3) what nation-state's sovereignty prevails when there is a controversy about the cyberspace. As mentioned before, there is no international treaty or international agreement that solves the problem of the 'right jurisdiction' when a data-access-issue occurs. So, how do the rules of UNCLOS work in this case, more concretely, how do the rules of the hot pursuit work in this case? From the arguments previously exposed, and as it will be explained in the following items, the application of the hot pursuit and the rules of UNCLOS calls to recognise what is known as the Internet fragmentation.

1. A Call for Nation-States: Bits under Nation-States' Sovereignty

A bit (b, short for 'binary digit') is the smallest storage unit used to quantify computer data. Bits are stored in a computer or similar device. A bit has a value, or code, of either 0 or 1, which is used to store data and implement instructions in groups of bytes.⁶⁶ In consequence: if bits are stored in a server and such server is located in a specific place in the world, are those bits subject to the sovereignty of the nation-state where the server is located? This is the main argument discussed in the *Microsoft Ireland* case.

Whether subject to applicable customary or conventional rules of international law, governments are entitled to exercise jurisdiction by subjecting objects and persons within its territory. That is their prerogative as the administrative entity of the nation-states. However, the ICJ established that this principle has a two-side-application: territorial sovereignty protects a nation-state against any form of interference by other nation-states, but the principle also imposes obligations. Nation-states are obligated to protect the rights of other nation-states within their own territories too. This includes the right to integrity and inviolability, alongside with the rights each nation-state may claim for itself and its nationals in the foreign territory.⁶⁷

⁶⁶ TechTerms, 'Bit Definition', TechTerms 2013, <<http://techterms.com/>>.

⁶⁷ ICJ, *Corfu Channel* (n. 40), para. 43; As cited by von Heinegg (n. 17), in his Separate Opinion Judge Alvarez stated: 'By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them.'

Regarding the hot pursuit principle, the first condition for its application is the suspicion of criminal activity committed within the territory under a nation-state's sovereignty. In the *Microsoft Ireland* case, the alleged criminal is located in US territory; the required data to solve the investigation is not. To access the data, nobody has to travel (physically) to Ireland for that purpose because the data is under the control of Microsoft and the company can retrieve it at will. Nevertheless, applying the rules of international law refrained the US of compelling Microsoft to retrieve the data; in application of the hot pursuit the US government pursuit stops at the very moment another nation-state territory is involved.

Nevertheless, according to section 2703(b) of SCA the disclosure of content information maintained by a remote provider is legal as long as the warrant is issued by an 'appropriate' state or federal judge. Here lays a procedural point of conflict: (1) For the US government, that judge is one based on US soil. (2) For the Irish law, it must be an Irish judge because to obtain the content of electronic mails it is required authorisation from an Irish District Court Judge.

According to the theory of the hot pursuit principle, no matter what type of criminal activity is under investigation, once the sovereignty of a different nation-state (other than the one where authorities are conducting the investigation) is involved, the pursuit must stop. The absolute end to any extraterritorial activity is the territory of another nation-state. Independently of the case, the pursuit must end as soon as the chased ship enters into the territorial sea of its nation-state or a third nation-state's territorial sea (entering into other nation's state territorial sea is the equivalent to enter into that nation-state's territory). The end of the pursuit means absolute respect to another nation-state's national sovereignty.

The *Microsoft* case was not conducted in an international court, and yet it is an example of an international controversy created by the collision of sovereignties and jurisdictions.

2. Direct Access v. MLATs: Private Actors Using Arguments of International Law

Under the application of both principles, the classic rule of international law (that requires one nation-state to protect other nation-state interests within its territory) and the hot pursuit, the US government (or any other government) can request data storage beyond its territorial borders but cannot access it directly. In this regard, the rule is clear, it is not possible to

access the server in another territory, even if there is no need of physical interaction with the server.

The fact that Microsoft (upon request of the US government) does not need to send people physically to retrieve the data does not change the fact that there are actions conducted within Irish territory. Such potential actions generated the Irish government protest.

To retrieve the data, the government that makes the request must follow the traditional mechanisms of communication from government to government, the traditional MLATs. The recognition of sovereignty among nation-states should be honoured by the other nation-state involved. Following the rules of UNCLOS and the hot pursuit, the US cannot access the data stored in foreign territories under the application of its national statute. As Professor Schmitt established, in terms of international law, when sovereignty is involved, 'stopping is a matter of law'.⁶⁸

This is a constant reminder in the Microsoft argumentation, and the Second Circuit Court of Appeals backed it up. According to the Court, SCA does not authorise US Courts to issue and enforce warrants against US-based service providers to get customer e-mail content stored exclusively on foreign servers.⁶⁹

Ironically this conclusion is aligned with those who defend the territorial sovereignty over the cyberspace to benefit their governments. For these academics and non-academics, there is an absolute principle of territorial sovereignty when the cyberspace is involved. Therefore, its infrastructure and activities are under the sovereignty of the government where that infrastructure is located. For these defenders of territorial sovereignty, nation-states are forbidden to interfere with the cyber-infrastructure located within another nation-state's territory.⁷⁰ According to this perspective, it is interesting to ask the question changing the role of the participants in the Microsoft Ireland case: Had Ireland been the nation-state interested in retrieving data stored abroad, would the US government have accepted direct access by the company that owns the server where the data is stored? Or, would the US government require Ireland to go to the long and bureaucratic MLAT process?

⁶⁸ Michael Schmidt, 'International Law and Cyber Operations – Launch of the Tallinn Manual 2.0', Atlantic Council 2017, <<https://www.youtube.com/watch?v=riP4kStBBJs>>.

⁶⁹ Stempel (n. 57).

⁷⁰ von Heinegg (n. 17); Shabtai Rosenne, *Essays on International Law and Practice* (Leiden: Martinus Nijhoff/Brill, 2007); White House, 'International Strategy for Cyberspace', 2011, <<https://www.whitehouse.gov/>>.

3. A 'Virtual Fragmentation' with 'Practical Consequences': A Call for the Nation-States Westphalian Model

UNCLOS policy of creating fictional spaces in the sea with specific sovereign rights in favour of coastal nation-states in each space is no other thing than 'fragmenting' the ocean until all of it gets 'full' of 'juridical meaning,' an old practice of international law.⁷¹ In this case, the juridical meaning is the allocation of sovereign rights in favour of nation-states in each space created by UNCLOS. Even international spaces ('High Seas' and 'The Zone'), where at least theoretically no nation-state has sovereign rights, have regulations that all nation-states are required to follow.

According to UNCLOS rules, there are no absolute rights in favour of nation-states. The latter remain the main actors in the international realm. In this situation, they are continually trying to use their sovereignty rights over others. Conflicts such as the South Sea in China, the Arctic, and constant claims of sea boundary delimitation are a clear example of this government practice.⁷²

Different from the sea, the cyberspace is aterritorial and invisible. However, the Internet infrastructure, one of the most vital elements of the cyberspace, is not. As defined, the Internet is a global collection of networks that connect in different ways to form the single entity known as 'the Internet'.⁷³ At the same time, the networks that compose the Internet share a similar architecture and protocols that allow communication within and among different constituent networks. The data that travels through the Internet is broken into small pieces, called 'packets', which are transmitted to their destination by routers and servers, using the 'TCP/IP protocol' (Transmission Control Protocol/Internet Protocol).⁷⁴

In this context, most Internet users assumed that universal connectivity would be a primary benefit. However, nation-states may decide to apply specific policies over the Internet infrastructure within their territories. When the policy decision of acting over the Internet infrastructure is political and is

⁷¹ Raul Ferrero Rebagliati, *Derecho Internacional Publico [Public International Law]* (Peru: Pontificia Universidad Católica del Perú, Facultad de Derecho y Ciencias Políticas 1962).

⁷² BBC, 'Why Is the South China Sea Contentious?' 2016, <<http://www.bbc.com/>>; Atle Staalesen, 'Conflict Over Arctic Shelf Unlikely', Barents Observer 2015, <<http://barentsobserver.com/>>.

⁷³ Jeff Tyson, 'How Internet Infrastructure Works', HowStuffWorks 2017, <<http://computer.howstuffworks.com/>>.

⁷⁴ David Clark, Thomas Berson, Herbert Lin and the National Research Council (US) (eds), *At the Nexus of Cybersecurity and Public Policy* (Washington D.C.: The National Academies Press 2014).

strictly in governments' hands, academics created the term 'Internet fragmentation'.⁷⁵ Fragmentation is a concept related to governments' policies and actions in the exercise of their sovereignty within their territorial borders. According to UNCLOS rules, there are no absolute rights in favour of nation-states. The latter remain the main actors in the international realm.⁷⁶ Fragmentation becomes the outcome of the collision point sovereignty and cyberspace.

It is possible to talk about Internet fragmentation when the conditions of the Internet infrastructure and government policies constrain or prevent specific uses of the Internet and do not allow interoperating and exchanging the Internet data packets consistently at all end points.⁷⁷ Governments worldwide are continually trying to exercise sovereignty rights and apply specific policies over the Internet infrastructure. These policies vary from censorship, filtering, data protection, and more drastic policies, such as the 'Internet kill switch'. These policies not only affect the Internet traffic; they are also significantly costly for the nation-states themselves.⁷⁸ Nevertheless, the fragmentation results from the basic principle of international law that governments (acting on behalf of the nation-state) exercise jurisdiction (as the application of the law) over the people and infrastructure located within the borders of their territory.

Following the tradition of governments' practices, the application of the hot pursuit into the cyberspace carries the possibility of fragmenting the Internet infrastructure alongside the territorial boundaries of national jurisdictions. Those are the basis of the hot pursuit, no matter how urgent the chase of a ship is, no matter how important it is, the chase must stop when another nation-state's sovereignty gets involved. Similar to other principles of international law, the hot pursuit and the rules of UNCLOS are built based on the strict respect of nation-states' sovereignty rights.

To some extent, the ICANN transition attempted to increase the resilience of the Internet because governments were not supposed to have control over the critical Internet resources. However, nation-states constantly try to construct borders around the Internet infrastructure to reaffirm their sovereignty one more time. When one government's actions affect another nation-state's

⁷⁵ Vint Cerf, 'The Fragmentation of the Internet', *IEEE Internet Computing* 20 (2016), 88-93.

⁷⁶ Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Hoboken: Wiley 2017).

⁷⁷ William Drake, Vint Cerf and Wolfgang Kleinwächter, 'Internet Fragmentation: An Overview', *EFF District Court Amicus Brief in Support of Microsoft*, World Economic Forum 2016, <<https://www.weforum.org/>>.

⁷⁸ Darrell M. West, 'Internet Shutdowns Cost Countries \$2.4 billion Last Year', Brookings Institution 2016, <<https://www.brookings.edu>>.

territory, a 'collision' of sovereignties is a possibility. The situation becomes more dangerous if nation-states decide to enforce national jurisdiction over global Internet services that happen to be incorporated in their national territories.⁷⁹ As it was mentioned before, when sovereignty and jurisdictions are involved, stopping becomes an obligation, a matter of law. In this case, consequences cannot be foreseen.

The application of UNCLOS's policy model and the hot pursuit into the cyberspace have similar negative consequences. Despite the existence of different stakeholders that do not exist in the sea, UNCLOS's policy is no other than a virtual fragmentation of the oceans. Therefore, the application of the hot pursuit carries the risk of falling into the traditional nation-states' Westphalian model, where the territorial sovereignty of nation-states is the rule and only source of law and practice.

4. More Centralised Government Control and Less of a Governance Model

Nation-states' persistent claims to apply policies over spaces beyond national jurisdictions reflect the Westphalian model that dominated the international realm until the twentieth century. Although questioned during the time of 'globalisation', now seems to be back.

The application of UNCLOS rules, the hot pursuit included, brings the possibility of a higher level of government control to the detriment of the multi-stakeholder governance model, the model that so far has kept the Internet free from a single point of control.

The multi-stakeholder model aims to bring together businesses, civil society, governments, research institutions, and non-government organisations to achieve joint decisions over the Internet infrastructure and create negotiated policies.⁸⁰

The multi-stakeholder model was also the conceptual framework behind the negotiated ICANN transition in 2016. Today the model is under questioning after the 'renaissance' of the nation-state sovereign model and the 'failure' of the globalisation process. In any case, there is interest in the international community, represented by ICANN, that the cyberspace re-

⁷⁹ Paul Fehlinger, 'Cyberspace Fragmentation: An Internet Governance Debate Beyond Infrastructure', *Internet Policy Review* 2014, <<http://policyreview.info/>>.

⁸⁰ Milton Mueller, John Mathiason and Lee McKnight, 'Making Sense of Internet Governance: Defining Principles and Norms', *Internet Governance Project Syracuse University – The Convergence Center* 2004, <<https://www.wgig.org/>>.

mains atterritorial and free of local legislation's execution. At the same time, it could be observed that the same international community has an interest in participating in any decision about how to regulate the cyberspace.

Whether in agreement with a model based on nation-states' sovereignty or the multi-stakeholder model, it has been the latter the one who has kept the Internet free from a single point of control. To some extent, the multi-stakeholder model is one of the 'palliatives' against the Internet fragmentation and centralised government control over the Internet infrastructure. As mentioned before, this fact is important because the Internet remains the primary physical element of the cyberspace that can remain under government control, and with its limitations, the multi-stakeholder model is the one that has allowed us to keep a free Internet as we have become to know.

Responsible Business in a Digital World – What’s International Law Got to Do With It?

Christine Kaufmann*

University of Zurich, Zurich, Switzerland

christine.kaufmann@uzh.ch

Abstract	782
Keywords	782
Introduction	782
I. Features of Digitalisation and Their Impact on Responsible Business Conduct	784
1. General Features of Digitalisation	784
a) Networks and Connectivity	784
b) Data	786
c) Big Data Analytics	787
2. Specific Business-Related Aspects	787
a) Digital Infrastructures: Blockchain	788
b) Digital Business Models	788
II. International Framework for Responsible Business: The OECD Guidelines for Multinational Enterprises	789
1. Legal Nature	789
2. Scope	791
a) Comprehensive Standard for Responsible Business Conduct (RBC)	791
b) Remedy Mechanism	792
c) Territorial Scope	794
d) Digitalisation and Responsible Business Conduct	796
3. Beyond Hard and Soft Law: Accommodating a Changing World	797
a) Distinctive Features of the Guidelines	797
b) Accommodating New Developments and New Actors	800
III. Interactions Between Digitalisation and Responsible Business Conduct	800
1. New Notion and Models of Business	800
a) Online Platforms	800
b) Accommodating New Business Models – Can the Guidelines Deliver?	803
2. Supply Chains and Due Diligence	803
a) Applying Due Diligence to Digital Technologies	804
b) Applying Digital Technologies for Conducting Due Diligence	807
IV. Conceptual Implications of Complex Interactions	808
1. Mind the Gap: Responsibilities of States and Business	809
2. Responsible Business Conduct by Design – In Regulation and Technology	811
V. Conclusion: A Call for a New Interface	813

* Professor of Public International Law, European and Constitutional Law at the University of Zurich. I am grateful to Rolf H. Weber, Patricia A. Vargas León and the anonymous reviewers for their valuable comments and feedback. While this article benefits from my insights in my role as the Chair of the OECD Working Party on Responsible Business Conduct, all views and opinions expressed are solely my own.

Abstract

The observation that digital transformation challenges some of the underpinnings of traditional international law and regulation also applies to responsible business conduct. The Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises are the most comprehensive international standard on responsible business conduct. This article discusses the impacts of digitalisation on responsible business conduct and the relevant case law by OECD National Contact Points and shows that as a *sui generis* instrument of international law the Guidelines can play an important role in accommodating business as the key driver of digital transformation and in addressing the related risks on people, the environment and society. However, several shortcomings of the existing regulatory framework are identified, particularly with regard to the imbalance of state and business responsibilities and the challenges for adequate regulatory responses in a highly dynamic environment where developments are driven by the private sector. Therefore, a holistic approach, based on ‘Responsible Business Conduct by Design’ both in technology and regulation is suggested. Given the specific features and impacts of digitalisation on responsible business conduct, such an approach would need to be of a hybrid nature by including a variety of actors and models of regulation beyond the state. To create a safe space for experimenting and testing new regulations and for mutual learning the article concludes with call for a new interface and for exploring a ‘regulatory sandbox’ at the international level.

Keywords

digitalisation – human rights – responsible business conduct – online platforms – supply chains

Introduction

‘The algorithms of the law must keep pace with new and emerging technologies’ is the opening sentence in a judgement of the High Court of Justice Divisional Court in Cardiff (UK) regarding the question whether current law in the United Kingdom adequately protects citizens’ right to privacy when facial recognition software is used by public authorities.¹

¹ High Court of Justice, *R v. The Chief Constable of South Wales Police and Others*, Judgement of 4 September 2019, EWHC 2341, para. 1.

At a time when cyberspace is permeating all aspects of life, blurring boundaries between material and virtual worlds,² the statement by the High Court can be interpreted in two ways. On the one hand, as a need for the law to ‘give in’ to new technologies by lowering the level of legal protection for those whose rights are negatively affected by these technologies. On the other, it can be seen as a call for upgrading and reconceptualising the existing (domestic) legal framework to accommodate new technological developments such as digitalisation.³ Often heard calls for more suitable approaches which would afford ‘better’ protection in a digital environment can go both ways: They can lower the level of protection by for example referring to voluntary, industry-led mechanisms instead of judicial scrutiny or result in innovative approaches to preserve legal protection while at the same time accommodating the specific features of digitalisation.⁴

This contribution will leave the domestic sphere and explore the role of international law in accommodating business as a key driver of digital transformation. In particular it will shed light on the role of the OECD Guidelines for Multinational Enterprises.⁵

The argument is structured as follows: First, selected *key features of digitalisation* and their impact on responsible business conduct are discussed with a focus on digital business models and digital infrastructures (I.). The second part (II.) analyses the OECD Guidelines and their distinctive features which qualify them as a *sui generis* instrument of international law that departs from the traditional focus on the state and provides flexibility to address new actors and new substantial issues. Against this background, the *interactions between digitalisation and responsible business conduct* are explored further in the third part (III.) with a discussion of relevant case law of OECD National Contact Points. The following section (IV.) identifies the conceptual implications of these interactions with a view to clarifying state and business responsibilities and suggests a ‘Responsible Business by Design’ approach. The article concludes with a call for a new interface (V.).

² Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven/London: Yale University Press 2020), 3.

³ The High Court’s findings were to a large extent overturned by the Court of Appeals, South Wales Court of Appeals, Bridges, *R (On the Application Of) v. South Wales Police*, Judgement of 11 August 2020, EWCA Civ 1058, para. 58: ‘The fact that this case involved the trial of a new technology does not alter the need for any interference with Article 8 rights to be in accordance with the law.’

⁴ A particularly challenging issue is the application of the rule of law in a digital context (below III.2.b)). Chris Reed and Andrew Murray, *Rethinking the Jurisprudence of Cyberspace* (Cheltenham (UK)/Northampton (USA): Edward Elgar Publishing 2018), 226–230.

⁵ OECD Guidelines for Multinational Enterprises 2011 edition (Paris: OECD Publishing 2011).

I. Features of Digitalisation and Their Impact on Responsible Business Conduct

Digitalisation includes both the *technical process* of converting physical, analogue information into a digital format and a *societal and social* dimension as the resulting interconnection affects our lives in manifold ways. This article will approach digital technologies by looking mainly at two concepts: digital *infrastructures* such as distributed ledger technologies and digital *services*, including the technical aspects of artificial intelligence and machine learning.

For the topic of this contribution networks and connectivity, data and new possibilities to process and analyse data are particularly relevant as they feed *inter alia* into the use of digital infrastructures in a business context, for example blockchain, and new digital business models such as online platforms. The following section summarises the relevant elements of these features.

1. General Features of Digitalisation

a) Networks and Connectivity

Networks allow for information to be passed between computers regardless of their physical location. Connectivity ensures the access to such networks for machines as well as humans. The Internet can be defined as the network of interconnected computer networks.⁶ For the purpose of this article, *social networks and platforms* and the *Internet of Things (IoT)* are of particular interest. According to the International Telecommunications Union (ITU) the Internet of Things is ‘a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies’.⁷ The Internet of Things thus extends the internet connectivity to physical objects, ranging from smart home devices to advanced applications like utilities, manufacturing lines, health monitoring systems or drones.⁸

⁶ Matthias Kettemann, *The Normative Order of the Internet* (Oxford: Oxford University Press 2020), 22-23.

⁷ International Telecommunications Union (ITU), Recommendation Y.2060: Overview of the Internet of Things, 15 June 2012, para. 3.2.2.

⁸ Rolf H. Weber and Evelyne Studer, ‘Cybersecurity in the Internet of Things: Legal Aspects’, *Computer Law & Security Review* 32 (2016), 715-728 (718-719); OECD, ‘The Internet of Things: Seizing the Benefits and Addressing the Challenges’, OECD Digital Economy Papers No. 252, 2016; DeNardis (n. 2), 29-31.

In all networks interoperability is essential for their functioning and accessibility because it is a prerequisite for seamlessly transferring data and other information across different platforms, systems and applications.⁹ Besides its manifold benefits, for example with convenient single consumer sign-on systems like Facebook's 'Login with Facebook', interoperability can also come with risks for instance on consumers' privacy and data security if such single sign-on identity is stolen.¹⁰ From a responsible business conduct perspective, this raises questions about the governance of interoperability and the related accountability of states and business. Often, interoperability is driven by private actors and industry initiatives. To whom should a user in the mentioned Facebook single sign-on example turn for compensation if her credentials are abused by a third party, such as an advertiser, with whom she has no contractual relationship?¹¹ Is it Facebook as the digital identity provider? What role is there for state regulation and responsible business conduct standards?

In fact, some of these questions have been addressed in national laws: The United States introduced legislation with the Communications Decency Act in 1996 to address specific aspects of online publishers' responsibility which states immunity from civil liability for providers and users of an interactive computer service.¹² A more general provision shielding media editors from criminal liability for the content of published contributions can be found in Swiss criminal law and the Swiss Federal Court recently held that social media platforms can fall within the scope of this norm.¹³ In March 2021, Australia introduced legislation on News Media and Digital Platforms which links the convenience of easily accessing news posted by Australian media on social platforms such as Facebook or Google with an expectation that these platforms share the benefits they earn from such content with the producers of the content.¹⁴

⁹ Urs Gasser, 'Interoperability in the Digital Ecosystem', ITU Global Symposium for Regulators (GSR) discussion paper 2015, 2.

¹⁰ Gasser (n. 9), 12-13.

¹¹ Gasser (n. 9), 14.

¹² Section 230 (c) US Communications Act of 1934, 47 USC § 230. Several bills for amending (H. R. 2154, H. R. 2000, H. R. 277) or repealing (S. 1384) this provision are pending in Congress as of 15 August 2021.

¹³ Article 28 para. 1 Swiss Criminal Code of 21 December 1937 (Systematische Sammlung 311.0): 'If an offence is committed and completed through publication in a medium, then, subject to the following provisions, only the author is liable to prosecution.' (unofficial translation); Swiss Federal Court, Decision of 18 November 2020, BGE 147 IV 65, 71, paras 5.4.4 and 5.5.

¹⁴ Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021 No. 21: An Act to amend the Competition and Consumer Act 2010 in relation to digital platforms, and for related purposes (2 March 2021).

These regulatory initiatives and reactions to digital developments illustrate the complex environment that states are faced with: squaring the enormous potential of digital technologies for sharing and accessing information, for communication and collaboration across borders and for innovation with their inherent risks of spreading misinformation and infringing on human rights to name just a few.

Since the technology is to a large extent driven by private actors, particularly tech companies, regulators will often be lagging behind. As a result, there is a need for not only ensuring *technical* interoperability but also what has been called *normative or legal interoperability*, which will be explored further in section IV.¹⁵

b) Data

At the heart of the networks described above are *data*. Before the digital age, data essentially meant information regarding content, collected by people. This changed with digitalisation: Data is now a ‘container’ for information.¹⁶ Today, most data is collected by machines and digital technologies fundamentally enhanced the value that can be taken or construed from *metadata*. Metadata as ‘data about data’ provide structured information about different aspects of data, such as for example the use of mobile phones or access to websites. Metadata thus facilitates targeted access to data and the analysis of large data samples. Moreover, with the increase in available data, handling and protecting *personal data* has become a more sensitive issue than ever before.¹⁷

Thanks to the internet, data can flow through cyberspace between people, businesses and machines across borders and the globe.¹⁸ Hence, since the impact of data is on real people and societies, questions about the territorial and legal attribution of such activities in an increasingly fragmented regulatory environment arise.¹⁹

¹⁵ Kettemann (n. 6), 214-215, 225.

¹⁶ Rolf H. Weber, Christian Laux and Dominic Oertly, *Datenpolitik als Rechtsthema: Agenda für Open Government Data* (Zürich/Basel/Genf: Schulthess 2016), 11; Florent Thouvenin, Rolf H. Weber and Alfred Früh, ‘Data Ownership: Taking Stock and Mapping the Issues’ in: Matthias Dehmer and Frank Emmert-Streib (eds), *Frontiers in Data Science* (Boca Raton: Taylor & Francis 2017), 111-145.

¹⁷ For different types of data see OECD, *Enhanced Access to Data: Reconciling Risks and Benefits of Data Sharing and Re-use* (Paris: OECD 2019), 25-27.

¹⁸ OECD, *Going Digital: Shaping Policies, Improving Lives* (Paris: OECD 2020), 23.

¹⁹ Rolf H. Weber, *Shaping Internet Governance: Regulatory Challenges* (Zürich: Schulthess 2009), 4.

c) Big Data Analytics

The third key feature is *new possibilities to process and analyse vast amounts of data* covering not only economic or business activities but all aspects of life. The value of large quantities of data depends substantially on the capacity to extract specific, consolidated information such as for example profiles, with *big data analytics*. The original concept of ‘Big Data’²⁰ which relates to the high volume, velocity and variety of information assets is however limited as it does not cover important other factors such as the reliability of data.²¹ This is particularly relevant when data analysis is increasingly not being undertaken by humans only, but based on algorithms which are trained to ‘learn’: artificial intelligence and machine learning. Artificial intelligence can be defined as the ability of machines and systems to acquire and apply knowledge by performing a variety of cognitive tasks such as pattern recognition, making decisions and predictions.²² Machine learning means a set of techniques that allow machines to learn in an automated manner through patterns and inferences and adjust their own parameters to improve the reliability of their predictions. For this purpose, machine learning systems are trained on large amounts of data.²³

2. Specific Business-Related Aspects

All these features lead to business operating in a new ecosystem of inter-dependent digital technologies. Of particular relevance are big data analytics, artificial intelligence, and distributed ledger technologies (DLT) – all supported by new forms of computer power which allow for processing information at an unprecedented speed.²⁴ With a view to preparing the ground for the discussion on the impacts of digitalisation on responsible business conduct, digital infrastructures and new digital business models warrant some further exploration.

²⁰ Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Boston/New York: Houghton Mifflin Harcourt 2013), 123-149.

²¹ Annabeth Aagaard, ‘The Concept and Frameworks of Digital Business Models’ in: Annabeth Aagaard (ed.), *Digital Business Models Driving Transformation and Innovation* (Cham: Palgrave Macmillan 2019), 1-26 (2).

²² OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2020), para. I; OECD (n. 18), 20.

²³ OECD, *Digitalisation and Responsible Business Conduct: Stocktaking of Policies and Initiatives* (Paris: OECD 2020), 9; Ashley Deeks, ‘High-Tech International Law’, *Geo. Wash. L. Rev.* 88 (2020), 574-653 (582-583).

²⁴ OECD (n. 18), 18-22.

a) Digital Infrastructures: Blockchain

As a distributed ledger technology, blockchain technology allows for the storage, distribution or exchange of values between different entities, including business and its stakeholders, on shared transaction ledgers. Since all transactions are automatically spread and synchronised among all participants of the network, blockchain facilitates the anonymous flow of information between stakeholders and can reduce information asymmetry and the related inefficiencies. From a business perspective and with a view to responsible business conduct, blockchain can improve the accuracy of supply chain information due to its immutability and decentralisation.²⁵ This leads to the question discussed in section III.2.b) whether blockchain could play a role in supply chain due diligence, i.e. in ensuring responsible business conduct across the whole supply chain.

In addition, so called *smart contracts* are often used to facilitate the execution of a business transaction. A smart contract is neither smart nor a contract. Rather it can be described as a computer routine which automatically executes the contractual terms between two or more parties without their intervention.²⁶ This additional layer of legal security also warrants to be considered in the context of supply chain due diligence (below III.2.b).

b) Digital Business Models

Recent research in management studies indicates that new digital technologies can on the one hand enhance or reshape existing business models: Examples are the use of big data analytics to better identify consumer preferences and adjust production accordingly or use a system of sensors based on Internet of Things technology to track goods while they are being shipped from the factory to consumers.²⁷ From the perspective of international law and international responsible business standards, such a scenario calls for applying *existing norms* to existing business which uses new instruments and tools – in other words, the analysis and particularly due diligence requirements will apply to *new issues (objects)*.

²⁵ OECD, *Is There a Role for Blockchain in Responsible Supply Chains?* (Paris: OECD 2019), 7-8.

²⁶ Rolf H. Weber, 'Smart Contracts: Do we Need New Legal Rules?' in: Alberto De Franceschi and Reiner Schulze (eds), *Digital Revolution – New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies* (Baden-Baden: Nomos/Beck 2019), 299-312, para. 12.

²⁷ Mirko Presser, Qi Zhang, Anja Bechmann and Michail Beliatas, 'The Internet of Things as Driver for Digital Business Model Innovation' in: Annabeth Aagaard (ed.), *Digital Business Models Driving Transformation and Innovation* (Cham: Palgrave Macmillan 2019), 27-55 (39).

On the other hand, digital technology has the potential to foster the development of *entirely new business models* where the underlying technologies are at the core of the value creation and delivery process.²⁸ Online platforms are a prime example in this regard. Typically, an online platform is a digital service which facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet. A unique feature of this interaction is the generation and work with user data which sets online platforms apart from other business models.²⁹ A broad variety of services is provided via online platforms including online marketplaces, social media, search engines, communication services, and specific platforms supporting the gig economy (e. g. Uber and TaskRabbit), among others.

From the perspective of international law and international responsible business conduct standards, this scenario of creating new business models is different from enhancing existing business models as it introduces *new actors* (*subjects*) and thus raises first the question on their legal status with regard to their nature as business: Is for example an online advertising platform a business? Second, their jurisdictional attribution to one or several states needs to be clarified: Which state is responsible for overseeing the mentioned online advertising platform's activities? And third the substance and potential need for redefining respective state responsibilities and obligations needs to be explored:³⁰ What exactly is a state required or expected to do regarding online advertising platform activities? Cases handled by the Polish and the French National Contact Point discussed in section III. will illustrate the relevance of these questions.

II. International Framework for Responsible Business: The OECD Guidelines for Multinational Enterprises

1. Legal Nature

By 1976, the year in which the OECD Guidelines for Multinational Enterprises were adopted as part of the OECD Declaration on International

²⁸ Zsolt Ugray, David Paper and Jeffrey Johnson, 'How Business Value Is Extracted from Operational Data: A Case Study' in: Annabeth Aagaard (ed.), *Digital Business Models Driving Transformation and Innovation* (Cham: Palgrave Macmillan 2019), 117-145 (119); Aagaard (n. 21), 6.

²⁹ OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (Paris: OECD 2019), 20.

³⁰ Kettemann (n. 6), 5; Deeks (n. 23), 640-643.

Investment and Multinational Enterprises,³¹ discussions on regulating the behaviour of multinational enterprises were in full swing after the number of reports about unethical and illegal activities undertaken by multinational corporations had increased significantly in the 1970s.³² In the same year, the newly formed United Nations (UN) Commission on Transnational Corporations decided to engage in the drafting of a code of conduct for multinational enterprises – an endeavour which would eventually fail. Also in 1976, the International Labour Organization (ILO) started negotiations which led to the adoption of the ILO Tripartite Declaration on Principles Concerning Multinational Enterprises and Social Policy by the ILO Governing Body in 1977.³³

The OECD Guidelines were not drafted as a stand-alone instrument but as part of a balanced approach to international investments which aimed at connecting protection, non-discriminatory treatment and responsible investor conduct. While the 1976 Guidelines contained strong provisions on employment and labour relations and addressed the main labour and social concerns regarding investors' behaviour of the day, they were nevertheless framed as a non-binding instrument. They were – and still are – framed as recommendations by governments to business. As one of the participants in the negotiations noted, OECD countries were giving a signal that they were willing 'to go far but not further',³⁴ i. e. not to commit to legally binding rules.

Since their adoption in 1976, the Guidelines were revised five times. With regard to their legal status a Decision adopted by the OECD Council in 2000 is particularly relevant. With this Decision, the OECD Council requires countries adhering to the Guidelines to establish so called National Contact Points (NCPs) with the double mandate to promote the implementation of the Guidelines and to serve as a grievance mechanism.³⁵ Since Decisions by the OECD Council are binding, countries adhering to the legally non-binding OECD Guidelines for Multinational Enterprises have now a legal obligation to establish a NCP (see below II.2.b)).

³¹ OECD, Declaration on International Investment and Multinational Enterprises, adopted on 21 June 1976, OECD/LEGAL/014.

³² Christine Kaufmann, *Globalisation and Labour Rights* (London: Hart/Bloomsbury 2007), 156.

³³ Kaufmann (n. 32), 166. The Declaration was last amended in 2017 to include, among others, developments in the UN and the OECD.

³⁴ Kari Tapiola, 'The OECD Guidelines as a Balanced Instrument' in: Nicola Bonucci and Catherine Kessedjian (eds), *40 ans de lignes directrices de l'OCDE pour les entreprises multinationales – 40 Years of the OECD Guidelines for Multinational Enterprises* (Paris: Pedone 2018), 29–32 (30).

³⁵ OECD, Decision of the Council on the OECD Guidelines for Multinational Enterprises, adopted on 27 June 2000, OECD/LEGAL/0307.

As a result, the Guidelines are still soft law for business but have in parts become hard law for governments.³⁶

2. Scope

a) Comprehensive Standard for Responsible Business Conduct (RBC)

The revision in 2011 substantially expanded the scope of the Guidelines in three ways: First, the revision incorporated the UN Guiding Principles (UNGPs)³⁷ by adding a new specific human rights chapter and updated other parts of the Guidelines.

Second, governments agreed to apply the Guidelines across the *whole* value chain. Companies are therefore expected to act responsibly and comply with the Guidelines not only in their own actions but also in their business relationships across the whole value chain. This also implied a departure from what was previously known as the 'investment nexus': Before the 2011 revision, only cases with a link to foreign direct investment could be handled by National Contact Points.

Third, according to the General Policies chapter of the Guidelines, supply chain due diligence applies to *all* topics covered by the Guidelines except for the chapters on science and technology, competition and taxation which were at the time considered not to be linked to negative impacts.³⁸ The Guidelines thus expand the scope of the due diligence framework beyond human rights to cover almost all areas of business activities.³⁹ The due diligence process entails six steps that business should follow: (1) embed responsible business conduct into policies and management systems; (2) identify and assess adverse impacts in operations, supply chains and business relationships; (3) cease, prevent or mitigate adverse impacts; (4) track implementation and results; (5) communicate how impacts are addressed; and (6) provide for or

³⁶ Roel Nieuwenkamp, '40 Years Guidelines and National Contact Points: A Beautiful Glass, But Only Half Full' in: Bonucci and Kessedjian (n. 34), 35-41, (36).

³⁷ UN, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 21 March 2011, UN Doc A/HRC/17/31, adopted by UNHRC Res 17/4: Human Rights and Transnational Corporations and Other Business Enterprises, 16 June 2011, UN Doc A/HRC/RES/17/4.

³⁸ OECD Guidelines for Multinational Enterprises, Commentary on General Policies, 2011 edition, OECD/LEGAL/0144, para. 14.

³⁹ John G. Ruggie and Tamaryn Nelson, 'Human Rights and the OECD Guidelines for Multinational Enterprises: Normative Innovations and Implementation Challenges', *Brown Journal of World Affairs* 22 (2016), 99-127 (106).

cooperate in remediation when appropriate. To support enterprises in the implementation of due diligence on the ground, the OECD Due Diligence Guidance for Responsible Business Conduct provides plain language explanations on the relevant provisions and applies to all enterprises across all sectors.⁴⁰ The (legal) standing of this Guidance was strengthened with its inclusion in a Recommendation by the OECD Council and by the strong support it received from all institutional stakeholders at the OECD.⁴¹ In addition, sector-specific guidance has been agreed for the minerals, extractive, garment and footwear, agricultural, and financial sectors. Except for the guidance for the financial sector, all have become the topic of Council Recommendations.⁴²

As a result, the Guidelines are now a comprehensive, government-backed RBC standard, covering essentially all areas where business interacts with society, including disclosure requirements, human rights, employment and industrial relations, corruption, consumer interests, science and technology, competition and taxation. With a view to digitalisation, it is particularly important to note that the Guidelines are conceived as a ‘living instrument’ by calling on governments to ‘participate in appropriate review and consultation procedures to address issues concerning interpretation of the Guidelines in a changing world’.⁴³

b) Remedy Mechanism

The OECD Guidelines are currently the only international comprehensive standard on responsible business conduct that is equipped with a

⁴⁰ OECD, *OECD Due Diligence Guidance for Responsible Business Conduct* (Paris: OECD 2018); OECD, Recommendation of the Council on the OECD Due Diligence Guidance for Responsible Business Conduct, adopted on 30 May 2018, OECD/LEGAL/0443.

⁴¹ OECD, Recommendation of the Council on the OECD Due Diligence Guidance for Responsible Business Conduct, adopted on 30 May 2018, OECD/LEGAL/0443.

⁴² OECD, Recommendation of the Council on Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, adopted on 25 May 2011, amended on 17 July 2012, OECD/LEGAL/0386; OECD, Recommendation of the Council on the Due Diligence Guidance for Meaningful Stakeholder Engagement in the Extractive Sector, adopted on 13 July 2016, OECD/LEGAL/0427; OECD, Recommendation of the Council on the OECD Due Diligence Guidance for Responsible Supply Chains in the Garment and Footwear Sector, adopted on 17 May 2017, OECD/LEGAL/0437; OECD, Recommendation of the Council on the OECD-FAO Guidance for Responsible Agricultural Supply Chains, adopted on 13 July 2016, OECD/LEGAL/0428; OECD, *Responsible Business Conduct for Institutional Investors: Key Considerations for Due Diligence Under the OECD Guidelines for Multinational Enterprises* (Paris: OECD 2017).

⁴³ OECD Guidelines (n. 38), Chapter I, Concepts and Principles, para. 11.

state-based, non-judicial remedy mechanism, the National Contact Points for Responsible Business Conduct. OECD member states and countries adhering to the OECD Investment Declaration and the Guidelines have a legally binding obligation to establish a functioning NCP.⁴⁴ As of August 2021, all 38 OECD members and 12 non-member-countries have adhered to the Guidelines.⁴⁵

National Contact Points are responsible for furthering the effectiveness of the Guidelines. They have existed since the 1983 update of the Guidelines and they have had the ability to receive cases, so called ‘specific instances’ related to the non-observance of the Guidelines since the year 2000.

The last revision of the Guidelines in 2011 not only brought about significant changes in the substantive chapters such as the inclusion of a new human rights chapter, but also with regard to the implementation procedures.

The Guidelines do not prescribe a model for establishing an NCP. Instead, a government has autonomy and flexibility in choosing the form and structure of its NCP as long as it complies with the Guidelines and ensures the effectiveness and functioning of the NCP. In line with the provisions for non-judicial grievance mechanisms in the UNGP,⁴⁶ the Guidelines require all NCPs to be visible, accessible, transparent and accountable. In addition, when handling cases NCPs must do so in a way that is impartial, predictable, equitable and in accordance with the Guidelines.⁴⁷ Since 2000, the NCPs have handled over 500 specific instances.⁴⁸

As a recent report illustrates, the Guidelines’ approach to square adherent countries’ sovereignty by leaving the institutional set-up in their hands with the need for a coherent grievance system that operates based on principles common to all NCPs, has only been partially successful. Some NCPs lack adequate government support in terms of institutional, financial and human resources which would enable them to address complex issues such as digital developments effectively. Some apply higher procedural bars than others,

⁴⁴ OECD, Decision (n. 35), para. I. 1.

⁴⁵ Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Jordan, Kazakhstan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Morocco, Netherlands, New Zealand, Norway, Peru, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Tunisia, Turkey, Ukraine, United Kingdom, United States, Uruguay.

⁴⁶ UNGP 31 (n. 37).

⁴⁷ OECD Guidelines (n. 38), Procedural Guidance, paras I. and I. C.

⁴⁸ OECD, *Annual Report on the OECD Guidelines for Multinational Enterprises 2019* (Paris: OECD 2020), 24.

making them less accessible. Finally, guaranteeing equitable and safe proceedings is an ongoing challenge.⁴⁹

c) Territorial Scope

In traditional international law, based on the concept of sovereignty a state is competent to establish (prescribe), apply (adjudicate), and enforce rules of conduct in respect of persons, property or events within its territory. From this perspective, *enforcing* rules extraterritorially is generally prohibited under international law unless permitted by specific rules or with the consent of the respective state.⁵⁰ Hence, domestic law can be *established* and *applied* on extraterritorial events provided that there is a sufficient territorial connection between the state and the extraterritorial event and no rule of international law prohibits such extraterritorial application.⁵¹ In contrast to this traditional general approach,⁵² extraterritorial legal practices have always been applied in competition and antitrust law based on the doctrine of effects⁵³. Moreover, they have recently rather become the rule than the exception in other areas of law, particularly in a digital context where they align at the *legal* level with developments aiming at *technical* interoperability as discussed above (I.1.a)).⁵⁴ Examples include regulations of transboundary data flows and data protection such as the General Data Protection Regulation (GDPR), which protects European users' data regardless of the jurisdiction it is processed in.⁵⁵ In other

⁴⁹ OECD, *National Contact Points for Responsible Business Conduct Providing Access to Remedy: 20 Years and the Road Ahead* (Paris: OECD 2020), 28-35.

⁵⁰ PCIJ, *The Case of the S. S. Lotus (France v. Turkey)*, judgment of 7 September 1929, PCIJ Reports Series A No. 10, 18-19.; PCA, *Netherlands v. United States of America (Island of Palmas)*, award of 4 April 1928, Reports of International Arbitration Awards II, 829-871 (838).

⁵¹ PCIJ, *S.S. Lotus* (n. 50), 19; Christine Kaufmann, Christoph Good, Sabrina Ghielmini and Charlotte Blattner, *Extraterritorialität im Bereich Wirtschaft und Menschenrechte: Extraterritoriale Rechtsanwendung und Gerichtsbarkeit in der Schweiz bei Menschenrechtsverletzungen durch transnationale Unternehmen* (Bern: Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)/Swiss Center of Expertise in Human Rights 2016), paras 28-29.

⁵² Menno T. Kamminga, 'Extraterritoriality' in: Rüdiger Wolfrum (ed.), *MPEPIL* (online edn., Oxford: Oxford University Press 2012), para. 3.

⁵³ Roger P. Alford, 'The Extraterritorial Application of Antitrust Laws: The United States and the European Community Approaches', *Va. J. Int'l L.* 33 (1992-1993), 1-50 (5, 8-27).

⁵⁴ Lorenz Langer, 'Cyberspace Does not Lie Within Your Borders – Jurisdiktion und Menschenrechte im digitalen Raum', *Swiss Review of International and European Law* 20 (2019), 3-21.

⁵⁵ EU Regulation 2016/679 (2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) applies to companies from outside the EU that use the personal data of European citizens.

words, legal protection should follow the data as it travels through interconnected networks and ideally provide an equal level of protection across technical systems and platforms.

Turning to the OECD Guidelines, their territorial scope may seem rather limited with 50 countries adhering to them. However, the reach of the OECD Guidelines goes beyond in two regards: First, they apply to all companies operating *in and from* the territory of the 50 adherents.⁵⁶ Second, cases of suspected non-compliance with the Guidelines can be filed with the NCP of the country *where the issues have arisen*.⁵⁷ The term ‘issue’ refers not only to impacts but can also entail policy decisions taken at company headquarters.

As a result of this broad scope, any NCP can address various scenarios involving companies

(a) based in the NCP’s country and operating in it; or

(b) based in any other country, whether adherent or not, and operating in the country of the NCP; or

(c) based in the NCP’s country and operating in any other country, whether adhering or not.⁵⁸

A third element that contributes to the expansion of the scope is the fact that the Guidelines cover the entire value chain and thereby allow for accommodating all relevant actors whether private or public, at home or abroad.

As a result of this broad scope, NCPs have since 2000 addressed cases involving issues arising in over 100 countries and territories, including over 50 non-adhering countries.⁵⁹ An example in this regard is a case filed with the United Kingdom (UK) NCP alleging that a UK based company had breached the general policies and human rights provisions of the Guidelines by supplying surveillance equipment to agencies of the Bahrain government which had used it to target pro-democracy activists.⁶⁰

In sum, the Guidelines take up the mentioned concept of ‘connection’ and allow for a deterritorialisation⁶¹ to the extent that they can apply to actors and issues beyond an adhering country’s territory.⁶² This is particu-

⁵⁶ See para. 1, OECD Declaration on International Investment (n. 31).

⁵⁷ OECD, *Guide for National Contact Points on Coordination when Handling Specific Instances, OECD Guidelines for Multinational Enterprises* (Paris: OECD 2019), 6.

⁵⁸ OECD, 20 years (n. 49), 19.

⁵⁹ OECD, 20 Years (n. 49), 19; OECD Annual Report 2019 (n. 48), 45.

⁶⁰ UK National Contact Point for the OECD Guidelines for Multinational Enterprises, *Privacy International & Gamma International UK Ltd.: Final Statement after Examination of Complaint*, December 2014 <<https://www.gov.uk/government/organisations/uk-national-contact-point>>.

⁶¹ On the notion of deterritorialisation see Kettemann (n. 6), 298–302.

⁶² OECD, *Guide on Coordination* (n. 57), 6.

larly important in the context of digital technologies which by design do not fit traditional categories of territorial jurisdiction. The fact that NCPs are framed as national institutions does not change this finding because the possibility of applying the Guidelines beyond an adherent's territory is part of the binding Council Decision on NCPs.⁶³ However, as mentioned (II.2.b)) NCPs apply different standards for accepting specific instances which may result in different practices for considering cases with an extraterritorial dimension and in the long term result in a risk for forum shopping.

d) Digitalisation and Responsible Business Conduct

While the Guidelines do not mention digitalisation, there are manifold links between the Guidelines' key topic responsible business conduct and digitalisation. On the one hand, digital tools can foster responsible business conduct as they support business in implementing the Guidelines, for example by allowing for assessing risks more effectively with artificial intelligence and big data analytics or tracing the origins of a product with the help of blockchain.⁶⁴

On the other, digitalisation can lead to new ways of business being associated with human rights infringements or social and environmental harms. Three main categories of such negative business impacts can be identified: First, *digital technologies themselves* may have negative impacts, for example a software based on artificial intelligence that applies criteria which lead to discriminatory results in recruiting.⁶⁵ A second group for such impacts relates to the *use or abuse of digital technologies by buyers*

⁶³ OECD, Council Decision (n. 35), para. I. 1 and the related Guidance on Coordination (n. 57), 6.

⁶⁴ OECD, *Digitalisation and Responsible Business Conduct: Stocktaking of Policies and Initiatives* (Paris: OECD 2020), 8-10; OECD, *Is There a Role for Blockchain in Responsible Supply Chains?* (Paris: OECD 2019), 13-15; Martijn Boersma and Justine Nolan, 'Can Blockchain Help Resolve Modern Slavery in Supply Chains?', *Academy of International Business (AIB) Insights*, 20 (2020), <<https://doi.org/10.46697/001c.13542>>; Kai Behnke and Marijn F. W. H. A. Janssen, 'Boundary Conditions for Traceability in Food Supply Chains Using Blockchain Technology', *International Journal of Information Management* 52 (2020), 101969, 4-5.

⁶⁵ An example is Amazon stopping the use of an AI-based recruitment tool because it discriminated against female applicants. Reuters, 'Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women', 18 October 2018 <<https://reut.rs/2Od9fPr>>; Prasanna Tambe, Peter Cappelli and Valery Yakubovich, 'Artificial Intelligence in Human Resources Management: Challenges and a Path Forward', *California Management Review* 61 (2019), 15-42 (16).

and consumers.⁶⁶ Examples include surveillance software which is used for privacy invasions⁶⁷ or the use of artificial intelligence with recognition tools for racial profiling leading for instance International Business Machines Corporation (IBM) to sunset its general purpose facial recognition and analysis software products.⁶⁸ The abuse of social media platforms by users for hate speech falls within the same group. In the environmental context, the substantial rise in energy consumption of applying digital tools such as blockchain mentioned before (I.2.a)) with its negative impact on the climate can be noted.⁶⁹ In these examples the question arises, who is responsible. The vendor or the buyer or both? The provider of the digital infrastructure such as the online platform or the blockchain? A third category of negative impacts can be identified with regard to *new digital business models and digital business methods*. For instance, online platforms can come with lower levels of worker protection, and automation as a digitalised means of production can displace jobs with negative effects on some workers while creating new opportunities and jobs for others.⁷⁰

Several cases filed with NCPs included a digital component; they will be discussed in more detail in section III.

The question thus remains how the Guidelines and international soft and hard law in general can accommodate this complex web of actors involved and attribute specific responsibilities to them to effectively ensure responsible business conduct.

3. Beyond Hard and Soft Law: Accommodating a Changing World

a) Distinctive Features of the Guidelines

Compared with other non-binding instruments on responsible business conduct addressed to states,⁷¹ the OECD Guidelines' regulatory approach is

⁶⁶ In the context of Artificial Intelligence seven use cases or patterns have been identified. See OECD, *Artificial Intelligence & Responsible Business Conduct* (Paris: OECD 2019), 1-2 <<http://mneguidelines.oecd.org/rbc-and-digitalisation.htm>>.

⁶⁷ South Wales Court of Appeals (n. 3).

⁶⁸ IBM CEO's Letter to Congress on Racial Justice Reform, 8 June 2020, <<https://www.ibm.com>>.

⁶⁹ Steffen Lange, Johanna Pohl and Tilman Santarius, 'Digitalization and Energy Consumption. Does ICT Reduce Energy Demand?', *Ecological Economics* 176 (2020), 106760, 3.

⁷⁰ International Labour Organization (ILO), *World Employment and Social Outlook 2021: The Role of Digital Labour Platforms in Transforming the World of Work* (Geneva: International Labour Office 2021).

⁷¹ E.g. UNGP (n. 37); ILO Tripartite Declaration (n. 33).

unique from an international law perspective because it not only combines binding obligations and soft law for states with non-binding 'hard expectations' on business but also adds a binding obligation for states to establish a grievance mechanism. This is to a large extent a continuation of efforts departing from traditional state-centred international law in order to acknowledge business as a relevant actor with specific responsibilities in international law. The discussions in the UN on a Code of Conduct on Transnational Corporations started in the 1970s but after decades eventually failed, and the following discussions on 'Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights' resulted in the UN Human Rights Commission taking note of them but not approving them and stating explicitly that they had no legal standing.⁷² The major breakthrough happened with the adoption of the UNGP in 2011 and the related revision of the OECD Guidelines in 2011: Business is acknowledged as a relevant actor with specific responsibilities. These responsibilities are framed in a legally non-binding instrument. With the OECD Guidelines, this lack of enforceability is partially compensated with the legally binding obligation for states to establish National Contact Points as a grievance mechanism.⁷³

While the combination of binding obligations on states with non-binding expectations on business is a well-known concept to overcome the conceptual difficulties in accommodating business as actors in international law, the way in which the NCP grievance mechanism is added to the substantive standards results in a rather puzzling picture: The non-binding Guidelines call on adhering governments to state clear expectations on business to act responsibly by conducting due diligence across the whole supply chain. The legally binding Decision by the OECD Council requires adhering countries to establish functioning National Contact Points to not only promote the Guidelines but also serve as a grievance mechanism for handling complaints. As a result, governments have a legal obligation to establish a National Contact Point as a grievance mechanism for the Guidelines, but companies are not required to participate in these procedures given that the Guidelines themselves are not binding for business.

However, the perspective of being affiliated with an alleged breach of the Guidelines and a respective NCP procedure adds some teeth to what may at first glance look like a purely voluntary instrument. In addition, apart from

⁷² UN Human Rights Commission, Decision 2004/116, Responsibilities of transnational corporations and related business enterprises with regard to human rights.

⁷³ Above n. 35 and accompanying text.

incorporating parts of the Guidelines and their due diligence concept in binding national law,⁷⁴ some governments, including among others Canada, Germany, and the Netherlands decided to tie their (soft) expectations on companies with 'hard' consequences in case of non-fulfilment such as the denial of trade diplomacy benefits or the consideration of responsible business conduct compliance in public procurement.⁷⁵

A final special feature of the OECD Guidelines relates to policy coherence. With the increasing demand on business to follow responsible business conduct standards, the role of governments has also gained attention. Internationally agreed RBC standards touch upon a range of policy areas including *inter alia* human rights, trade and investment policies, and health issues. Accordingly, the UN Guiding Principles and the OECD Guidelines have included provisions on policy coherence.⁷⁶ In their implementation governments are therefore called upon to mainstream responsible business conduct across relevant national policies to ensure coherence with the international standards they have agreed to. In addition, the OECD Council emphasised at various occasions the role of governments in fostering policy coherence on responsible business conduct⁷⁷ and explicitly included 'promoting national and international policy coherence on responsible business conduct' as an overarching objective in the renewed mandate for

⁷⁴ Countries that are considering or have already introduced mandatory due diligence requirements based on the OECD Guidelines include France (Loi no. 2017-399 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre of 27 March 2017), Finland, Germany, (Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten of 16 July 2021, BGBl 2021 I Nr. 46, 2959), The Netherlands, Norway, and Switzerland.

⁷⁵ Canada: 'There are consequences if Canadian companies do not participate, or do not engage in good faith and constructively, in the NCP dispute resolution process. Consequences are withdrawal of Government of Canada trade advocacy support abroad. Further, non-participation or the lack of good faith participation will also be taken into account in the Corporate Social Responsibility-related evaluation and due diligence conducted by the Government of Canada's financing crown corporation, Export Development Canada, in its consideration of the availability of financing or other support.' <<https://www.international.gc.ca/trade-agreements-accords-commerciaux/ncp-pcn/>>; In the Netherlands endorsement of and compliance with the OECD Guidelines have been a hard requirement for companies applying for a grant or private sector support under the foreign trade and development budget. See NL Ministry of Foreign Affairs, From Giving Information to Imposing Obligations: A new Impulse for Responsible Business Conduct (The Hague: Ministry of Foreign Affairs, Policy note, 16 October 2020 <<https://www.government.nl/topics/responsible-business-conduct-rbc/evaluation-and-renewal-of-rbc-policy>>), 9-10.

⁷⁶ UNGP 8 (n. 37), OECD Guidelines (n. 38), preface, para. 9.

⁷⁷ For example in the Recommendation of the Council on the Policy Framework for Investment adopted on 13 May 2015, OECD/LEGAL/0412 and the Policy Framework for Investment, adopted on 12 May 2015, C/MIN(2015)5.

the Working Party on Responsible Business Conduct which entered into force on 1 January 2019.⁷⁸

b) Accommodating New Developments and New Actors

With the mentioned features the Guidelines hardly fit the traditional categories of binding hard law on the one hand and non-binding, voluntary standards on the other. Instead, their non-binding format combined with hard expectations and sometimes hard consequences places them somewhere in between and allows them to overcome the dichotomy between binding and non-binding rules. This *sui generis, hybrid regulatory model* and the fact, that the Guidelines address both public and private actors and include global value chains contribute to a *holistic responsible business conduct approach*. Such a hybrid, holistic approach can respond to new developments in a more flexible and timely manner than traditional instruments of international law.

Still, the question remains whether and how these distinct features succeed in addressing the new challenges that digitalisation poses on responsible business conduct, or whether a new regulatory design is needed. The following section will look at some key effects of digitalisation and the related challenges for responsible business conduct.

III. Interactions Between Digitalisation and Responsible Business Conduct

Until March 2021, 14 cases with a digital component were submitted to National Contact Points. This section presents the cases that address the key issues discussed in this article, it is based on publicly available information only.⁷⁹

1. New Notion and Models of Business

a) Online Platforms

As outlined above (I.2.b)), online platforms are still a relatively recent phenomenon and they raise specific questions with regard to responsible

⁷⁸ Mandate of the Working Party on Responsible Business Conduct, revised on 27 November 2018, DAF/INV/RBC(2018)26, published in the On-Line Guide to OECD Intergovernmental Activity <<https://oecdgroups.oecd.org>>.

⁷⁹ OECD database on specific instances <<http://mneguidelines.oecd.org>>.

business conduct:⁸⁰ What is the distinction between online platforms as tech companies and physical, real-world companies?⁸¹ Is Uber an online platform or a transport company, or both?⁸² Can such platforms be considered a multinational enterprise under the OECD Guidelines and therefore be responsible for conducting due diligence and be subject to proceedings before National Contact Points? What are the specific duties and responsibilities of platform operators towards platform users? How far do due diligence requirements for platform operators go?⁸³

The Polish National Contact Point recently addressed some of these issues in a case submitted by a non-governmental organisation (Frank Bold Foundation) against a company (Grupa OLX) located in Poland and operating an online advertising platform.⁸⁴ The company is a member of the OLX Group with its headquarters in the Netherlands. The NGO argued that the company had breached several provisions of the OECD Guidelines by placing advertisements on its portal concerning sale offers for furnaces for, *inter alia*, burning processed oil and discarded wooden railway sleepers. Since burning such hazardous waste would result in negative environmental impacts and was prohibited by law, the company should take actions to prevent users of its portal to post such sale offers.

⁸⁰ For the manifold regulatory challenges see European Law Institute, *Model Rules on Online Platforms* (Vienna: European Law Institute 2019), 7; Alain Strowel and Wouter Vergote, 'Digital Platforms: To Regulate or Not to Regulate? Message to Regulators: Get the Economics Right First, then Focus on the Right Regulation' in: Bram Devolder (ed.) *The Platform Economy: Unravelling the Legal Status of Online Intermediaries* (Cambridge: Intersentia 2019), 3-30; Manfred Weiss, 'The Platform Economy, the Main Challenges for Labour Law' in: Lourdes Mella Méndez (ed.), *Regulating the Platform Economy: International Perspectives on New Forms of Work* (London/New York: Routledge Taylor & Francis Group 2020), 11-20.

⁸¹ DeNardis (n. 2), 12.

⁸² The European Court of Justice qualified Uber as a 'service in the field of transport' within the meaning of Article 58(1) TFEU and thus outside of the scope of Article 56 TFEU and the Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1; ECJ, *Asociación Profesional Élite Taxi v. Uber Systems Spain SL*, judgment of 20 December 2017, case no. C-434/15, ECLI:EU:C:2017:981 and ECJ, *Uber France SAS v. Nabil Bensalem*, judgment of 10 April 2018, case no. C-320/16, ECLI:EU:C:2018:221. In contrast, it considered Airbnb as an 'information society service' under Directive 2000/31; ECJ, *X v. Airbnb Ireland and others*, judgment of 19 December 2019, case no. C-320/18, ECLI:EU:C:2019:1112.

⁸³ Karin Buhmann and Roxana Olivera, 'Human Rights and Social Media Platforms: The Corporate Responsibility to Respect Human Rights in Regard to Privacy Infringements Involving Photo Posting', *Australian Journal of Human Rights* 26 (2020), 124-141, (134-137).

⁸⁴ Polish National Contact Point for the OECD Guidelines for Multinational Enterprises, *Grupa OLX Sp. z o.o. and Frank Bold Foundation*, <<http://mneguidelines.oecd.org/database/instances/pl0005.htm>>.

In its initial assessment, the Polish NCP qualified the company as a multinational enterprise operating in the Polish market. For the following procedure, two questions were of particular relevance for the Polish NCP: First, the responsibilities of entities operating online advertisement portals, and second the responsibility of entities marketing products the use of which has an adverse impact on the environment.⁸⁵

From the outset, the parties had agreed that the company in its role as provider of the online platform was not directly responsible for the sale of the products but that it should seek to prevent the posting of sale offers for products which are highly probable to violate the provisions on the environmental protection. As a result of the mediation, the company accepted its responsibilities under Chapters II (General Principles), VI (Environment) and VIII (Consumer Interests) of the OECD Guidelines and the parties agreed on a set of measures to prevent the publication of advertisements concerning products and services which might have an adverse impact on the environment. Following-up on the NCP procedure, more than 16'000 advertisements were eventually removed by the company, and in more than 6'500 cases advertisers were reminded by the company to take environmental issues into account.

Another case relating to new digital business models was submitted to the French National Contact Point in March 2020 by a French business association in the tourism and hospitality sector concerning activities of the online platform Airbnb in France. While the submission raises issues about the application of the Guidelines' Chapter XI on Taxation, the French NCP also had to consider the nature of Airbnb, i. e. the question of whether it qualifies as a multinational enterprise under the Guidelines. The qualification is relevant because the Guidelines with their specific expectations for due diligence and their grievance mechanism are only applicable to 'multinational enterprises'. However, the Guidelines deliberately do not provide a definition and even state that 'a precise definition of multinational enterprises is not required for the purposes of the Guidelines'.⁸⁶ In the absence of an authoritative interpretation⁸⁷ there is room for considering new phenomena such as online platforms. Accordingly, in its Initial Assessment the French NCP refers to Airbnb as a 'digital company' within the scope of the Guidelines.⁸⁸

⁸⁵ Polish OECD NCP (n. 84), Final Statement of alleged non-observance of the OECD Guidelines for Multinational Enterprises, 13 June 2019, 4.

⁸⁶ OECD Guidelines (n. 38), para. I. 4.

⁸⁷ Which would be with the Investment Committee: OECD Guidelines (n. 38), Procedural Guidance, para. II. 1.

⁸⁸ French National Contact Point for the OECD Guidelines for Multinational Enterprises, Initial Assessment *Airbnb in France*, 14 December 2020, para. 4.2 and the related Statement of 4 June 2020, acknowledging receipt of the specific instance. The Final Statement was issued on 1 June 2021. <<http://mneguidelines.oecd.org/database/instances/fr0031.htm>>.

b) Accommodating New Business Models – Can the Guidelines Deliver?

The Polish case is one of the few cases related to digital technologies that have been handled by National Contact Points. While statements by individual NCPs do not serve as precedent for others, the Polish case is nevertheless particularly relevant because it shows that the Guidelines with their broad unspecified notion of multinational enterprise can in principle accommodate *new business models* such as online platforms. However, it may be more complex to determine which National Contact Point should take the lead when several countries are involved in the provision of a digital service⁸⁹ or in business models based on distributed ledger technologies (blockchain) and smart contracts (above I.2.a)).

A second interesting conclusion is the role of the Guidelines in fostering *policy coherence* which was emphasised in the Polish case: The due diligence requirements of the online platform provider were interpreted with a view to align them with the goals of the environmental protection law. This is an important finding with regard to ongoing regulatory efforts to address online platform providers' responsibility, particularly in Europe. New regulations such as the GDPR,⁹⁰ the Regulation on platform-to-business relations⁹¹ and the European Commission's plans to address the development of new digitally-based business models in its Digital Service Act package⁹² illustrate that a more holistic approach in defining online platforms' responsibilities and protecting their users is gaining momentum. Such a holistic approach has also been developed by Australian regulators with a call for reforming the public sector data infrastructure with an integrated, comprehensive framework that would enhance data access and use and foster innovation and competition while at the same time establishing new corresponding consumer rights.⁹³

2. Supply Chains and Due Diligence

Digital technologies, services and infrastructures such as artificial intelligence, distributive ledger (blockchain) or big data affect the structure of

⁸⁹ French OECD NCP, *Airbnb France* (n. 88).

⁹⁰ Above n. 55.

⁹¹ EU Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

⁹² Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final, 15 December 2020.

⁹³ Australian Government Productivity Commission, 'Data Availability and Use', Inquiry Report, No. 82, 31 March 2017, 173-175, <<https://www.pc.gov.au>>.

global supply chains and as well as methods and instruments for conducting due diligence. In addition, using these technologies can lead to more efficient transactions and facilitate adjustments to changing environments such as consumer demands.

a) Applying Due Diligence to Digital Technologies

The following selected cases brought before National Contact Points illustrate how the OECD Guidelines due diligence requirements can apply to digital products and services.

The German National Contact Point was seized with the question whether a company assuming maintenance responsibilities for surveillance technology for the Bahraini government contributed to human rights violations through the prosecution and government authorities in Bahrain. The NCP rejected the complaint as far as it alleged that the company was partly responsible for human rights violations in Bahrain but offered its help to resolve the questions raised in the context of the allegation that the company did not have a management system in place to analyse the risk of any possible negative effects of its business activities on human rights. However, the complainants decided not to take part in the process offered by the NCP.⁹⁴

A related case received by the UK National Contact Point in the same context against the UK based company Gamma led to interesting findings.⁹⁵ The submitting NGO argued that Gamma supplied to the Bahrain authorities 'malware' products which allowed them to access and record private conversations, correspondence, and other records (e.g. address books) of individuals involved in pro-democracy activities in Bahrain. In a first step, the NCP concluded that while neither party had provided direct evidence about a supply by Gamma to Bahrain, the evidence provided suggested that the company's product may have been used against Bahraini activists. For this reason, the NCP decided to accept the case for further consideration regarding the company's obligations to conduct appropriate due diligence and to address its impacts.⁹⁶

⁹⁴ German National Contact Point for the OECD Guidelines for Multinational Enterprises, *ECCHR et al. and Trovicor GmbH*, <<http://mneguidelines.oecd.org/database/instances/de0015.htm>>, Final Statement, 21 May 2014.

⁹⁵ UK OECD NCP, *Specific Instance Notified by the NGO Privacy International Regarding the Activities of Gamma International UK Operating in Bahrain*, <<http://mneguidelines.oecd.org/database/instances/uk0034.htm>>.

⁹⁶ UK OECD NCP (n. 95), Initial Assessment, June 2013, para. 25.

After mediation had taken place, the NCP published its Final Statement. This Statement is remarkable in several regards: First, it contains – as it seems for the first time in a digital context – a section on the ‘UK NCP’s understanding of the product’. In this section, the NCP identifies the elements of the technology which are relevant for determining the company’s due diligence requirements.⁹⁷ Among them were the design of the software tools, their targets and the underlying contracts. While the NCP could not verify the allegations that Gamma was linked to human rights abuses through a supply to Bahrain, it concluded that the company’s due diligence did not comply with the Guidelines and that its approach was not consistent with the Guidelines general obligation to respect human rights. Interestingly, the NCP acknowledged, although in rather general terms, the sector’s specific needs for limiting the information publicly available about products, customers, and operating standards.⁹⁸

The case illustrates that in the absence of a company’s engagement it is very difficult if not impossible for the NCP to establish the facts and obtain a more thorough understanding on how the technology works. In an area where developments are mainly driven by the private sector as mentioned afore the lack of a corporate obligation to engage in the process and provide information is particularly challenging. The UK NCP reflected on this unsatisfactory situation in its Follow-up Statement. The NCP clearly stated that software providers are not dispensed from complying with the Guidelines and that the company’s ‘failure to engage was therefore an individual choice rather than an unavoidable result of the nature of the business’.⁹⁹ Turning back to the quote at the outset of this article, the UK NCP thus gave a clear answer.

Another case relates to the Internet of Things (above I.1.a)) and specifically to drone attacks in Yemen in 2012 and 2013 in which allegedly communication technology developed by a German company was used via a US company supplying the drones for the US armed forces. Since the German company had only entered an agreement with the US company about supplying radio transmitters in 2014, the German NCP did not consider the specific human rights violations taking place in 2012/13 but the German company’s general due diligence policy. In this context, it analysed whether supplying the radio transmitters could establish a ‘direct link’ to potential human rights abuses as defined in Chapter IV (Human Rights), para. 3 of the OECD Guidelines, i. e. the question whether the company caused or con-

⁹⁷ UK OECD NCP (n. 95), Final Statement, December 2014, paras 29-31.

⁹⁸ UK OECD NCP (n. 95), Final Statement, December 2014, para. 63.

⁹⁹ UK OECD NCP (n. 95), Follow-up Statement, February 2016, para. 11.

tributed to such abuses. After examining the functioning of the drones and the role of the radio transmitters, it came to the conclusion that a direct link could be ruled out since the radio transmitters covered by the agreement were unable to navigate drones, particularly over greater distances. As a result, the case was not accepted for further consideration.¹⁰⁰

In June 2020, the Swiss NCP received a specific instance from an NGO against Union Bank of Switzerland (UBS), an investment bank and financial services company, concerning alleged human rights violations in the context of UBS' business relationship with the Chinese company Hikvision. According to the submitting party, Hikvision manufactures technology used to monitor Uighurs in the Chinese province of Xinjiang. The Swiss NCP decided in its initial assessment that some of the issues raised merit further consideration.¹⁰¹ The case concerns complex questions about the development and use of facial recognition software and thus an application of artificial intelligence (above I.1.c)) and the alleged involvement of an investor in related human rights abuses.

The examples confirm that the Guidelines' due diligence framework is not limited to analogue business, products and services but applies to the digital world as well. This expands the extraterritorial reach of the Guidelines and the related due diligence expectations considerably, given that as outlined before, digital services and platforms are inherently of a transboundary nature. At the same time, applying due diligence in a specific case that relates to digitalisation provides several challenges: Unlike in the analogue world, private companies and actors are the main drivers of digital innovation, and state regulation will by design in many cases lag behind.¹⁰² In addition, new developments are often protected by business confidentiality regulations and National Contact Point procedures are of a voluntary nature. As a result, establishing the facts, including the key operational facts of digital product or service may be challenging for National Contact Points and government authorities at large. For example, determining whether the use of facial recognition software may have discriminatory effects requires insights in the criteria which are programmed into the algorithm and thus a feature which

¹⁰⁰ German OECD NCP, *NGO in the UK and Communication Technologies*, Final Statement, 13 July 2015, <<http://mneguidelines.oecd.org/database/instances/de0024.htm>>.

¹⁰¹ Swiss National Contact Point for the OECD Guidelines for Multinational Enterprises, *Society for Threatened Peoples Switzerland and UBS*, Initial Assessment, 20 January 2021, <<http://mneguidelines.oecd.org/database/instances/ch0021.htm>>.

¹⁰² A notable exception is the new Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 COM (2020) 593 final, 24 September 2020, which *inter alia* aims at Facebook's Libra (now Diem) project and thus a crypto-currency that does not yet exist.

may be essential for a company's competitive advantage and be protected by business secrecy rules.¹⁰³

b) Applying Digital Technologies for Conducting Due Diligence

Digital technologies are not only subject to due diligence themselves but can also play a role in facilitating due diligence. In this regard, *big data analytics* feature prominently in corporate risk management systems as they allow for gathering large quantities of data which could not be analysed by humans. As recent studies indicate machine learning and artificial intelligence could further assist companies in assessing risks related to their supply chains.¹⁰⁴ Including a responsible business conduct lens in the application and the development of such instruments would allow for an integrated approach as it has been suggested by scholars.¹⁰⁵

In addition, due to its specific features mentioned above (I.2.a)), *block-chain* can play an important role in conducting due diligence.¹⁰⁶ It can support business in addressing some of the supply chain challenges such as the lack of transparency due to inconsistent or missing data, inaccuracy of risk information, fragmented supply chains due the lack of interoperability of data systems between the different actors and the complexity of tracing the origin and provenance of goods.¹⁰⁷ Due diligence projects using block-chain have been successfully initiated in various sectors, including garment, agriculture, minerals and information and communications technology (ICT).¹⁰⁸

Moreover, *smart contracts* (above I.2.a)) are important to note from a responsible business conduct perspective because of the reduced risk of tampering and the added layer of legal security given that a change of the

¹⁰³ Moritz Büchi, Eduard Fosch Villaronga, Christoph Lutz and Aurelia Tamò Larrieux, 'The Chilling Effects of Algorithmic Profiling: Mapping the Issues', *Computer Law & Security Review* 36 (2020), 105367.

¹⁰⁴ George Baryannis, Sahar Validi, Samir Dani and Grigoris Antoniou, 'Supply Chain Risk Management and Artificial Intelligence: State of the Art and Future Research Directions', *International Journal of Production Research* 57 (2019), 2179-2202.

¹⁰⁵ Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment', *Computer Law & Security Review* 34 (2018), 754-772; Rolf H. Weber, 'Socio-ethical Values and Legal Rules on Automated Platforms: The Quest for a Symbiotic Relationship', *Computer Law & Security Review* 36 (2020), 105380.

¹⁰⁶ Sina Rafati Niya, Danijel Dordevic, Atif Ghulam Nabi and Tanbir Mann, 'A Platform-independent, Generic-purpose, and Blockchain-based Supply Chain Tracking', *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (Seoul: 2019), 11-12.

¹⁰⁷ OECD, *Blockchain* (n. 64), 10-11.

¹⁰⁸ OECD, *Blockchain* (n. 64), 15.

contractual terms on a blockchain is – by its technical design – hardly possible.¹⁰⁹

As a result, it has been argued that blockchain technology can increase overall confidence in the proper operation of a particular system such as a supply chain and eliminate the need for a centralised trusted authority or even trust in the participants of a blockchain network. However, this requires an underlying system of good governance to prevent actors from acting in a way that undermines confidence in the system as a whole.¹¹⁰ The obvious option of applying principles of rule of law to the digital world has already been discussed in the broader context of Internet Governance.¹¹¹ Yet it is complex with regard to blockchain because of the inherent tension between the rule of law as a principle defined and enforced by states on the one hand, and the ‘rule of code’ defined and enforced by technology on the other.¹¹² With a view to existing international standards on responsible business conduct it therefore needs to be explored how rule of law principles can be applied in the context of a blockchain based system that is by definition decentralised with neither a central coordination authority nor a mechanism for enforcing the rules on all participants. Finally, while applying blockchain in this context seems promising, the tremendous levels of energy consumption required for operating at least some distribute ledger technologies and their impact on the climate also need to be part of the analysis.¹¹³

IV. Conceptual Implications of Complex Interactions

As the previous sections show, digitalisation introduces new actors, new notions and models of business and new types of impacts on peoples’ daily lives that are relevant in a responsible business context. While the OECD Guidelines for Multinational Enterprises with their *sui generis*, hybrid nature are on the one hand strongly anchored in international law and on the other designed as a flexible living instrument, the question still arises whether they are able to fully accommodate new developments in the digital world and

¹⁰⁹ Weber (n. 26), para. 16.

¹¹⁰ Primavera de Filippi, Morshed Mannan and Wessen Reijers, ‘Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance’, *Technology in Society* 62 (2020), 101284, 8-9.

¹¹¹ Rolf H. Weber and R. Shawn Gunnarson, ‘A Constitutional Solution for Internet Governance’, *Columbia Science and Technology Law Review* 14 (2012), 1-71.

¹¹² De Filippi, Mannan and Reijers (n. 110), 9.

¹¹³ For a nuanced view: Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen and Robert Keller, ‘The Energy Consumption of Blockchain Technology: Beyond Myth’, *Business and Information Systems Engineering* 62 (2020), 599-608.

what lessons can be drawn from the discussion so far for the role of international law in this context.

1. Mind the Gap: Responsibilities of States and Business

As mentioned before, innovation and technological progress in a digital world is to a large extent driven by private actors, including industry and individuals. Recent examples illustrate how challenging it is for states to keep up with digital developments both in applying such technologies as well as in regulating them in an environment where the underlying interconnected technology and infrastructures (networks) do not stop at national borders due to their interoperability.¹¹⁴ And still, under current international law the main legal responsibility for implementing responsible business conduct, including the business and human rights agenda, is on states. Therefore, the observation of a conceptual gap which originally triggered the debate on complementing business' influence on international relations and peoples' lives with corresponding responsibilities under international law is again relevant in the digital age¹¹⁵ and also – on a broader scale – at the heart of the discussions on a binding instrument on business and human rights in the UN.¹¹⁶

The OECD Guidelines address this gap in a general manner as they attempt to balance state and business responsibilities in two ways: Similar to the UN Guiding Principles' corporate responsibility to respect human rights, they first contain a set of clear expectations on business to act responsibly. Second, they strengthen the soft character of the non-binding Guidelines with a legally binding obligation for states to establish a grievance mechanism, the National Contact Points. However, they stop somewhere half-way since business is not required to participate in NCP procedures. This is particularly relevant because NCPs could play an important role in addressing negative impacts of business activities in a digital context. Given that the development in this sector is driven by industry, public institutions, including courts and state-based non-judicial remedy mechanisms depend on the private sector's knowledge and information when assessing digital technologies

¹¹⁴ Rikke Frank Jorgensen, 'When Private Actors Govern Human Rights' in: Ben Wagner, Matthias C. Kettemann and Kilian Vieth (eds), *Research Handbook on Human Rights and Digital Technology* (Cheltenham: Edward Elgar 2019), 346-363 (359).

¹¹⁵ Jay Butler, 'The Corporate Keepers of International Law', *AJIL* 114 (2020), 189-220 (207-209).

¹¹⁶ United Nations Human Rights Council, Mandate for an open-ended Intergovernmental Working Group (IGWG) to elaborate an international legally binding instrument on Transnational Corporations and Other Business Enterprises with respect to human rights, 25 June 2014, A/HRC/26/L.22/Rev.1; IGWG, Third revised draft, 17 August 2021.

and their impacts. As the selected examples of NCP cases illustrate, business engagement, both in the dialogue itself as well as in sharing information is a key factor of success. This leads to the interim conclusion that by complementing a soft law instrument with a binding requirement for states to establish an effective grievance mechanism with the National Contact Points and the resulting *sui generis* nature of the Guidelines, they partially bridge the gap between business impacts on the ground and the existing substantive international standards on responsible business conduct. These standards are contained in three aligned international instruments,¹¹⁷ the UN Guiding Principles, the OECD Guidelines, and the ILO Tripartite Declaration.¹¹⁸ However, the OECD Guidelines' approach to complement a soft law instrument with a binding requirement for states to establish an effective National Contact Point without a corresponding duty for business to engage will not succeed in fully accommodating digital developments.

In this regard, a new instrument developed by the Dutch government with the goal to bridge the gap between its own binding obligations under international law and the non-binding nature of international responsible business conduct standards for business is highly interesting. Since 2014 the Dutch government has concluded nine out of 13 planned agreements on responsible business conduct with Dutch industry sectors and civil society organisations.¹¹⁹ The agreements set out how companies can work with civil society organisations and government to prevent abuses in the areas of human rights, labour rights, and the environment and they are equipped with independent monitoring mechanisms. While participating in these agreements is voluntary the government made it clear from the outset that it would consider declaring these agreements binding at a later stage. A recent evaluation of these agreements shows that despite some remarkable successes more action is needed, particularly with regard to monitoring and setting incentives for companies to participate.¹²⁰ In essence, the regulatory agenda needs to be connected with the contractual model more effectively.

¹¹⁷ OECD, ILO and UNOHCHR, *Responsible Business: Key Messages from International Instruments* (Paris, Geneva 2019) <<http://mneguidelines.oecd.org/RBC-Key-Messages-from-International-Organisations-ENG.pdf>>.

¹¹⁸ Above II.1. and II.2.a).

¹¹⁹ Dutch Agreement on Sustainable Garments and Textile; Dutch Banking Sector Agreement; Agreement to Promote Sustainable Forestry; Responsible Gold Agreement; Agreement for the Food Products Sector; Agreement for International Responsible Investment in the Insurance Sector; Agreement for the Pension Funds; RBC TruStone Initiative; RBC Agreement for the Metals Sector <<https://www.government.nl/topics/responsible-business-conduct-rbc>>.

¹²⁰ Verena Bitzer et al., *Evaluation of the Dutch RBC Agreements 2014-2020: Are Voluntary Multi-Stakeholder Approaches to Responsible Business Conduct Effective?* (Amsterdam: KIT Royal Tropical Institute 2020).

2. Responsible Business Conduct by Design – In Regulation and Technology

Collaboration among stakeholders is essential for addressing the responsible business challenges in digital context and it relates to what has been outlined before on interoperability of not only systems and actors but also standards and regulations (above I.1.a)). Noteworthy for the purpose of this article are specific proposals that have recently been launched by business and public authorities to foster collaboration in a regulatory context to address data portability and data sharing (mutualisation).¹²¹

Since NCP procedures are – in contrast to court proceedings – designed as a flexible process to find a solution for specific issues and prevent future harm, they leave room for creative solutions, including cooperative approaches as seen in the Polish case with the company and the submitter working together in the implementation of the agreed measures.¹²² The same is true for the substance of the Guidelines themselves. Given that they call on states to ensure that the instrument remains fit for purpose they underline their character as a living instrument.¹²³

In addition, decisions by National Contact Points do not serve as precedent; it is for the Investment Committee to provide authoritative interpretation of the Guidelines if required.¹²⁴ This leaves room for NCPs in addressing new developments in the digital context. ‘Digitalisation’ does not appear in the Guidelines but as the selected cases illustrate NCPs were able to apply them to new digital phenomena. In practice, NCPs benefit from exchanges with their peers and they are supported by the OECD Secretariat.¹²⁵

With this framework the Guidelines provide a space which in the broader regulatory landscape can serve as a laboratory to explore the impacts of digitalisation on responsible business conduct and identify potential lacunae in existing regulation. This is particularly relevant in the light of the increasing regulatory uptake of the Guidelines and their due diligence concept in

¹²¹ For example Facebook, *Charting a Way Forward on Privacy and Data Portability*, White Paper, September 2019 and Bank of England, *Transforming Data Collection from the UK Financial Sector*, Discussion Paper, January 2020.

¹²² Polish OECD NCP (n. 84), 2-4.

¹²³ OECD Guidelines (n. 38) Chapter I Concepts and Principles, para. 11.

¹²⁴ OECD Guidelines (n. 38), Procedural Guidance to the Council Decision pertaining to NCPs, para. C. 2 c.

¹²⁵ For this purpose, a special seminar was organised in November 2019 to explore the impacts of new technologies on responsible business conduct.

binding national¹²⁶ and regional¹²⁷ legislation. Referring to the Guidelines supports national regulators in addressing the imbalance of state and business responsibilities under international law and at the same time fosters regulatory coherence. In other words, it allows for including a comparatively flexible international instrument in national law.

Since legislation will notoriously lag behind when it comes to capture risks associated with digital developments, integrating responsible business conduct considerations in the technology right from the start, thus '*Responsible business conduct by design*', is essential. This requires engagement with the industry and other stakeholders and calls for new forms of legislation which better accommodate the dynamics of technological development as well as the variety of actors and drivers.

At the national level, so called *regulatory sandboxes* are increasingly being established for this purpose.¹²⁸ They are particularly common in the financial sector to address new developments in Fintech.¹²⁹ At the regional level, in the EU, two proposals which contain regulatory sandboxes are currently on the way: a Regulation on Markets in Crypto-Assets (MiCA) combined with a Pilot Regime for Market Infrastructures based on Distributed Ledger Technology (PDMIR)¹³⁰ and a Regulation on Artificial Intelligence (Artificial Intelligence Act, AIA).¹³¹ Regulatory sandboxes are set up by the legislator or a public regulator and serve as safe spaces for innovative regulation. In the context of responsible business by design, new regulation and new technologies for privacy by design could be tested for a limited time, usually with a clearly defined number of actors and under close regulatory supervision. In

¹²⁶ Above n. 74.

¹²⁷ For example the EU Regulation 2017/821 on Conflict Minerals; EU Regulation 2019/2088 on sustainability-related disclosures in the financial services sector.

¹²⁸ Dirk Zetzsche, Ross P. Buckley, Douglas W. Arner and Janos Nathan Barberis, 'Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation', *Fordham Journal of Corporate and Financial Law* 23 (2017), 31-103.

¹²⁹ The first regulatory sandbox was launched by the UK Financial Conduct Authority (FCA) in November 2015, since then more than 50 countries followed: Giulio Cornelli, Sebastian Doerr, Leonardo Gambacorta and Ouarda Merrouche, *Inside the Regulatory Sandbox: Effects on Fintech Funding*, BIS Working Papers No. 901, November 2020, 2.

¹³⁰ Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final, 24 September 2020; Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology COM(2020) 594 final, 24 September 2020. PDMIR creates a sandbox for private sector participants which will be reviewed after 5 years of its entry into force and complements the review which is scheduled in MiCA to take place 3 years after its entry into force.

¹³¹ Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence ACT) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 21 April 2021.

this scenario, the sandbox would on the one hand benefit participating companies to better understand how to navigate the complexities of regulations with regard to their new technology. On the other, public authorities including regulators can learn about new digital technologies and emerging trends which allow them to better identify potential risks and anticipate future trends.

Stakeholder engagement as a prerequisite for collaboration is a key feature of the Guidelines and reflected in the institutional set-up of the OECD.¹³² Business, trade unions and civil society are institutionally represented with Business at OECD (BIAC), the Trade Union Advisory Committee (TUAC), and OECD Watch. The last revision of the Guidelines in 2011 and the development of the various Guidances on Due Diligence¹³³ which involved all stakeholders illustrate the potential of this institutional framework for tackling also new issues such as digitalisation and the need for RBC by design.

Building on the Guidelines as a comprehensive international standard for responsible business conduct which is supported by all stakeholders and equipped with a grievance mechanism together with the lessons learnt from national approaches in addressing new technologies from a regulatory perspective could result in creating a flexible regulatory space inspired by international law within a stable (national) framework. Such a model would share some characteristics of regulatory sandboxes.¹³⁴

V. Conclusion: A Call for a New Interface

Where does this leave us with regard to the role of international law? The role of business and its responsibilities have been a topic of intense discussions since the 1970s. The UN Guiding Principles on Business and Human Rights and the revised OECD Guidelines for Multinational Enterprises entered new territory in overcoming the traditional dichotomy of binding state obligations on the one and voluntary business engagement on the other hand with their concept of expected business behaviour. While this approach led to successful outcomes in the analogue world its limitations become obvious in a digital context: Industry is the main driver in the development

¹³² Christine Kaufmann, 'From Profit to People and Planet: Rethinking the Purpose of the Corporation' in: Rolf H. Weber, Walter A. Stoffel, Jean-Luc Chenaux and Rolf Sethe (eds), *Aktuelle Herausforderungen des Gesellschafts- und Finanzmarktrechts*, Festschrift für Hans Caspar von der Crone zum 60. Geburtstag (Zürich/Basel/Genf: Schulthess 2017), 3-20 (8-9).

¹³³ See n. 40 and n. 42.

¹³⁴ Zetzsche, Buckley, Arner and Barberis (n. 128), 58-70.

of new technologies which impact on all aspects of life and are developed and adjusted at a speed that states and state regulation can hardly keep up with. The crucial role of industry in new technologies therefore adds another dimension to the existing imbalance between state and business responsibilities. Traditional international law with its focus on the sovereign state and the related sharp divide between binding and non-binding rules is inadequately suited to accommodate this development.

However, international law is in motion: *Hybrid* instruments such as the OECD Guidelines which combine existing concepts and standards of international law with a new notion of business responsibility could be an option to overcome this dilemma. Still, a link is missing to bridge the conceptual gap between states as acknowledged subjects of international law on the one hand and the private sector as the main driver of digital innovation which is currently not included in this equation on the other. In fact, to keep pace with new technological developments and address their impacts, traditional regulatory instruments such as state-based national regulation and international treaties are increasingly being replaced by more flexible policies, principles, or non-binding soft law instruments.¹³⁵ Given their non-binding nature, their effective implementation heavily depends on all actors' commitments. This is also true for the OECD Guidelines, but in contrast to other soft law instrument, the OECD's approach to add some teeth to the Guidelines with a binding requirement on states to establish a grievance mechanism seems to be a step in the right direction. Still, this obligation only applies to states, not to companies. The result is a somewhat imbalanced system which calls for leveling the playing field regarding corresponding business responsibilities.

We therefore need a *new interface* for better linking new concepts of responsible business conduct in a digital world with international law and accommodate the intrinsic dynamics of digital developments. Such a regulatory interface will have to be conceptualised outside traditional categories of binding and non-binding international law. Inspiration could be drawn from the regulatory uptake of the Guidelines at the national level and innovative regulatory instruments such as the Agreements on International Responsible Business Conduct which the Netherlands introduced in the form of contractual agreements between the government, business, trade unions, and civil society¹³⁶. Experiences with regulatory sandboxes at the national level and

¹³⁵ Shin-yi Peng, 'The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?', *Journal of International Economic Law* 22 (2019), 1-27 (4-9); Christine Kaufmann, 'Rechtsstaatlichkeit und Internationalisierung' in: Oliver Diggelmann, Maya Hertig Randall and Benjamin Schindler (eds), *Verfassungsrecht der Schweiz* (Zürich: Schulthess 2020) Vol. 2, IV.3, n. 16-20.

¹³⁶ See n. 119.

new approaches in the European Union can serve as a further source of inspiration. Framing such an interface as a new type of international regulatory sandbox would allow for evaluating the results and move towards smart regulation over time.¹³⁷

Such an interface at the international level could include three elements: First, a binding international framework which – other than the currently discussed legal instrument on business and human rights¹³⁸ – would not focus on detailed provisions of conduct but outline the general principles of government obligations regarding RBC in the digital age. Second, a model contract for a binding agreement to be concluded at the national level by governments, business and civil society organisations which could draw from the experience with the Dutch Agreements¹³⁹ and include the internationally agreed responsible business conduct standards of the OECD Guidelines as a reference. Third, non-binding industry and multistakeholder initiatives could complement this regulatory package.

In sum, such an interface would apply a *translational* approach¹⁴⁰ which draws on the advantages of hybrid regulatory models¹⁴¹ and combine a binding regulatory framework at the national and international level with contractual elements as well as non-binding instruments anchored in them. Creating this interface as a safe space in terms of an *international regulatory sandbox* would allow all actors to test new regulatory approaches and learn along the way towards smart regulation. It may be a promising step for international law to stay fit for purpose in an era of digitalisation and ensure that its algorithms keep pace with new and emerging technologies.

¹³⁷ Zetzsche, Buckley, Arner and Barberis (n. 128), 58-70.

¹³⁸ See n. 116.

¹³⁹ See n. 119.

¹⁴⁰ Christine Kaufmann, 'The Covenants and Financial Crises' in: Daniel Moeckli, Helen Keller and Corina Heri (eds), *The Human Rights Covenants at 50: Their Past, Present and Future* (Oxford: Oxford University Press 2018), 302-333 (329-333).

¹⁴¹ A similar approach with regard to a future Treaty on Business and Human Rights is proposed by Anne Peters, Sabine Gless, Chris Thomale and Marc-Philippe Weller, 'Business and Human Rights: Making the Legally Binding Instrument Work in Public, Private and Criminal Law', Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2020-06, 37.

Cyberspace as an Example of Self-Organisation from a Network Perspective

Cäcilia Maria Hermes*
Berlin, Germany
cc.hermes@googlemail.com

Abstract	817
Keywords	818
I. Introduction	818
II. Regulation of Cyberspace	820
1. IETF	820
a) IETF's Structure and Working Procedure	820
b) IETF's Networked Standard Setting	821
2. ICANN	822
a) ICANN's Evolution	822
b) ICANN's Structure and Working Procedure	823
(i) Stakeholder Structure	823
(ii) Individual Internet Users	824
(iii) Governments	825
c) Touchstone: The .xxx-Case	825
d) Hybrid Regulation of a Global Resource	826
3. IGF	827
a) Evolution of the IGF	827
b) Structure and Processes, Criticism and Reform	827
c) Towards Comprehensive Cyberspace Regulation?	829
4. Interim Conclusion	829
III. Networks as Regularity in Irregularity	830
1. Network Perspective	830
a) Early Reception of Networks in International Relations	831
b) Reception of Networks in International Law Scholarship	832
2. Cyberspace Governance Through the Lens of Network Perspective	834
a) IETF, ICANN and IGF as Non-State Networks	834
b) The Legitimacy of Networks and Their Decisions	834
c) Feeding and Exploiting of the Knowledge Pool	835
d) Networks' Law and Legal Quality	837
3. Order and Legitimacy Through Networks	838
IV. Concluding Remarks	838

Abstract

The present contribution defends network theory empirically by considering the governance of cyberspace. It aims to normatively explain the largely

* Ph.D. student at the Institute of International Law at the University of Giessen, researching on the emergence of norms in cyberspace.

non-state regulation of cyberspace with the help of network theory. To this end, it first introduces key conglomerates of cyberspace governance and analyses their structures and processes. The empirical analysis of the organisational structures forms the basis for the concluding theoretical evaluation. The contribution can serve as an impulse for further research on global governance in a departure from state-centred perceptions.

Keywords

network theory – cyberspace governance – norm development

I. Introduction

It is particularly in the context of cyberspace governance that decisions – affecting citizens' daily lives worldwide and directly – are made without being preceded by political will-building processes. The question therefore arises whether and how these decisions are legitimised.

Cyberspace is a global electronic communication system that allows both computers and their users to network in order to exchange information. Thus, cyberspace embraces two dimensions: on the one hand, it contains a technical infrastructure that enables electronic communication between computerised devices,¹ but on the other hand, it also contains the social aspect of its use by different actors.² A number of diverse participants are involved in the regulation of Cyberspace: Companies that provide tools for its infrastructure, user devices and applications, institutions that guarantee the interoperability of networks and devices by either developing Internet protocols and standards³ or by managing the Internet's address system,⁴ and governments that have an interest in ensuring that their normative decisions are not undermined in Cyberspace, to name only a few. All these actors pursuing their own interests make their respective decisions of either technical or political nature. Yet, their ways of decision-

¹ David J. Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (London: Routledge 2011), 13; Elisabeth Longworth, 'The Possibilities for a Legal Framework for Cyberspace – Including a New Zealand Perspective' in: Bruno de Padirac (ed.), *The International Dimensions of Cyberspace Law* (London: Routledge 2019), 4.

² David Goe, Michael S. Goodman and Alicia Wanless, 'Rebalancing Cybersecurity Imperatives: Patching the Social Layer', *Journal of Cyber Policy* 4 (2019), 117-137.

³ The Internet Engineering Task Force, see below II.1.

⁴ Internet Corporation for Assigned Names and Numbers, ICAAN, see II.2.

making differ significantly depending on the goals pursued: In the political sphere, the struggle for the right implementation of morals and values is in the foreground,⁵ while actors with a technical orientation collaborate in their focus on improving the infrastructure's efficiency and on practical questions of a coherent administration. In doing so, they all follow their own distinctive agendas. However, these decisions with their different aims and directions are in principle accepted by those affected by them – the users of cyberspace. In other words: Globally binding decisions made by state and non-state actors are *de facto* accepted, although there is no institutionalisation in sight: neither exist comprehensive treaties under international law nor a superordinate organisation dealing with the regulation of cyberspace. Therefore, legal theory is faced with a dilemma: Are these decisions legitimised? And if so, how?

Network theory can help to bring light into the darkness. It attempts to adapt legal theory to the development of an increasingly networked society by turning away from the classical understanding of (international) law theory, according to which it is primarily the formation of political will within states that has a legitimising effect on regulatory activity. Instead, it states that non-state actors, too, follow their own normative order and derive the legitimacy for their decisions from their own specific sources. In this way, network theory is able to link the seeming disorder of global regulatory efforts in general, and those in Cyberspace in particular, back to legal theory.

The present contribution looks at the activities of different non-state actors of cyberspace governance through the lens of network theory and examines if and how their decisions are legitimised. To this end, the first block (II.) analyses three particularly relevant actors involved in the governance of Cyberspace. Their mandates, structures, and the processes preceding their decisions are described in detail. The second part (III.) then uses network theory to examine if and how the entities' structures and processes affect the decisions' quality and legitimacy. To this end, network theory is first introduced (III.1.) and then carefully placed in relation to the previously analysed actors (III.2.). In this way, on the one hand, the statements of network theory are illustrated, and on the other hand, the legitimisation paths of non-state actors' decisions in Cyberspace become comprehensible. The last part (IV.) summarises the findings of the study.

⁵ See only Alex Grigsby, 'The End of Cyber Norms', *Global Politics and Strategy* 59 (2017), 109-122.

II. Regulation of Cyberspace

The selected institutions deal with the regulation of essential components of cyberspace. At the same time, their emergence follows chronologically the evolution of cyberspace development: Starting with the Internet Engineering Task Force (IETF), originator of Cyberspace' purely technical regime, followed by the Internet Corporation for Assigned Names and Numbers (ICANN) at the interface between the Internet's technical infrastructure and its increasing use by the general public and, last, the Internet Governance Forum (IGF), which provides a broad platform for exchange on technical as well as political issues of Cyberspace.

1. IETF

The IETF develops standards and protocols that ensure that any software can be used smoothly on any hardware, thus guaranteeing the Internet's interoperability.⁶ As the first and to date the most important standardisation organisation on the Internet, it is the crucial entity for the technical development of the Internet and the constant improvement of its functioning.⁷ The IETF is not of state origin: instead, it is a large and open community of network architects, Internet operators, users and scientists, all distinguished by technical excellence, working in an anarchic organisational structure.⁸ The standards and protocols developed by the IETF have *de facto* validity on a global scale through their acceptance by developers of both software and hardware.

a) IETF's Structure and Working Procedure

In terms of work processes, the IETF places particular emphasis on ensuring that the standards and protocols it develops are the result of consensus among its members rather than of democratic processes.⁹ The nature of this *consensus* is further defined in the most important rule that IETF has given itself: 'IETF consensus does not require that all participants agree although

⁶ Matthias C. Kettmann, *The Normative Order of the Internet* (Oxford: Oxford Scholarship Online 2020), 31-32.

⁷ About the IETF <<https://www.ietf.org>>.

⁸ See the IETF Mission Statement, RFC 3935, <<https://tools.ietf.org>>.

⁹ See the IETF's motto: 'We reject: kings, presidents, and voting. We believe in: rough consensus and running code.', IETF, RFC 7282, <<https://tools.ietf.org>>.

this is, of course, preferred. In general, the dominant view of the working group shall prevail. (However, it must be noted that “dominance” is not to be determined on the basis of volume or persistence, but rather a more general sense of agreement.) Consensus can be determined by balloting, humming, or any other means on which the Working Group agrees (by rough consensus, of course).¹⁰ With regard to the structure of the IETF, the most striking characteristic is its openness to all persons interested. Standards and protocols are set in an open and transparent process in which all members can participate.¹¹

The IETF splits its activities into thematic *Areas*, each of which consists of several *Working Groups* related to the focus of that Area; each Area is headed by an *Area Director* (AD), who is nominated for a two-year term by the Nominating Committee (NomCom),¹² which chairs the IETF.¹³ Together with the Chair of the IETF, the ADs form the Internet Engineering Steering Group (IESG).¹⁴

The IETF’s decisions are found in a dialogical, recursive process. When creating standards, the working groups publish their results as Requests for Comments (RFC). By doing so, the drafts enter into the approval process.¹⁵ As soon as the IESG approves an RFC, the standard becomes a *Proposed Standard*. It remains in this status for a period of six months during which it is discussed by all of the IETF-community. In case it is promoted to a *Draft Standard*, it enters into an implementation and test phase after which it can finally become an *Internet Standard*.

b) IETF’s Networked Standard Setting

Since its foundation, the IETF follows the dogma of effectiveness and functionality. It aims at technical excellence, at being always up-to-date, and it realises a high degree of transparency by documenting every single development step of any protocol or standard. The open structure of the IETF and the fact that anyone interested can participate in the development of standards and protocols has the effect that all knowledge available among

¹⁰ IETF, RFC 7282, <<https://tools.ietf.org>>.

¹¹ IETF, RFC 3935 <<https://tools.ietf.org>>.

¹² The NomCom is composed of a random selection of IETF volunteers, <<https://www.ietf.org>>.

¹³ IETF, RFC 8318, <<https://tools.ietf.org>>.

¹⁴ The IESG is responsible for the overall operation of the IETF; IETF, RFC 5742, <<https://tools.ietf.org>>.

¹⁵ A description of the several steps can be found in RFC 2026, <<https://tools.ietf.org>>.

individual actors is collected and made accessible via the RFCs, which circulate permanently among all members. The subsequent test phases assure that only those proposals that best solve the respective problem prevail. Therefore, the IETF's openness and its recursive processes assure that the maximum knowledge can be first collected and then channelled to be summarised in a decision.

2. ICANN

ICANN is a not-for-profit corporation, responsible for coordinating, administrating, and allocating the management of unique names and addresses on the Internet, known as domain names (e. g.: www.example.com). It also coordinates the operation and development of the root server system¹⁶ and organises the development of policies on Domain Name System (DNS)¹⁷ management issues.¹⁸ Thus, the technical management of a global key resource of the Internet lays in the hands of a non-governmental, decentralised entity that is neither a product of an international treaty nor an international organisation.¹⁹ Instead, representatives of various sectors – civil society, business, and governments – cooperate to produce decisions, which have an immediate effect on Cyberspace, and are accepted by the entire Internet community.

a) ICANN's Evolution

The DNS was developed by scientist and Internet pioneer Jon Postel who managed it with the Internet Assigned Numbers Authority (IANA) under the responsibility of the Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defence.²⁰ With the massive increase in Internet use also beyond the research community in the 1990 s, and simultaneously growing commercial interests in the use of rele-

¹⁶ Thirteen root servers exist worldwide: ICANN Office of the Chief Technology Officer, Brief Overview of the Root Server System, 6 May 2020, 4.

¹⁷ The DNS translates the names of websites into binary addresses that the computer can read, and back again, e. g.: www.example.com = IPv4-Adresse: 93.184.216.34.

¹⁸ See Art. 1. 1 (a) (i) ICANN Bylaws. The Bylaws have undergone several updates. The rules quoted here are dated 28 November 2019, <<https://www.icann.org>>.

¹⁹ Kettemann (n. 6), 106.

²⁰ Memorandum of Understanding on the Generic Top Level Domain Space of the Internet Domain Name System, (gTLD-MoU), <<https://web.archive.org>>.

vant domain names, a more comprehensive management system became necessary. In 1998, the US-Government proposed the privatisation of DNS management in order to open up the Internet to a wider international scope and to strengthen it as a medium for communication and competition.²¹ The same year, ICANN was handed over to the international community,²² and established as a private non-profit entity under the Law of California – ‘a non-governmental organisation with significant responsibilities for administering what is becoming a global resource’.²³ Since then, ICANN operates the IANA functions²⁴ as the crucial entity at the interface between the technical network of Cyberspace and its use by the general public.

b) ICANN’s Structure and Working Procedure

The rules and procedures of ICANN are set out in the Articles of Incorporation²⁵ and the Bylaws.²⁶ ICANN organises ‘the development and implementation of policies [...] through a bottom-up consensus-based multistakeholder process’.²⁷ Following this mandate, ICANN’s structure is kept as open as possible to give those actors interested the possibility to participate. It is guided by IETF methods: when seeking decisions, general consensus should be realised wherever possible.²⁸ Therefore, ICANN’s operations are characterised by decentralised governance in which stakeholders from different sectors – individuals, industry, organisations with non-commercial interests, and governments – interact on an equal footing.²⁹

(i) Stakeholder Structure

ICANN is headed by a Board of Directors composed of 21 members, representing three Supporting Organisations (sub-groups focusing on specific sections of ICANN’s responsibilities), independent representatives of the general public interest, and finally the President and Chief Executive

²¹ National Telecommunications and Information Administration, Statement of Policy on the Management of Internet Names and Addresses, 5 June 1998.

²² Letter from Lawrence Strickling, NTIA, to Steve Crocker, regarding the Affirmation of Commitments, 6 January 2017, <<https://www.icann.org>>.

²³ Jon Postel, Letter to William Daley, Secretary of Commerce, 2 October 1998, <<https://www.ntia.doc.gov>>.

²⁴ IANA, Introduction, <<https://www.iana.org>>.

²⁵ <www.icann.org>.

²⁶ <www.icann.org>.

²⁷ Art. 1. 1 ICANN Bylaws.

²⁸ ICANN Participation Booklet, <<http://archive.icann.org>>, 8.

²⁹ ICANN, <www.icann.org>.

Officer (CEO), appointed by the rest of the Board. In addition, ICANN can rely on several Advisory Committees, which make recommendations to the Board on matters that are within their respective areas of responsibility.³⁰ The general public is involved especially via the Generic Names Supporting Organization (GNSO), which plays an important role among the supporting organisations.³¹ It is the responsibility of the GNSO council³² to develop and recommend to the ICANN board substantive policies regarding the generic Top Level Domains (gTLD)³³ based on the input from four stakeholder groups,³⁴ which reflect the great diversity of groups and individuals that make up the ICANN community, and from the ‘constituencies’³⁵ which each represent groups of Internet users sharing specific interests.

(ii) Individual Internet Users

To give individual Internet users a channel to advise on ICANN activities ‘insofar as they relate to the interests of individual Internet users’,³⁶ the At-Large Advisory Committee (ALAC) was created in 2002 to be the ‘primary organisational home within ICANN for individual Internet users’.³⁷ Again, a bottom-up mechanism ensures that all voices of individuals find their way up to the ALAC: any group in which individual users come together to share and discuss their views on ICANN issues can be registered as an At-Large Structure (ALS).³⁸ These ALSes can take part in discussions hosted by the Regional At-Large Organizations (RALOs),³⁹ which nominate two members of the ALAC each.

³⁰ Art. 12 ICANN Bylaws.

³¹ The two other Supporting Organisations are the Address Supporting Organization (ASO), working on issues regarding the IP address allocation, and the country code Name Supporting Organization (ccNSO), developing country code policies.

³² On the structure of GNSO, see <<https://gnso.icann.org>>.

³³ Cross-border domains such as .com.

³⁴ The Commercial Stakeholder Group, Non-Commercial Stakeholder Group, Registrars – selling domains – Stakeholder Group and Registries – maintaining TLDs – Stakeholder Group, <<https://gnso.icann.org>>.

³⁵ Technical term for internet users who group themselves according to certain topics or interests (within the Commercial Stakeholder Group, for example: the constituency of Commercial Business Users, Internet Service Providers or Intellectual Property).

³⁶ Art. 12. 2. (d) (i) ICANN Bylaws.

³⁷ Art. 12. 2. (d) (i) ICANN Bylaws.

³⁸ <<https://atlarge.icann.org>>; e.g.: Computer User Organization, Internet civil society groups, consumer advocacy groups etc.

³⁹ African (AFRALO), Asian, Australian and Pacific Islands (APRALO), European (EURALO), Latin American and Caribbean Islands (LACRALO) and North American (NARALO), see <<https://atlarge.icann.org/>>.

(iii) Governments

National Governments are represented in the Governments Advisory Committee (GAC),⁴⁰ which advises ICANN on ‘activities as they relate to concerns of governments’.⁴¹ With regard to governments, the core values state that, although ICANN remains grounded in the private sector, it recognises the governments’ and public authorities’ responsibility for public policy.⁴² ICANN therefore commits to ‘duly taking into account the public policy advice of governments and public authorities’.⁴³ While the GAC has no direct control over ICANN, the Board must take particular account of the advice of the GAC and, for example, give specific reasons for any action that deviates from the GAC’s vote or find mutually acceptable solutions in a special procedure.⁴⁴ In addition, Article 12.2 (a) (xi) of ICANN’s Bylaws gives the GAC a genuine veto right.

c) Touchstone: The .xxx-Case⁴⁵

The fact that the possibilities of governments to influence ICANN are nevertheless precisely defined and limited became clear with the .xxx-case, when governments attempted to disrupt the balanced stakeholder relationship within ICANN. Following the GNSO’s recommendation to introduce a limited number of new gTLDs, the ICANN Board launched the bidding process for the allocation of new gTLDs. The company *ICM Registry* responded by bidding for a gTLD named .xxx, which was specifically intended for ‘adult-only’ content. Already in 2000, ICANN had stated in response to moral concerns expressed by the GAC to recommend against the gTLD’s selection ‘because of the controversy surrounding [...] .xxx’.⁴⁶ After ICANN agreed in principle to ICM Registry’s application in the following procedure in 2005, and started contract negotiations,⁴⁷ the process was initially suspended in 2006⁴⁸ following pressure from certain

⁴⁰ Art. 12. 2 (a) ICANN Bylaws.

⁴¹ Art. 12. 2 (a) (i) ICANN Bylaws.

⁴² Art. 1. 2 (b) (vi) ICANN Bylaws.

⁴³ Art. 1. 2 (b) (vi) ICANN Bylaws.

⁴⁴ Art. 12. 2 (a) (x) ICANN Bylaws.

⁴⁵ See the in-depth analysis by The Berkman Center for Internet & Society at Harvard University, *Accountability and Transparency at ICANN – An Independent Review*, 20 October 2010, Appendix D: The .xxx Domain Case and ICANN Decision-Making Processes.

⁴⁶ ICANN, Report on TLD Applications of the August 15 Criteria to Each Category or Group, 9 November 2000, <<https://archive.icann.org>>.

⁴⁷ ICANN, A Special Meeting of the Board, 1 June 2005, <<https://www.icann.org>>.

⁴⁸ The Berkman Center (n. 45), 23.

governments.⁴⁹ However, after talks resumed in 2007, ICM's application was ultimately rejected on the grounds that it did not meet formal criteria.⁵⁰ It was only in 2010 after several proceedings, that an Independent Review Panel (IRP), one of three mechanisms purposed for the review of ICANN board activities and decisions,⁵¹ decided that ICANN had made a legal error by listening to moral arguments, since it was only called upon to decide technical issues.⁵² The IRP also criticised the particular influence of the US, which wanted to impose its own ideas on morality (pornography respectively) in the online environment. As a result, the panel recommended ICANN to stay within its mandate and to act neutrally and 'consistently with relevant principles of international law',⁵³ to which ICANN has committed itself in Art. 4 of the Articles of Incorporation.

d) Hybrid Regulation of a Global Resource

Similar to the IETF, ICANN's open and accessible structure ensures that all interested stakeholders can voice their interests within the DNS governance process. The rule is that the interests of all stakeholders are considered equally. This means that all interests are first collected and taken into account as far as necessary. However, because DNS governance is more complex in that it is not only about technical but also non-technical issues, ICANN's structure is split into many subgroups and therefore more complex than the IETF's structure. Although individual stakeholders, such as the governments, are formally given special recognition, it is nevertheless ensured that they do not negatively influence ICANN's core tasks. However, the .xxx-case showed that it was necessary to activate an independent institution to guard the organisation's rules and the fulfilment of its mandate.⁵⁴

⁴⁹ The USA and the US Department of Commerce were the main advocates, ICDR Case No. 50 117 T 00224 08, Declaration of the Independent Review Panel, 19 February 2010, 17-19.

⁵⁰ ICANN, Meeting of the ICANN Board, Lisbon, 28 March 2007, <<https://www.icann.org>>.

⁵¹ Art. 4. 2. ICANN Bylaws; an IRP is an arbitration tribunal. It is created any time there is an allegation against the Board and the appellant petitions for an independent review.

⁵² International Centre for Dispute Resolution, *ICM Registry, LLC v. ICANN*, ICDR Case No. 50 117 T 00224 08, Independent Review Panel Declaration (2010).

⁵³ *ICM Registry, LLC v. ICANN*, No. 140, 152.

⁵⁴ The Uniform Domain Name Dispute Resolution Policy (UDRP) is another popular example to illustrate the emergence of a regime within ICANN that is independent of national and international law. See David Lindsay, *International Domain Name Law: ICANN and the UDRP* (Oxford: Hart Publishing 2007), 95-96 and Jochen von Bernstorff, 'The Structural Limitations of Network Governance: ICANN as a Case in Point' in: Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *Transnational Governance and Constitutionalism* (London: Hart Publishing 2004), 252-287 (270).

3. IGF

The Internet Governance Forum is an open discussion platform on central legal, political, social, and technical issues of the Internet. The IGF's mission is to develop ideas about the future shape of cyberspace. It therefore has a very broad approach to Cyberspace governance. All interested parties, especially non-state actors, can participate in the IGF's activities. However, the IGF has no decision-making power and (to date) merely serves as an opportunity for a broad exchange of ideas on Cyberspace governance.

a) Evolution of the IGF

The IGF was established in 2003/05 in the context of the World Summit on the Information Society (WSIS). The WSIS was organised by the International Telecommunications Unit (ITU) in implementation of UN General Assembly Resolution 56/183⁵⁵ and took place in two phases, in Geneva in 2003 and in Tunis in 2005. The reason for the IGF's creation was that Internet governance issues were increasingly being discussed at international level, but no agreement was reached on the concrete future shape of Internet governance within the WSIS or elsewhere. The only agreement that could be reached in the end was that not only governments and institutions close to them, but also other sectors should be involved not only in the implementation of rules for Cyberspace but also in their creation. Accordingly, the Tunis Agenda as the final document of the WSIS formulates the conviction of the international community: '[...] The international management of the Internet should be multi-lateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organisations.'⁵⁶

b) Structure and Processes, Criticism and Reform

The Tunis Agenda did not define the organisation of the IGF in detail, it only contains basic guidelines for the structure of the processes within the IGF: The IGF should work multilaterally, democratically, and transparently, following the multi-stakeholder model,⁵⁷ while complementary stakeholders

⁵⁵ UNGA Res 56/183 of 31 January 2002, A/RES/56/183, para. 1.

⁵⁶ WSIS, Tunis Agenda for the Information Society of 18 November 2005, WSIS-05/TUNIS/DOC/6(Rev.1)-E (in the following short: The Tunis Agenda), para. 29.

⁵⁷ The Tunis Agenda, para. 29.

should be taken into account.⁵⁸ Following his mandate, the UN Secretary-General established an office in Geneva in 2006 to support the IGF. He also created the Multistakeholder Advisory Group (MAG)⁵⁹ to advise him during the annual IGF meetings. Many different activities also take place between the meetings, such as platforms for discussions on policy issues related to the Internet or Dynamic Coalitions.⁶⁰ In addition, there are annual regional IGFs, which have no decision-making powers and are open to all interested parties acting formally on an equal footing.⁶¹

The IGF was conceived purely as a platform for discussion, in particular to prevent it – endowed with any form of decision-making power – from becoming a battleground for national governments with their differing views on Cyberspace.⁶² Accordingly, the individual sessions should produce neither decisions nor resolutions or norms,⁶³ but instead recommendations. It was hoped that neutral discussions, in which all different opinions would be heard, would lead to good compromises based on facts, practicability and efficiency rather than on ideological differences or national power politics.⁶⁴ This meant a conscious shift away from purely political will building and decision making. In addition, the Internet community, too, found it difficult to give the IGF decision-making power, to define its mandate too broadly or to set stricter standards for its processes; The IGF thus provides for a comprehensive exchange of ideas on a regular basis, keeping issues on the agenda for a long term.⁶⁵

In the past few years, reform efforts have taken place to increase the IGF's influence. The major and much criticised disadvantage can be found in the fact that resulting ideas are not transferred or implemented into practical negotiations.⁶⁶ For this reason, the UN initiated a global consultation process on the future architecture of Internet governance as part of its strategy to increase the effectiveness of cooperation in the field of communications and the Internet.⁶⁷ These consultations resulted in an *Options Paper*, which brings

⁵⁸ The Tunis Agenda, para. 73.

⁵⁹ <<https://www.intgovforum.org>>; The MAG has 55 members representing governments, the private sector and civil society, including representatives from the academic and technical sectors.

⁶⁰ Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum* (Perth: Terminus Press 2004), 379-380; See the list at <<https://www.intgovforum.org>>.

⁶¹ See <<https://www.intgovforum.org>>.

⁶² Malcolm (n. 60), 466.

⁶³ <<http://www.intgovforum.org>>.

⁶⁴ Malcolm (n. 60), 356.

⁶⁵ Kettemann (n. 6), 114.

⁶⁶ Daniel Voelsen, 'Das Internet Governance Forum auf dem Prüfstand', SWP-Aktuell 59 (November 2019), <<https://www.swp-berlin.org/10.18449/2019A59/>>.

⁶⁷ The UN Secretary General's High-level Panel on Digital Cooperation (HLPDC), The Age of Digital Interdependence, June 2019, 30, <<https://www.un.org>>.

together the views of various stakeholders – the private sector, governments, civil society, technology, and science. It concludes that the IGF with its existing structures should be retained as the central platform for discussion, but should be significantly strengthened and made more effective.⁶⁸ By transforming it into an Internet Governance Forum Plus (IGF+), more access and better coordination of all stakeholders should be promoted through financial support and a central information point. Furthermore, the IGF+ results are to be recorded in more action-oriented recommendations or reports so that they can be incorporated into political decision-making processes (still without the IGF becoming a treaty-making forum).⁶⁹ The so-called Digital Commons Architecture (DCA)⁷⁰ and the Distributed Co-Governance Architecture (CoGov) were discussed as alternative models,⁷¹ and elements of both models will be adopted in the IGF+.⁷²

c) Towards Comprehensive Cyberspace Regulation?

The IGF was founded with the aim of coming closer to a comprehensive cyberspace governance. The open structure and the conception as a pure discussion platform are supposed to contribute to the gathering of as many ideas and conceptions on Cyberspace governance as possible, and to the alignment of expectations via dialogue. The IGF is thus designed for consolidation, but without being able or wanting to bring about decisions. Interestingly, however, it is precisely this characteristic, that is likely to prevent individual actors such as governments from becoming too strong.

4. Interim Conclusion

When looking at IETF, ICANN and IGF, we see a multitude of different actors coming together in different entities, in order to govern

⁶⁸ UN HLPDC, Recommendation 5A/B, Options for the Future of Global Digital Cooperation, 2.

⁶⁹ UN HLPDC (n. 68), 8.

⁷⁰ The DCA places special emphasis on the use of technology to achieve the Sustainable Development Goals. Based on the 'Global Commons' in environmental law, it would focus on questions of accountability and trustworthiness.

⁷¹ The latter is essentially based on the self-forming network approach of ICANN and IETF and was intended to consist of various networks: 'Digital Cooperation Networks' should temporarily link various working groups on specific topics horizontally with each other; 'Network Support Platforms' would support the Digital Cooperation Networks; a 'Network of Networks' would perform coordination functions.

⁷² UN HLPDC (n. 68), 4.

certain areas of Cyberspace. Hardly any instructions *from the outside* or *from above* are received or implemented in the processes of IETF, ICANN, or IGF; rather, governance *emerges* in the course of discursive processes, and is consolidated in decisions. However, these collections of actors and processes seem to fulfil their respective governance tasks efficiently, since the results are accepted and implemented worldwide. Since all three institutions are non-governmental, their decisions are not tied back to states; also, there is no overarching set of norms to guide the actors. Ways of legitimisation linked to states is therefore excluded. However, this does not necessarily mean that all the regulatory activities described are illegitimate. Rather, it is precisely the possibilities of legitimisation beyond the state that must be sought.

III. Networks as Regularity in Irregularity

One theory that presents a concept of international order by putting a special focus on transnational constellations is network theory. In the following, this theory will be briefly presented. It will be both illustrated and tested on the basis of the observations made on Cyberspace governance. Ultimately, an attempt is made to answer the question of where the order of Cyberspace governance derives its legitimacy from.

1. Network Perspective

To comprehend network theory, it is helpful to start with the very simple picture of a network and its properties: If one visualises a network, one thinks of a construct consisting of individual nodes, of the connections running between the nodes and of how the tension between the nodes hinders them to leave their place, ensuring that they cannot be arranged hierarchically but stay in a stable and heterarchic relationship to each other. The type and number of nodes and connections define the network's size and character, but are not necessarily predetermined. This idea of the network, initially established as a metaphor, has increasingly been elaborated as a fixed concept in various disciplines. The reception of network theory in international law scholarship has essentially taken place via governance research,⁷³ an academic discipline in natural proximity to international law scholarship.

⁷³ Michael M. Atkinson and William D. Coleman, 'Policy Networks, Policy Communities and the Problems of Governance', *Governance* 5 (1992), 154-180.

In order to be able to grasp the significance of network theory for international law, the entry point here, too, is chosen via the insights of international relations.

a) Early Reception of Networks in International Relations

Already at an early stage, network theory was taken up in the discipline of International Relations in order to explain an increasingly empirical recognisable 'global governance'.⁷⁴ Transgovernmentalism⁷⁵ in particular uses the concept of a network to explain political and international issues, since the Westphalian model, according to which states only interact at government level, was not sufficient to explain the phenomena of globalisation. Keohane and Nye, for example, pointed out that the governmental level of interaction only represents one single segment of state interaction. According to them, interstate interaction is much more comprehensive and also takes place beyond the government level.⁷⁶ They also noted an increasingly slow response capacity of individual governments to global problems and coined in this context the term 'ineffectiveness challenge'.⁷⁷ These considerations were further specified by Slaughter. Slaughter considers the state to be a collection of private and public institutions such as banks, courts, or governments,⁷⁸ having equivalents in other states. Like nodes of a network, these institutions are capable of making contact and exchange information with their counterparts abroad⁷⁹ in order to jointly and coherently regulate matters under their responsibility.⁸⁰ This process is driven by the communications revolution⁸¹ and results in an increasingly dense network of the international community: one of public authorities at different levels of state hierarchy on the one

⁷⁴ James N. Rosenau, 'Governance, Order and Change in World Politics' in: James N. Rosenau and Ernst Otto Czempiel (eds), *Governance without Government: Order and Change in World Politics* (Cambridge: Cambridge University Press 1992), 1-29 (1-3).

⁷⁵ See for example Anne-Marie Slaughter, 'Government Networks: The Heart of the Liberal Democratic Order' in: Gregory H. Fox and Brad R. Roth (eds), *Democratic Governance and International Law* (Cambridge: Cambridge University Press 2000), 199-235 (201).

⁷⁶ Joseph S. Nye Jr. and Robert O. Keohane, 'Transnational Relations and World Politics: An Introduction', *International Organization* 25 (1971), 329-349.

⁷⁷ Robert O. Keohane, 'Governance in a Partially Globalized World', *Am. Polit. Sci. Rev.* 95 (2001), 1-13.

⁷⁸ Anne-Marie Slaughter, 'Global Government Networks, Global Information Agencies, and Disaggregated Democracy', *Mich. J. Int'l L.* 24 (2003), 1041-1071.

⁷⁹ von Bernstorff (n. 54), 261.

⁸⁰ See comprehensively Anne-Marie Slaughter, *A New World Order* (Princeton and Oxford: Princeton University Press 2004), 261-271.

⁸¹ Slaughter (n. 75), 200.

hand,⁸² and one of non-state actors on the other.⁸³ Slaughter summarises her observations with the concept of the ‘disaggregated state’,⁸⁴ in which the state does not dissolve, but where it also no longer exclusively follows a hierarchical order. As a result, very different, relatively formal networks with global reach exercise the governance of functionally different areas, such as bank regulation and environmental protection.⁸⁵ Slaughter believes that these kinds of networks could take over the functions of a world government without needing to establish a hierarchy.⁸⁶ She thus departs from a strict distinction between domestic and foreign policy and instead calls for the use of transnational network structures to cope with global challenges, since these can hardly be mastered by the states alone.⁸⁷

b) Reception of Networks in International Law Scholarship

Novel governance phenomena in the form of horizontal, transnational cooperation were initially clearly perceived in environmental law and international financial law. The increasing importance of non-state actors on the one hand and tendencies deviating from state sovereignty in connection with globalisation on the other could not be ignored for a long time in international law studies. However, a normative framework to capture these observations has long been lacking. Especially the classification of rules produced by non-state entities, questions about their normative quality and legitimacy posed a challenge to classical theories of law, which were characterised by an understanding of norm hierarchy, and based on the premise that norms are firstly legitimised by a will organised in the nation states. Connected to the latter premise is the notion of states as the only legitimate actors in international relations,⁸⁸ and a shift away from this idea meant a radical rethinking of a fundamental premise of international law theories. Aimed at filling the

⁸² Slaughter (n. 75), 201.

⁸³ Jan Hauke Pläßmann, ‘Selbstermächtigung exekutiver Akteure: Demokratische Defizite und konzeptionelle Herausforderungen zwischenstaatlicher Netzwerke’ in: Jonathan Bauerschmidt, Bardo Fassbender, Michael Wolfgang Müller and Angelika Siehr (eds), *Konstitutionalisierung in Zeiten globaler Krisen* (Berlin: Nomos 2015), 71-104 (74).

⁸⁴ Slaughter (n. 80), 12; Slaughter (n. 75), 201; resp. with a focus on state sovereignty: Anne-Marie Slaughter, ‘Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks’, *Government and Opposition* 39 (2004), 159-190.

⁸⁵ Slaughter (n. 80), 2-3, 52-55; Slaughter (n. 75), 200, 214-216.

⁸⁶ Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World* (New Haven and London: Yale University Press 2017), 202-206.

⁸⁷ Slaughter (n. 75), 203, 234-235; Pläßmann (n. 83), 74-76.

⁸⁸ Karl-Heinz Ladeur, ‘Ein Recht der Netzwerke für die Weltgesellschaft oder Konstitutionalisierung der Völkergemeinschaft?’, *AVR* 49 (2011), 246-275 (254).

normative gap, the idea of the network has gradually established itself as a concept of international law⁸⁹ and provides an increasingly well-defined term for conglomerates of heterarchic relationships between different more or less autonomous levels of multi-level governance. Network theory understands the formal definition criteria of international law as too rigid to be able to capture the area that lies between national law and international law. It therefore attempts to adapt legal theory to the networked society by creating a new framework for those forms of international governance that exist alongside formal state or intergovernmental institutions, and 'regulatory mechanisms in a sphere of activity which function effectively even though they are not endowed with formal authority'.⁹⁰ By considering the emergence of functionally differentiated systems and their ways of interaction, network theory intends to assign a conceptual place to these networks and the law they produce – a place networks *de facto* possess.

Ladeur addressed the questions that globalisation poses for law at an early stage.⁹¹ He observed the transnational convergence of certain thematic areas (such as environmental or financial issues) on the one hand and transnational regulatory efforts within these areas across territorial borders on the other. Other theorists such as Castells,⁹² Vesting,⁹³ Viellechner,⁹⁴ and Teubner have followed in noting that non-state actors increasingly produce non-state norms of varying legal quality which, even if not of equal strength, in principle have a globally binding effect. By escaping increasingly from national control, they saw functionally differentiated systems becoming networked, while the core of norm making processes shifted from its former nation-state centres to an independent transnational periphery.⁹⁵ They noted that law does not develop

⁸⁹ Thomas Vesting, *Staatstheorie* (Munich: Beck 2018), 157-176; Rakhyun E. Kim, 'Is Global Governance Fragmented, Polycentric, or Complex? The State of the Art of the Network Approach', *International Studies Review* (2019), 1-29; Manuel Castells, *The Information Society: Economy, Society and Culture, Vol. 1: The Rise of the Network Society* (Oxford: Blackwell 1996).

⁹⁰ Rosenau (n. 74), 5.

⁹¹ See Karl-Heinz Ladeur, *Postmoderne Rechtstheorie: Selbstreferenz, Selbstorganisation, Prozeduralisierung* (Berlin: Duncker und Humblot 1992).

⁹² Manuel Castells (n. 89); Manuel Castells, *The Information Society: Economy, Society and Culture, Vol. 2: The Power of Identity* (Oxford: Blackwell 1997); Manuel Castells, *The Information Society: Economy, Society and Culture, Vol. 3: End of Millennium* (Oxford: Blackwell 2000).

⁹³ Thomas Vesting, *Die Medien des Rechts: Computernetzwerke* (Weilerswist: Velbrück Wissenschaft 2015); Thomas Vesting, *Rechtstheorie* (2nd ed., Munich: Beck, 2015).

⁹⁴ Lars Viellechner, *Transnationalisierung des Rechts* (Weilerswist: Velbrück Wissenschaft 2013); Lars Viellechner, 'The Network of Networks: Karl-Heinz Ladeur's Theory of Law and Globalization', *GLJ* 9 (2009), 516-536.

⁹⁵ Galf-Peter Callies, 'Systemtheorie: Luhmann/Teubner' in: Sonja Buckel, Ralph Christensen and Andreas Fischer-Lescano (eds), *Neue Theorien des Rechts* (Stuttgart: Lucius & Lucius 2009), 71-74.

exclusively hierarchically, but is increasingly produced by non-state actors who coexist heterarchically⁹⁶ and replace the state as the sole author of law.⁹⁷ These processes can be recognised in principle at 'all levels of public order, from the nation states to the global order'.⁹⁸

2. Cyberspace Governance Through the Lens of Network Perspective

In the following, network theory is explained in the context of the IETF, ICANN, and IGF. The ideas of network theory are introduced and explained with reference to the three institutions. A focus is placed on the network characteristics, and how they affect the quality of the entities' regulatory activities and decisions. In this way, firstly, the claims of network theory are illustrated and made comprehensible. Secondly, however, the legitimisation paths within the three institutions also become apparent.

a) IETF, ICANN and IGF as Non-State Networks

It has become very clear, that IETF, ICANN, and IGF perform tasks of the global Cyberspace Governance by developing coherent solutions across state borders, while existing and acting independent of nation States. If we think of the individual institutions as networks, in this picture the individual actors take the places of network nodes that are in permanent exchange with each other, which builds a connection between the Network nodes. There is no hierarchy between the network nodes; if any functions are assigned to individual members of the network, they are of coordinative nature.

b) The Legitimacy of Networks and Their Decisions

From the *de facto* accepted regulatory activity of non-state actors, network theory deduces that there is obviously no need for transcendental reasons

⁹⁶ Angelo Jr Golia and Gunter Teubner, 'Networked Statehood: An Institutionalized Self-Contradiction in the Process of Globalization?', MPIL Research Paper No. 2020-40, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725646>, 5.

⁹⁷ Kettemann (n. 6), 189.

⁹⁸ Karl-Heinz Ladeur, 'Globalization and the Conversion of Democracy to Polycentric Networks: Can Democracy Survive the End of the Nation State?', EUI Working Paper LAW 4 (2003), 23.

inherent to a state to legitimise regulatory actions and decisions.⁹⁹ While society is developing into a 'knowledge society',¹⁰⁰ the channelling, collection, and exploitation of knowledge is replacing morality and value concepts as sources of legitimacy.¹⁰¹ According to network theory, the interaction of various participants (visualised as network nodes),¹⁰² which all follow their own mandates differing in terms of content and function, results in an exchange of actor-specific knowledge by means of communication (visualised as connections between nodes), that can be collected in a common knowledge pool which then becomes the legitimating basis for actions.¹⁰³ The fact that this pool of knowledge serves as a legitimising basis becomes particularly evident in the case of IETF and ICANN, whose decisions derive their normative force obviously not from the same grounds of legitimacy that underlie state decisions. With their focus on cyber specific regulatory activities, they primarily feed on technical knowledge and practical considerations. In case of the IETF, no need for transcendent grounds of legitimacy exists because of the decisions purely technical nature. It gets more interesting (and more obvious) with ICANN, where other than practical considerations, such as those of a moral nature, do not influence the work of ICANN (as could be seen very well in the .xxx-case).¹⁰⁴ In the case of the IGF, the matter is more difficult because following the IGF's broad mandate, a large number of different interests convene. But here, too, the intention is to achieve governance precisely by turning away from states' and their grounds' influence.

c) Feeding and Exploiting of the Knowledge Pool

The next question is how exactly this knowledge pool is used. How is it fed and how does the knowledge in the network converge into decisions? Both is achieved through the network structure as well as through the processes inherent to networks.

⁹⁹ Angelo Jr Golia and Gunther Teubner, 'Societal Constitutionalism (Theory of)', MPIL Research Paper No. 2021-08, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=38040941>, 1.

¹⁰⁰ Viellechner, Network (n. 94), 520.

¹⁰¹ Viellechner, Network (n. 94), 520.

¹⁰² Golia and Teubner (n. 96), 5.

¹⁰³ Ladeur (n. 98), 17-20.

¹⁰⁴ Which, by the way, does not mean that states cannot make political decisions within their own territory; they remain free, for example, to block certain domains altogether or to ban specific content.

The network structure, in which the participants stand next to each other in a heterarchically, allows the knowledge pool to be filled with as many information as possible. By allowing all interested parties to become part of the network, their existing knowledge can be fed into the network. Since the link between the actors of a network is, firstly, based on cooperation¹⁰⁵ and, secondly, relatively permanent, without being corporatised and too fixed,¹⁰⁶ any actor can join the network without major difficulties and contribute with its specific knowledge to the common pool, the integration of as many participants as possible minimises the possibility that specific knowledge is overlooked.

How knowledge is collected within networks can be illustrated well by looking at the structure and functioning of IETF, ICANN, and IGF. The accumulation of as much information as possible provides the basis from which decisions are made. For the IETF it applies that there is no formal membership of the IETF; instead, any interested party can participate in the development of standards without representing specific bodies, to make sure that anyone's knowledge may find its way into the processes.¹⁰⁷ The same is true for ICANN and IGF, where all stakeholders stand side by side in a strictly non-hierarchical way and where everyone who wishes can participate in both ICANN's and the IGF's tasks.

In a next step, the knowledge in the network is channelled to converge into decisions. That all knowledge available among the individual actors becomes accessible and finds its way into the decision-making, is ensured by the recursive, communicative processes between the network nodes.¹⁰⁸ Within IETF, all members are granted the possibility to contribute to problem solving; everyone's suggestions are heard and considered until the best suitable standard or protocol prevails. The same applies to ICANN: All decisions are developed jointly by all participants in a discursive process. ICANN even established governing bodies to ensure that structure and processes are adhered to by all. IGF's processes, too, ensure that as much knowledge of different actors as possible is considered, even if the IGF does not (yet) produce binding decisions or norms. So far, it can be rather understood as one institutionalised discursive process on Cyberspace

¹⁰⁵ Viellechner (n. 94), 520; Karl-Heinz Ladeur, *Das Umweltrecht der Wissensgesellschaft* (Berlin: Duncker und Humblot 1995), 22–45.

¹⁰⁶ Gunther Teubner, 'Die vielköpfige Hydra: Netzwerke als kollektive Akteure höherer Ordnung' in: Patrick Kenis and Volker Schneider (eds), *Organisation und Netzwerk: Institutionelle Steuerung in Wirtschaft und Politik* (Frankfurt/Main: Campus-Verlag 1996), 189–216 (193).

¹⁰⁷ IETF, RFC 2028, <<https://www.rfc-editor.org>>, 3.

¹⁰⁸ Golia and Teubner (n. 96), 19.

governance;¹⁰⁹ anyhow, the very fact that the IGF has no decision-making power is likely to encourage participants to engage rather unreservedly in the discourses which at least leads to filling the common knowledge pool.¹¹⁰

d) Networks' Law and Legal Quality

According to network theory, the work of the networks is not just a random regularity, but rather follows a certain order that is maintained by a specific law inherent to the networks which also defines the legal quality of the networks themselves. Teubner undertakes to specify both the law inherent to networks and, in a next step, the legal quality of networks themselves. As the special function of the law of networks, he recognises their capacity to bind uncertainties between the actors.¹¹¹ By convening in the network, the actors are empowered to permanently observe themselves and others: Since the network nodes are permanently focused both on their own purpose and on the network's purpose (Teubner describes the nodes as *double oriented*), any decision, as soon as it is made, binds both the nodes themselves, but also the entire network (*double attribution*).¹¹² By this way of permanent mutual observation and communication, they can both stabilise their expectations¹¹³ and strengthen the network as such. He further examines intensively the question of whether networked systems have their own particular constitution. In order to define a genuine constitutional concept for non-state regimes, he detaches the concept of the constitution from the nation state and considers which elements form its core, so that they can be absorbed and re-applied to new phenomena. He finds that it is not decisive whether or not a constitutional document exists, but if certain processes and key actors have been socially institutionalised.¹¹⁴ The decisive criterion for determining whether a constitution exists, is whether a network manages to keep its balance by resisting tendencies of monopolisation of individual actors.¹¹⁵ What is meant by this can again be clarified and further elaborated with reference to the IETF, ICANN, and IGF.

¹⁰⁹ Kettemann (n. 6), 114.

¹¹⁰ Kettemann (n. 6), 115.

¹¹¹ Gunther Teubner, 'Das Recht hybrider Netzwerke', ZHR 165 (2001), 550-575 (554-557).

¹¹² Teubner (n. 106), 199.

¹¹³ Teubner (n. 106), 199.

¹¹⁴ Gunther Teubner, 'Globale Zivilverfassungen: Alternativen zur staatszentrierten Verfassungstheorie', HJIL 63 (2003), 1-28 (10).

¹¹⁵ Teubner (n. 114), 14-18.

Assuming that a network's decision is best when all essential information is given equal attention, it is important not to give excessive weight to either individual pieces of information or single actors, because in this way, the process of knowledge channelling would be corrupted. A look at IETF and ICANN makes this clear: within the IETF, all actors pursue the uniform interest of finding best technical standards and protocols. Interests of a different than purely technical nature, such as moral-oriented ones, are irrelevant. Therefore, it is not conceivable that any other than technical interests influence the decision-making processes of the IETF. In contrast, when looking at ICANN and the .xxx-case, it becomes clear what is meant by monopolisation of individual actors (the push of states to impose their values onto Internet's infrastructure). Here, ICANN manages to counter these tendencies by establishing an independent dispute resolution body that interprets and applies the rules ICANN gives itself. In the case of the IGF, where value- or morality-related interests are raised alongside technical issues, monopolising tendencies are not only in principle conceivable. It was precisely to prevent such tendencies, namely the monopolising of state actors with their respective ideologies and interests, that it was not given decision-making power in the first place as a precaution. From a network perspective, IETF, ICANN, and IGF all have their own constitutionality.

3. Order and Legitimacy Through Networks

At the end of these considerations, it becomes clear that IETF, ICANN and IGF each realise network characteristics. On the one hand, these characteristics have the effect of creating knowledge pools of their own kind, which become a basis for decisions. These knowledge pools replace transcendent or otherwise superior reasons as the only sources of legitimacy. The network-specific structures and the processes cause that knowledge is first collected and made accessible, and then channelled in such a way that, firstly, irrelevant considerations with regard to the specific question are filtered out and, secondly, that knowledge can converge into decisions that are primarily knowledge-based.

IV. Concluding Remarks

In the course of the study, it has become clear that essential institutions of cyberspace governance do not act randomly at all and that there is no cause

for concern in view of the fact that essential regulatory decisions in cyberspace do not primarily originate from or are controlled by states. Rather, an order can be discerned in the activities that allows conclusions to be drawn about new stocks of legitimacy. Network theory is therefore able to provide information about these new stocks of legitimacy. It therefore seems in principle suitable for capturing new types of governance phenomena in legal theory.

Cyberspace seems to be a particularly good field for examining network theory. Indeed, it seems that what network theory has elaborated on a theoretical level becomes particularly clear in cyberspace, especially when one considers the beginnings of cyberspace and its development through associations of anarchic IT experts (such as the IETF). The comparison of IETF, ICANN, and IGF has also shown that all three entities follow the same pattern in their structure and processes. It is also noticeable that the complexity of their order grows with the complexity of their respective mandates. The more different interests have to be integrated into governance, the more difficult it is to maintain the balance between the participants. A particular difficulty seems to be the involvement of political or ideological stakeholders: ICANN has succeeded in countering monopolising tendencies of states by installing an external panel; if, on the other hand, one wanted to endow the IGF with more decision-making power, one would have to consider whether and which mechanisms could be installed to prevent monopolisation there, too, so that the IGF can produce efficient results.

Nevertheless, it should be borne in mind that this contribution only considered three individual institutions of cyberspace governance. It did not address how the institutions interact with each other, nor did it describe and analyse other entities. Therefore, it is by no means possible to deduce general statements about the governance of cyberspace. However, perhaps this contribution can at least serve as a proposal for further exploration of network theory. This engagement need not be limited to the activities of international non-state actors. Rather, it also seems worthwhile to examine it in the context of regulatory activity in general – be it national, international, non-state or state, since it may bring essential further development of legal theories.

Interpretive Community 2.0: How Blogs and Twitter Change International Law Scholarship

Ralph Janik*

University of Vienna, Vienna, Austria

ralph.janik@univie.ac.at

Abstract	841
Keywords	842
I. Introduction	842
II. The Peculiarities of International Law Scholarship	845
1. An Interpretive Community ...	845
2. ... or an Interpretive Society?	847
III. Social Media and International Law Academia: Risks and Opportunities	849
1. Challenging Gatekeeping	851
2. Academic Tortoises	856
3. Global Reach and Access Inequality	858
4. Two Practical Examples of the Interaction Between Social Media and International Law	860
a) The Good: A Blog Survey on the US-Led Strikes against Assad and the Curious Case of Article 2(4)	860
b) The Bad (and the Ugly?): The International Criminal Court vs. the 'Blogosphere'	862
IV. Conclusion	865

Abstract

Using Stanley Fish's description of interpretive communities, this paper examines the impact of Social Media as an additional tool in international law scholarship. On the one hand, it might work against Western-centrism as debates could become more open and accessible for academics from different backgrounds and regions. On the other hand, there is a real risk that some of the downsides we may observe in political online debates – polarisation and a decline of basic decency – could also extend to the academic realm. It is about time to ask ourselves whether and how we can ensure that the benefits outweigh the costs.

The following article is divided into two main parts: The first will refer to Stanley Fish's notion of 'interpretive communities' to outline how Social

* The author teaches international law at the University of Vienna, SFU, Andrassy University, and Webster Private University Vienna.

Media may influence the pre-existing special and distinctive features of international law scholarship. The second, then, will show how the benefits of blogging and tweeting outweigh justified worries: Social Media increases participation in and readership of international law-related debates and allows qualified commentary to be published (almost) instantly.

Keywords

social media – internet law – interpretive communities – international law theory

I. Introduction

‘Web 2.0’ or, to use the nowadays more fashionable term, Social Media, has brought profound changes to how we communicate, share ideas, or get information. Obviously enough, this general transformation of mere passive consumers into producers of online content also has a tremendous impact on the science of international law. Long gone seem the days of the Westphalia myth, of Gentili or Grotius, the later rise of legal scientificism and international law societies,¹ or regional or national self-encapsulation of scholars due to geographic and other obstacles causing academic time-lags when debating new judgements, treaties, or other impactful international events.

You can now discuss anything in real time, anywhere, with anyone. In the age of globalisation, hardly an aspect of our lives escapes international regulation:² much to talk and disagree about, not only among scholars but also the (sometimes neglected) countless practitioners behind the myriad of abstract entities we describe as subjects of international law,³ chief among them the 200 or so states – which often speak with two or even more different tongues, as the government may differ from the findings of national courts –, uncounted international organisations, or international courts and tribunals.

In this setting, the lines between theory and practice, between official and unofficial statements, both on- and offline, are often blurred: Law

¹ See, above all, Martti Koskenniemi, *The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870-1960* (Cambridge: Cambridge University Press 2001).

² See David J. Bederman, *Globalization and International Law* (New York: Palgrave Macmillan 2008).

³ See Andrea Bianchi, *International Law Theories: An Inquiry into Different Ways of Thinking* (Oxford: Oxford University Press 2016), 297-298; for a specific and extensive elaboration on the role of individuals behind an abstract entity like the International Criminal Tribunal for Rwanda (ICTR), see Nigel Eltringham, *Genocide Never Sleeps: Living Law at the International Criminal Tribunal for Rwanda* (Cambridge: Cambridge University Press 2019).

professors may be appointed as judges, arbiters, or special rapporteurs, while legal advisors or members of courts give lectures, participate in conferences, and engage in academic writing. One of the peculiarities of international law is the broad array of individuals from different professional backgrounds and countries contributing to the evolvement of new rules and the adaption of existing ones through revolving doors – a group Oscar Schachter famously described as the ‘invisible college of international lawyers’.⁴

From a more general perspective, we may further observe that this college equally forms what Stanley Fish famously described as an ‘interpretive community’,⁵ namely

‘not so much a group of individuals who shared a point of view, but a point of view or way of organizing experience that shared individuals in the sense that its assumed distinctions, categories of understanding, and stipulations of relevance and irrelevance were the content of the consciousness of community members who were therefore no longer individuals, but, in so far as they were embedded in the community’s enterprise, community property’.⁶

As I will show below, Social Media challenges both Schachter’s college and the generally established thinking on interpretive communities in several ways: First, it has the potential to open academic membership and the associated admission criteria. Second, the already ongoing inflation of scholarship has now expanded even further since traditional venues have been supplemented by international law-blogs, some of which have established themselves as new intermediary *fora* between the lengthy and all too often painful peer review-process of journals and completely non-curated ad hoc-comments. Third, more and more international lawyers go beyond *any*

⁴ Oscar Schachter, ‘The Invisible College of International Lawyers’, *Nw.U.L.Rev.* 72 (1977), 217-226.

⁵ Applying Fish’s concept to international law(yers) is not new, see already Ian Johnstone, ‘Treaty Interpretation: The Authority of Interpretive Communities’, *Mich. J. Int’l L.* 12 (1991), 371-419; Detlev F. Vagts, ‘Treaty Interpretation and the New American Ways of Law Reading’, *EJIL* 4 (1993), 472-505; for more recent scholarship in this regard, see Michael Waibel, ‘Interpretive Communities in International Law’ in: Andrea Bianchi, Daniel Peat and Matthew Windsor (eds), *Interpretation in International Law* (Oxford: Oxford University Press 2015), 147-165; Jean d’Aspremont, *Epistemic Forces in International Law: Foundational Doctrines and Techniques of International Legal Argumentation* (Cheltenham/Northampton: Edward Elgar Publishing 2015), 18; d’Aspremont repeated these introductory elaborations in his book chapter ‘The Professionalisation of International Law’ in: Jean d’Aspremont, Tarcisio Gazzini, André Nollkaemper, and Wouter Werner (eds), *International Law as a Profession* (Cambridge: Cambridge University Press 2017), 19-37 (29 f.).

⁶ Stanley Fish, *Doing What Comes Naturally: Change, Rhetoric, and the Practice of Theory in Literary and Legal Studies* (Durham and London: Duke University Press 1989), 141.

academic intermediaries by using personal Social Media accounts – first and foremost Twitter, but also Facebook – to promote themselves, share their work, exchange with colleagues and the broader public, voice their personal (sometimes political, sometimes legal) views, or simply seek mutual self-assurance that international law indeed exists.

International law scholars have already noted a number of ensuing pros and cons or risks and chances of these developments: Increasing participation by less-known voices and a corresponding further democratisation of debates⁷ vs. fears over less restrictive standards of scholarly production⁸ and a digitalised Matthew effect where big names retain disproportionate influence;⁹ emancipation from big publishers to acquire broader readership for one's own work¹⁰ vs. academic self-marketing, often coupled to self-restraint to avoid offending one's readers;¹¹ new possibilities for permanent academic exchange vs. digital polarisation caused by emotions, biases, or even ad hominem-arguments leaving little room for the principle of charity or other argumentative tools to ensure an open, fair, and rational debate (if such a thing may even exist);¹² or the value of quick and still qualified ad hoc-comments on new developments or events¹³ vs. a 'speed kills'-commenting mentality at the expense of substance.¹⁴

⁷ Carsten Stahn and Eric de Brabandere, 'The Future of International Legal Scholarship: Some Thoughts on "Practice", "Growth", and "Dissemination"', *LJIL* 27 (2014), 1-10.

⁸ Jean d'Aspremont and Larissa van den Herik, 'The Public Good of Academic Publishing in International Law', *LJIL* 26 (2013), 1-6.

⁹ Hannah Birkenkötter, 'Blogs in der Wissenschaft vom Öffentlichen Recht. Ein Beitrag zur Erschließung neuer Formate' in: Andreas Funke and Konrad Lachmayer (eds), *Formate der Rechtswissenschaft* (Weilerswist-Metternich: Velbrück Wissenschaft 2016), 117-140; Christine Schwöbel-Patel, 'Insta-Scholarship: the Self-Branding Practices of the "Digital Humanitarian"' in: Lianne J. M. Boer and Sofia Stolk (eds), *Backstage Practices of Transnational Law* (Oxon and New York: Routledge 2019), 125-142.

¹⁰ Roger Alford, 'Self-Publishing Legal Scholarship', 12 April 2011, <<http://opiniojuris.org/>>.

¹¹ Schwöbel-Patel (n. 9) explicitly mentions Philippe Sands as an example of a particularly influential international law scholar with a personal Twitter account; on Social Media becoming part of regular academic profiles see also Stahn and de Brabandere (n. 7); further highlighting the seemingly increasing need to use Social Media as part of self-promotion, Dapo Akande's campaign for a seat in the International Law Commission has set up a distinct Twitter account in January 2021 (@UKILCCampaign); Akande, one of the foremost contributors to *EJIL:Talk!*, has also been nominated by Nigeria, see <<https://www.law.ox.ac.uk>>.

¹² See the discussion of the pros and cons of blogging by Jean d'Aspremont, 'In Defense of the Hazardous Tool of Legal Blogging', 6 January 2011, <www.ejiltalk.org/>.

¹³ Antoine Duval, 'Publish (Tweets and Blogs) or Perish? Legal Academia in Times of Social Media', *Tilburg Law Review* 23 (2018), 91-108.

¹⁴ Constance Duncombe, 'The Politics of Twitter: Emotions and the Power of Social Media', *International Political Sociology* 13 (2019), 409-429; Larissa van den Herik, 'Introduction: *LJIL* in the Age of Cyberspace', *LJIL* 25 (2012), 1-8; see also Schwöbel-Patel (n. 9).

Addressing these issues on the basis of understanding international law academia as one or several interpretive communities, I will argue that Social Media's positively (!) disruptive potential has not yet been fully exploited. A small caveat, however, is due at this point: In times of rapid technological change, my elaborations on the possible effect of Social Media and the associated dangers or opportunities may read like odd speculations in a few decades. In hindsight, I might be making a fool of myself. A small risk I am willing to take.

II. The Peculiarities of International Law Scholarship

1. An Interpretive Community ...

The following observations on the (changing) dynamics of international law academia proceed from the simple observation that legal documents and corresponding comments in blog entries or tweets are, at the end of the day, texts. Scholarly research has always been an act of 'storytelling' based on the construction, de-construction, and exchange of arguments, coupled to the underlying hope of establishing authority and/or convince not only one's academic peers but also practitioners of all sorts.¹⁵ International lawyers examine how legal documents came into being and how these 'living instruments'¹⁶ are being changed over time while respecting that their interpretation depends on who is working with them – one (applicant) state's prosecutor could be another (respondent) state's defence counsel.

These trends reflect striking parallels to literature and literature theory:¹⁷ different contents, similar processes. From this perspective, we may further wonder to what extent the 'invisible college of international lawyers' also features elements of an interpretive community and whether it can also exist online and in a legal academic setting.

¹⁵ This analogy has been pointed out by Bianchi (n. 3), 291-293.

¹⁶ The European Court of Human Rights (ECtHR) first used this term to describe the European Convention on Human Rights in 1978, see ECtHR, *Tyrer v. the United Kingdom*, judgment of 25 April 1978, no. 5856/72, para. 31.

¹⁷ See, among countless others, Ekaterina Yahyaoui Krivenko, 'International Law, Literature and Interdisciplinarity', *Law and Humanities* 9 (2015), 103-122; Ekaterina Yahyaoui Krivenko, 'Engaging International Law and Literature with Kafka, Deleuze and Guattari' in: Christina Binder, Mary E. Footer and August Reinisch (eds), *International Law and ...: Select Proceedings of the European Society of International Law*, Vol. 5 (Oxford and Portland, Oregon: Hart Publishing 2014), 393-404; Andrea Bianchi, 'Terrorism and Armed Conflict: Insights from a Law & Literature Perspective', *LJIL* 24 (2011), 1-21; on law and literature in general, see James Boyd White, 'Law and Literature: "No Manifesto"', *Mercer. L. Rev.* 39 (1988), 739-751.

At the outset, Fish coined this idea under completely different circumstances, namely the final remarks of his discussion of a commentary on poems of John Milton from 1976. Yet, they were never confined to the ‘real’, i. e. offline world but could equally be applied to older long-distance, impersonal academic exchange. Fish always focused on communication as such, not the means. Literature theorists and lawyers have long shared the feeling of wondering whether they have read the same text as their counterparts. In an attempt to break free from what Fish described as the ‘tyranny of the text’¹⁸ at another occasion, he raised the *Gretchenfrage* of whether there can be an objective understanding in such an inherently subjective experience as reading poetry: Is the reader or the text the true source of meaning, can different readers of the same text ever come to the same conclusions and, if so, how and why?

Fish’s answer was that it was indeed possible to distinguish between the informed expert with the necessary background knowledge to tell others what they *ought* to think and those who are doomed to fail at truly understanding a given text.

In this sense, neither the interpreter nor the text ‘produce meanings and are responsible for the emergence of formal features’ but rather ‘interpretive communities’¹⁹ – exclusive debate clubs ‘made up of those who share interpretive strategies not for reading (in the conventional sense) but for writing texts, for constituting their properties and assigning their intentions’.²⁰

Lastly, we need to ask the fundamental question whether there can really be an interpretive *community* in international law. While the ability of engaging in interpretation is a human trait, the strategies and methods behind it are being learned and can thus be changed, exchanged, or forgotten. One and the same legal document is not only transformed over time²¹ but also by the composition of the respective community working with it. There is no such thing as a stable text.

As will be shown below, the real challenge posed by Social Media is its gradual expansion of membership in international law’s interpretive community.

The increased possibilities for truly worldwide academic participation highlight how its allegedly universal character may simultaneously prevent

¹⁸ Stanley Fish, *Is There a Text in This Class? The Authority of Interpretive Communities* (Cambridge, Massachusetts: Harvard University Press 1980), 7.

¹⁹ Fish (n. 18), 14.

²⁰ Stanley Fish, ‘Interpreting the “Variorum”’, *Critical Inquiry* 2 (1976), 465–485 (483).

²¹ One may thus consider the notion of intertemporal law as an artificial attempt to re-discover lost interpretation strategies, see Philip C. Jessup, ‘The Palmas Island Arbitration’, *AJIL* 22 (1928), 735–752.

scholars from ever developing a truly shared set of techniques, understandings, and language for interactions between liberal and illiberal states, the West and the rest, North and South, poor and rich, developing and developed, former colonial powers and former colonised peoples, and so on.

2. ... or an Interpretive Society?

Due to this heterogeneity, international lawyers not only have much to discuss but are also doomed to disagree. To begin with, international law results from the well-known constant tension between the desire to justify governmental practices and a collective endeavour to overcome individual state-interests.²² Scholars are often practitioners et vice versa. Already Schachter raised the still-unsettled ‘question of objectivity in international law’ as the fundamental problem for the invisible college since

‘[t]he mingling of the scholarly and the official affects both categories, and often creates tension as individuals move from one role to another or perceive themselves as acting in the dual capacity of objective scientist and government advocate. Concern over this kind of “dédoublement fonctionnel” has been manifested by both government officials and scholars. Government officials often tend to suspect or disdain “objective” views as divorced from reality and insufficiently responsive to national aims. This attitude can have a significant impact on some international lawyers. It may lead them to adopt a strong “national interest” and “realpolitik” line, or it may convince them of the necessity of foregoing this dual capacity and maintaining their objectivity removed from government influence’.²³

Probably even more importantly for present purposes, legal education pulls into two opposite directions here: On the one hand, Western conceptualisations and academic institutions are still predominant:²⁴ the ‘invisible college’ was and is not truly ‘global’ but, as Anne Peters has noted, ‘an elite college of scholars of the developed world, a college in which academics from the so-called Global South are relegated to the role of the eternal students’.²⁵

²² Martti Koskeniemi, *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge: Cambridge University Press reissue 2006).

²³ Schachter (n. 4), 218.

²⁴ See, among others, James Thuo Gathii, ‘International Law and Eurocentricity’, EJIL 9 (1998), 184-211 or Lauri Mälksoo, ‘Civilizational Diversity as Challenge to the (False) Universality of International Law’, Asian Journal of International Law 9 (2019), 155-164.

²⁵ Anne Peters, ‘International Legal Scholarship Under Challenge’ in: Jean d’Aspremont, Tarcisio Gazzini and André Nollkaemper (eds), *International Law as a Profession* (Cambridge: Cambridge University Press 2017), 117-159 (119).

On the other hand, the ‘landmark judgments’ or approaches towards international law depend on where a lawyer comes into contact with it. We can no longer deny that international law is not *truly* international.²⁶ Lawyers from different countries or regions operate with completely different understandings of central terms like sovereignty – the ‘S-word’²⁷ –, human rights, or democracy. Those who studied and work in more dominant states view the world with different eyes than their peers in weaker ones, those from the Global South experience international law different than scholars in richer countries,²⁸ governments may start targeted Social Media campaigns to promote their legal views (such as the one launched by Israel against the International Criminal Court after the Office of the Prosecutor announced its investigation of the situation in Palestine²⁹). Great Powers are more assertive and keener on protecting their freedom to act while smaller ones emphasise the need for international cooperation and the rule of law³⁰ – if you have no weapons, you are left with words, a cynic could say.

Looking at the permanent five of the Security Council, for example, one can see at least three, maybe four, possibly even five different understandings and – in the case of Russia and China, outright instrumentalisation – of international law: The United States (US) oscillates between isolationism and partly geopolitical, partly humanitarian interventionism, between democracy promotion as part of constructing and defending a rules-based ‘liberal world order’ and unilateralism whenever it suits its sovereign interests.³¹ France and the United Kingdom, as the other two members of the community of liberal states, face the difficult task of coping with their relative decline: While the

²⁶ Anthea Roberts, *Is International Law International?* (Oxford: Oxford University Press 2017); see also Martti Koskeniemi, *The Politics of International Law* (Oxford and Portland, Oregon: Hart Publishing 2011), 50: ‘Instead of a “common law of mankind”, international law becomes its ideological contrary; a divisive weapon; a protective shield under which the privileges of some can be upheld against the claims of others; and a unilateral weapon in the hands of the hegemon.’

²⁷ Louis Henkin, ‘That “S” Word: Sovereignty, and Globalization, and Human Rights et cetera’, *Fordham L. Rev.* 68 (1999), 1-14.

²⁸ See e.g. Jochen von Bernstorff and Philipp Dann (eds), *The Battle for International Law: South-North Perspectives on the Decolonization Era* (Oxford: Oxford University Press 2019) or the TWAII Perspectives on ICL, IHL, and Intervention, *AJIL Unbound* 109 (2015) <<https://www.cambridge.org/>>.

²⁹ Israel worked with google ads and created a website dedicated to explain why the ICC does not have jurisdiction over the situation in Palestine, see the criticism by Kevin John Heller, <<https://twitter.com/kevinjohnheller/status/137233319221319168>>.

³⁰ Austria, for example, has been coordinating the 50 states part of the ‘Group of Friends of the Rule of Law’ since 2005, see <<https://www.bmeia.gv.at>>.

³¹ ‘Multilateral when we can, unilateral when we must’, as Madeleine Albright put it, quoted in Joy Gordon, ‘When Unilateralism is Invisible: A Different Perspective on the Oil-for-Food Scandal’, *Global Governance* 13 (2007), 59-77 (59).

former also takes a leading role in the European Union,³² the latter has voted to leave and walk a still undefined route.

Meanwhile, Russia and China like to portray themselves as anti-liberal antagonists in the sense that both defend a much more robust, traditional understanding of sovereignty and a preference for pluralism on the international level (of political systems, that is) while seeking homogeneity (e.g. when it comes to party politics, minority rights, or freedom of speech) inside of states.³³

For these reasons, the common argumentative ground of international law academics from different national or regional backgrounds is shaky. The lack of coherent shared legal techniques, understanding of the law and its conflation with politics make it difficult to draw the line between dogmatic arguments and moral philosophy, legal theory, or political science.³⁴

Perhaps the interpretive community of international lawyers should thus rather be described as an interpretive *society*, i.e. one with only weak terminological and dogmatic bonds.³⁵ International law academia is as fragmented as its field of activity. There is not one, but several interpretive communities.

III. Social Media and International Law Academia: Risks and Opportunities

Social Media has added another layer to international law's complex web of actors and approaches. To begin with, the abundance and lack of originality of scholarship has already been bemoaned before the rise of legal blogs.³⁶ Further growth and the corresponding impossibility to keep track of

³² In the 2019 Aachen treaty, France and Germany, as the two foremost powerhouses of the European Union, decided to 'closely coordinate their positions [...] also in accordance with the positions and interests of the European Union' and pledged to 'work together to promote the positions and promises of the European Union in connection with global challenges and threats'. The treaty can be accessed at <<https://www.bundesregierung.de>> (German version) or <<https://www.elysee.fr>> (French version).

³³ See Rein Müllerson, 'Ideology, Geopolitics and International Law', *Chinese Journal of International Law* 15 (2016), 47-73.

³⁴ This conflation has been observed by Anne Peters, 'Die Zukunft der Völkerrechtswissenschaft: Wider den epistemischen Nationalismus', *HJIL* 67 (2007), 721-776 (750-751).

³⁵ On this distinction in international law in general, see Russel Buchan, *International Law and the Construction of the Liberal Peace* (Oxford and Portland, Oregon: Hart Publishing 2013).

³⁶ David J. Bederman, 'What's Wrong with International Law Scholarship? I Hate International Law Scholarship (Sort of)', *Chinese Journal of International Law* 1 (2000), 75-84 (81).

what has been said, by whom, and where adds another dimension to the pre-existing problem of academic inflation.

What is more, academia is not immune to the general risk of creating or further strengthening digital ‘echo chambers’ where confirmation biases run rampant and users are increasingly detached from other viewpoints. However, echo chambers are usually not as isolated as commonly thought.³⁷ Furthermore, such tendencies can also be observed in the traditional academic sphere. There is a thin line between the understandable ambition to preserve and strengthen regionalised or national approaches in smaller or Eastern European countries and an almost complete self-encapsulation as can be observed in Russia.³⁸

In this connection, Social Media accounts and user comment sections in newspapers (or blogs, for that matter) further stand accused of bringing out the worst in people, from not even bothering to read others’ arguments carefully and being ready to overthink one’s position to trolling or even hate speech. By now we have all witnessed the spread of online hostility, not only by anonymous accounts but even official ones, most prominently Donald Trump in his capacity as the 45th president of the United States.³⁹ The absence of many of the social restraints operating in the ‘real world’ may lead to a collapse of even minimum standards of civility.⁴⁰

³⁷ On these social networks phenomenon in general and challenging the view of rising online ‘segregation’ in a non-scholarly context, see Seth Flaxman, Sharad Goel and Justin M. Rao, ‘Filter Bubbles, Echo Chambers, and Online News Consumption’, *Public Opinion Quarterly* 80 (2016), 298-320.

³⁸ For example, the Polish Yearbook of International Law explicitly states its ‘preference for Central Eastern European scholarship and manuscripts which focus on the region’, <<http://www.pyil.inp.pan.pl>>; the Finnish Yearbook of International Law, while open to submissions from all over the world, explicitly ‘aspires to honour and strengthen the Finnish tradition in international legal scholarship’, see <<http://fsil.fi/fybil/>>; Russian scholarship is a particularly drastic example since most publications are being written in Russian and primarily aimed at a domestic audience, see Lauri Mälksoo, *Russian Approaches to International Law* (Oxford: Oxford University Press 2015).

³⁹ Brian L. Ott, ‘The Age of Twitter: Donald J. Trump and the Politics of Debasement’, *Critical Studies in Media Communication* 34 (2017), 59-68; on the question to which extent Tweets by governments and states leaders might be interpreted as *opinio juris* and state practice, see already Special Rapporteur Michael Wood’s Second report on identification of customary international law, 22 May 2014, A/CN.4/672, para 29: ‘[...] in determining what the relevant practice actually is and to what extent it is indeed accepted as law, and different weight may be given to different evidence [...] the care with which a statement is made is a relevant factor; less significance may be given to off-the-cuff remarks made in the heat of the moment.’

⁴⁰ See, among countless others, Emma A. Jane, ‘Flaming? What Flaming? The Pitfalls and Potentials of Researching Online Hostility’, *Ethics and Information Technology* 17 (2015), 65-87; Ben Martin and Thera Rising, ‘Why is Everyone on the Internet so Mean?’, 8 February 2018, <<http://thera-rising.com/>>; Erin E. Buckels, Paul D. Trapnell and Delroy L. Paulhus, ‘Trolls Just Want to Have Fun’, *Personality and Individual Differences* 67 (2014), 97-102.

There is no guarantee that this decline of etiquette witnessed in public debates stops at the academic gates.⁴¹ One should not forget that traditional communication between scholars is not necessarily a casebook example of courtoisie either.⁴² Cooperation, mutual academic trust, and basic decency can be thwarted: less filters, more problems. There are real psychological risks of being overly confronting when typing blog posts or comments instead of talking in person. ‘Publishing’ by clicking on ‘send’-buttons instead of thinking twice or going through a lengthy peer-review may lead to hostility instead of benevolent interpretation, added confusion instead of clarity, or eagerness to be the ‘first mover’ when it comes to commenting on new developments instead of exercising scholarly restraint and avoid making a fool of oneself. Non-redacted statements, be they submitted via Twitter accounts, personal blogs, or in the comments-section of blogs – which can, as one should not forget, at times not be deleted or edited by the authors themselves –, might be off the mark.

As indicated, most of these problems are not entirely new. Digital means of communication cannot cause disruption by themselves but rather aggravate existing troubles. Yet, even if they do, I will argue that the benefits for the interpretive community of international law still outweigh the costs. Digital hyperconnectivity enables genuinely global academic exchange and can expose scholars to views outside of their ‘bubble’, be it from interested laymen or academics from the Global South for whom tweeting or blogging is easier than travelling to conferences. As to the passive side, Social Media can attract much larger audiences than traditional scholarly work and make international law more accessible for regional or academic ‘outsiders’. With some sense of naivety, it may ultimately contribute to making international law truly international.

1. Challenging Gatekeeping

One of the focal points of academic concerns over Social Media is its most fundamental characteristic, the absence or reduced role of gatekeepers.⁴³ A

⁴¹ By way of example, the University of Bern updated Social Media guidelines from April 2021 call on its staff to exercise self-restraint and coordinate to a minimum degree within faculties when voicing their opinions, in particular in connection with ‘sensitive issues’, see <<https://www.unibe.ch>> and the corresponding comment by Evelyne Schmid <<https://verfasungsblog.de>>.

⁴² While I do not want to point fingers here, one recent example of a particularly harsh critique is Carl-Friedrich Stuckenberg’s review of Frauke Rostalski’s habilitation in ZIS online 4 (2021), 279-297 <<http://www.zis-online.com/>>.

⁴³ See already Brian Leiter, ‘Why Blogs Are Bad for Legal Scholarship’, Yale L.J. Pocket Part 116 (2006-2007), 19 September 2006, <<https://www.yalelawjournal.org/>>.

personal blog or Twitter account is only a few clicks away, no publisher or editor standing in the path of voicing one's opinion, the only barrier being the scrutiny of authorities or readiness of those who feel their reputation is being harmed by online comments to go to court and the corresponding limits of free speech.

By using Social Media, younger scholars or those on the fringes of academia have additional chances to practice legal writing – the very core of their profession⁴⁴ – and gaining access to academic fora. It is e.g. easier for blogs to improve and later publish entries that initially had certain fundamental shortcomings, perhaps attributable to the writer's lack of access to resources, but still develop truly novel thoughts that deserve to be published.

In so doing, however, they might, inadvertently or not, openly or implicitly, defy long-established codes and hierarchies (more on that later).⁴⁵ To prevent or remedy violations of the unwritten rules of international law's interpretive communities, blogs or personal social media accounts will always be tied to some level of explicit (who may publish on a curated blog) or implicit (who 'deserves' an answer in a blog's comments section or on Twitter) gatekeeping.

In general, expertise, evidenced by one's profession, can serve as a 'passport for legal blogging'.⁴⁶ Often enough, membership in international law's interpretive community and hence access to debates is beyond doubt: Bourdieu's critique of the unofficial 'intellectual hit parade' among French thinkers⁴⁷ can easily be transplanted to the field of international law: Some scholars are more often read and cited than others,⁴⁸ receive votes for awards by their

⁴⁴ Duval (n. 13).

⁴⁵ D'Aspremont (n. 12).

⁴⁶ D'Aspremont (n. 12); Birkenkötter (n. 9), 126.

⁴⁷ To quote Pierre Bourdieu's critique of a ranking of French public intellectuals of all sorts, among them writers, philosophers, or journalists: 'The intellectual hit parade represents a sort of artificial reconstruction, and thus one easier to observe, of the process which is constantly at work in the field of cultural production and which elaborates and defines one of the most powerful representations (because objectified and widely broadcast) of the hierarchy of intellectual values. This process, which is no doubt also equivalent to judicial procedure or, in other words, a process of making up prices (as verdicts of the market, is accomplished through "informal" exchange of private and sometimes confidential judgments ("don't say I said so, but so-and-so's book is absolute rubbish") between journalists, between writer-journalists and journalist-writers, but also through the public verdicts of book reviews, critical works, invitations to broadcast on radio or television, and finally the hit parades, ratings and rankings, not to mention the more traditional acts of institutional consecration, like appointment to an academy, which, essentially, only ratify the whole set of these verdicts, etc.', see Pierre Bourdieu, *Homo Academicus* (Stanford: Stanford University Press 1984/1988), 259 f.

⁴⁸ See already Fred R. Shapiro, 'The Most-Cited Legal Scholars', JLS 29 (2000), 409-426; see also Lianne J.M. Boer, 'The Greater Part of Jurisconsults': On Consensus Claims and Their Footnotes in Legal Scholarship', LJIL 29 (2016), 1021-1042.

colleagues, and media attention may not be evenly distributed (obviously enough, not all lawyers want it anyhow). Relatedly, the status of their academic institutions matters just as much as whether they also serve additional functions, from series editors to special rapporteurs or appointments as judges at international courts and tribunals.

The devil in the detail remains. When it comes to one's institutionalised embeddedness, there are difficulties when comparing different academic systems and positions even within Europe, not to speak of the global level. When focusing on legal professionalism, one needs to keep the heterogeneity of the large group of those teaching and researching under precarious conditions in mind: Is it sufficient to be employed to teach one international law-related class per year to be counted as an academic? What about retired and well-respected legal advisors without any formal connections to academic institutions?⁴⁹ Could membership in the international law interpretive community even include non-lawyers who are familiar with the basic tenets of the legal field while accepting the limits of their expertise?

The flexibility of interpretive communities' composition can help to fill such gaps. The community itself regulates admission:

"The only "proof" of membership is fellowship, the nod of recognition from someone in the same [interpretive] community, someone who says to you what neither of us could ever prove to a third party: "we know".⁵⁰

What thus counts is the stability of interpretive strategies, not that of membership. It ensures that debates will keep going until a collectively-established agreement leading to a text's emancipation from its readers is reached, an outcome prevented by the lack of shared codes and methods between and within interpretive communities. The 'interpretive battles'⁵¹ will remain alive as long as there is sufficient mutual understanding of the respective others to prevent the weak common ground from breaking apart.

Some forty years after first coining the notion of interpretive communities, Fish further contrasted the interpretive community of law with groups of people forming associations because they 'share some of the same ideas and aims' like fans from the same movies or sports teams. Interpretive communities are rather

⁴⁹ By way of example, Maurizio Ragazzi, who gave a presentation at the 2014 European Society of International Law meeting agora on international law and theology, described himself as an 'Independent Researcher, former Senior Counsel International Law, World Bank, Washington, D. C.', see <<https://esil2014.univie.ac>>.

⁵⁰ Fish (n. 20), 484.

⁵¹ Fish (n. 20), 484.

‘made up of those who, by virtue of training, experience, and practice, have internalized the norms of some purposive enterprise – law, education, politics, plumbing – to the point where they see with its eyes and walk in its ways without having to think about it. Interpretive community members are not independent agents who self-consciously choose to think and act in a certain way; if they are deeply embedded in the community they have no choice; the world just appears by the emphases and urgencies that are the community’s content’.⁵²

Becoming part of an interpretive community thus requires not so much institutional embeddedness, but being acquainted not only with the terminology, key documents, and practices, along with the hidden rules and hierarchies: Knowing the academic celebrities (and why), trustworthy publishers, leading journals, institutions, and faculties as well as the prerequisite of having read the standard treatises and articles, or being familiar with the formalities of citations, etc.

Most importantly, perhaps, one needs to know the arguments and counter-arguments that have been exchanged already (and by whom). You should not try to bridge the gap between law and policy from the perspective of ‘world order’ without referring to McDougal, Lasswell, and Reisman. You should not ‘discover’ that international law has been fragmented into different ‘sub-universes’ without taking Guillaume, Simma, Hafner, or Koskeniemi into account. And you should certainly not talk about the colonial origins of international law as an instrument to justify oppression without being familiar with the works of Bedjaoui, Weeramantry, Anghie, or Chimni. If these criteria are met, even academics from other fields, most notably international relations, or (well-informed) journalists with non-legal backgrounds may join.

Social Media not only requires us to overthink superficial assumptions of position-based membership in interpretive communities but also the hierarchies within journals and publishers. The big publishing houses and most-cited journals can afford to be much more restrictive than blogs. By way of example, the American Journal of International Law explicitly takes pride of its impact factor and ranking and receives several hundreds of submissions each year.⁵³ Meanwhile, and as noted above, periodicals in smaller countries

⁵² Stanley Fish, *Winning Arguments* (New York: HarperCollins 2016), 122 (eBook version).

⁵³ See <<https://ajil.scholasticahq.com/>> and <<https://www.cambridge.org/>>; the website also embeds a video on the value of the review process, see <<https://youtu.be/CDuA44rx1ag/>>; the rankings can be accessed at <<https://scholar.google.com/>>; yet, one needs to keep in mind that not all journals are included here, see Roger Alford, ‘Google Rankings of the Most-Cited International Law Journals’, 20 March 2013, <<http://opiniojuris.org/>>; for a critique of the tyranny of such numbers see Marko Milanović, ‘Horrible Metrics’, 24 August 2016, <www.ejiltalk.org/>.

often focus on strengthening domestic legal traditions and, in the most extreme cases, become isolated debate clubs among scholars from the same country or region.⁵⁴

Yet, blog editors have long recognised the potential to call the above-described hierarchies into question by giving more weight to new voices, be they younger,⁵⁵ less well-connected, or from neglected regions and institutions: AJIL Unbound ‘seeks to broaden and diversify the scholarly exchanges on international law begun in the pages of [the American Journal of International Law]’,⁵⁶ the German *Völkerrechtsblog* website states the desire ‘to contribute to opening up and diversifying the discourse in international legal scholarship’,⁵⁷ *OpinioJuris* ‘particularly welcome[s] guest posts from women and from the Global South’⁵⁸ and IntLawGrrls ‘aims to give voice to women scholars, lawyers, policymakers, leaders, activists [...] We are particularly mindful of foregrounding voices of junior lawyers and scholars and others who are less often heard in international legal dialogue’.⁵⁹

Obviously enough, upholding minimum standards remains crucial. International law’s interpretive community has always recognised the need to strike the balance between excessive gatekeeping and letting the chains of academia completely loose. There is a reason why some questions ought not to be asked – Fish explicitly mentions Holocaust denial⁶⁰ – and why some people are either dispelled from or ignored by the academic community.⁶¹ Still, scholarship always stands on the verge of being a self-encapsulated field with little ‘real life’-relevance.

While non-personal academic law blogs are, by their very nature, not as selective as law journals, they still have some filters in place.⁶² Those mentioned above (and others, most notably EJIL:Talk!) have their own advisory

⁵⁴ See the footnotes and text to n. 38.

⁵⁵ *OpinioJuris* first started a call for ‘new voices’, i.e. blogposts by international law students or recent graduates in April 2013, see <<http://opiniojuris.org/>>.

⁵⁶ See <<https://www.cambridge.org/>>.

⁵⁷ See <<https://voelkerrechtsblog.org/>>.

⁵⁸ See <<http://opiniojuris.org/>>.

⁵⁹ See <<https://ilg2.org/>>.

⁶⁰ Fish (n. 52), 134 f.

⁶¹ One example would be Daniele Ganser’s book on NATO’s ‘unlawful wars’ and ‘how NATO countries sabotage the UN. A chronic from Cuba to Syria’, where he does not cite a single academic on the use of force, see Daniele Ganser, *Illegale Kriege: Wie die NATO-Länder die UNO sabotieren. Eine Chronik von Kuba bis Syrien* (Zürich: Orrell Füssli 2016); Ganser routinely laments that he has been expelled from the academic community for asking questions no one dares to ask such as NATO’s role in post-World War II Europe or challenging conventional wisdom concerning 9/11.

⁶² D’Aspremont and van den Herik (n. 8).

boards or at least some form of academic vetting.⁶³ No one doubts that academia's gatekeeper function to e.g. prevent unfounded claims and/or activism – for example, the confirmation bias of politically-motivated theses – from putting on pseudo-scientific clothes also extends to the online world.

Be as it may, some might view certain peer-review processes as being based on artificial constructions or as overly formalistic attempts to keep fundamental challenges to the status quo out of the academic arena. One may thus make use of the fact that there exist far less obstacles to setting up a blog than trying to convince a publisher to initiate yet another international law journal. As Fish put it,

'if the learned journals are keeping you and your friends out and labelling what you do "unprofessional" or "non-academic", you can start a journal of your own and devote its first issue to explaining why the current definitions of "professional" and "academic" are too narrow and mask an ideological position that is not announcing itself. In the academy it is always possible to set up a "rogue" territory where what is done is frowned upon by the conservative establishment'.⁶⁴

Entire blogs or blog series – where several articles are being published jointly, often also cross-referencing to one other – can thus be set up dedicated to a certain perspective on international law – e.g. Third World Approaches to International Law (TWAIL) – or research question.

2. Academic Tortoises

Another reason for the disruptive potential of Web 2.0 is speed. As indicated above, the peer-review process takes time, often a lot of it. The 'first view' option or the possibility of publishing the unedited submission via SSRN and similar platforms might be helpful to react comparatively quick, but in no way enables journals to keep up with the hastiness of the internet.

The European Journal of International Law editors readily admit that

'[i]n the old days a time lag of six to nine months was considered very topical. That has become laughable – our production process, even at its best, is a tortoise to the internet hare'.⁶⁵

⁶³ The *Völkerrechtsblog's* 'Scientific Advisory Board' consists of some 38 'post-doctoral' members, the German *Verfassungsblog* 18 'associate editors' at the PhD or (junior) professor level, while EJIL:Talk! arguably has the most distinguished editorial team of all blogs since it includes numerous well-established (tenured) scholars.

⁶⁴ Fish (n. 52), 131.

⁶⁵ See <<https://www.ejiltalk.org/>>.

Blog entries, in turn, can be written and published within hours after a judgement has been rendered, a resolution adopted, a military strike made, etc. Special rapporteurs or governmental advisors, in turn, may rely on such early comments in their (ad hoc-) analyses.⁶⁶

This quickness itself does not cause concern. While one should not underestimate the risk of errors made in the heat of the moment, experts usually can rely on years of research and knowledge acquisition to come up with timely and still valuable analysis. By way of example, Dapo Akande and Marko Milanović wrote their comment on resolution 2249 (2015) concerning the call to fight the ‘Islamic State’ without actually authorising the use of force literally during night time (time difference mattered here).⁶⁷ Having written the first analysis of this kind, they secured the academic sweet spot of being the main point of reference for scholars writing on this topic after them.⁶⁸ While the first subsequent blog entries followed in the next days and weeks,⁶⁹ journal articles were only published some seven months later.⁷⁰

⁶⁶ By way of example, Special Rapporteur on extrajudicial, summary or arbitrary executions Agnès Callamard not only immediately responded to the targeted killing of Iranian general Qassem Soleimani via Twitter herself (see <<https://twitter.com/AgnesCallamard/status/1212910555809361920>>) but also quoted numerous blog comments in her report on this subject-matter published some six months later, see *Use of Armed Drones for Targeted Killings: Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, 29 June 2020, A/HRC/44/38. The Research Services of the German Parliament (Wissenschaftliche Dienste des Deutschen Bundestags) also routinely rely on and quote blog entries, see for example their report on the legal implications of the US-British-French military strike against chemical weapons depots in Syria from 14 April 2018 (*Völkerrechtliche Implikationen des amerikanisch-britisch-französischen Militärschlags vom 14. April 2018 gegen Chemiewaffen-einrichtungen in Syrien*) or its assessment of the Global Compact for Safe, Orderly and Regular Migration from 30 November 2018.

⁶⁷ Dapo Akande and Marko Milanović, ‘The Constructive Ambiguity of the Security Council’s ISIS Resolution’, 21 November 2015, <www.ejiltalk.org/>.

⁶⁸ One could say we could have had a problem with the anchoring, i.e. the ‘cognitive bias where an individual depends too heavily on an initial piece of information offered to make subsequent judgments’ <<https://en.wikipedia.org/>>; needless to say, their mostly descriptive findings proved to be entirely correct and the bias potential negative impact was thus limited if not non-existent.

⁶⁹ See e.g. Marc Weller, ‘Permanent Imminence of Armed Attacks: Resolution 2249 (2015) and the Right to Self Defence Against Designated Terrorist Groups’, 25 November 2015, <www.ejiltalk.org/> or Paulina Starski, ‘“Legitimized Self-Defense” – Quo Vadis Security Council?’, 10 December 2015, <www.ejiltalk.org/>; Ralph Janik, ‘Der Kampf gegen den “Islamischen Staat” – die großen Probleme liegen nicht im Völkerrecht’, *Junge Wissenschaft im Öffentlichen Recht*, 9 December 2015, <<https://www.juwiss.de/>>.

⁷⁰ Peter Hilpold, ‘The Fight Against Terrorism and SC Resolution 2249 (2015): Towards a more Hobbesian or a more Kantian International Society?’, *IJIL* 55 (2016), 535-555; Karine Bannelier-Christakis, ‘Military Interventions against ISIL in Iraq, Syria and Libya, and the Legal Basis of Consent’, *IJIL* 29 (2016), 1-33.

In this sense, blogs eventually sent agorae on current legal events (such as the ones by the American Journal of International Law⁷¹) to the deathbed or at least made them less relevant. By the time of their publication, everything might have been said already, albeit not by everyone. This would not necessarily be a great loss but rather enable journals to focus on their key purpose, namely embedding fresh developments in a broader context and add value beyond initial reactions. Or, to put it more simply: The publication of articles that age well.⁷²

3. Global Reach and Access Inequality

The final disruptive element to be mentioned here concerns dissemination and accessibility. Writing in 2000 and thus before the arrival of Social media, Bederman lamented that the exploding number of journals can only be explained by increased demand:

‘But by whom? I suspect by only two constituencies: law students and international law faculty. Who else reads this stuff?’⁷³

In contrast, blogs can be read by everyone and aim for the broadest audience possible, from those without any academic access at all or stu-

⁷¹ See e.g. the 1990 ‘U.S. Forces in Panama’ agora in volume 84 of *The American Journal of International Law* from April 1990 and thus some four months after the US invasion against Manuel Noriega had begun or the 1984 Agora on ‘the U. S. Action in Grenada’ in volume 78 from January 1984 and thus two months after the beginning of the invasion, or, last but not least, the ‘Appraisals of Nicaragua v. United States’ agora in volume 81 from January 1987 and thus some six months after the decision was made.

⁷² To some extent, this was both foreseeable and happened already. As the European Journal of International Law’s EJIL.Talk!-blog states, it might enable the editors ‘to effect a certain mutation in the identity of EJIL itself: We will give increasing preference to articles which deal with the fundamentals, with First Things, which look at an “Incident” or “decision of a Tribunal” with a view to exploring wide systemic meaning; in short, to articles which we predict will have lasting value – that will be interesting four or five or more years after publication. EJIL.Talk! and EJIL may thus complement each other.’ <<https://www.ejiltalk.org/>>; Complementarity of the traditional, established journal and online contributions is also explicitly in the description of AJIL Unbound (n. 56); see also Stahn and de Brabandere (n. 7), 8: ‘This trend is already visible in the relationship with blogs, where a new division of labour is taking shape. Journals appear to be moving away from coverage of specific types of discourse (e.g. current events, case commentary), in light of the comparative advantages of blogs. There is thus a trend towards self-restriction. It raises new questions what should be published in traditional form, and to what extent it is useful for journals to outsource debates to their own or other blogs (e.g. discussion of articles, review of books).’

⁷³ Bederman (n. 36), 80.

dents from universities facing difficulties to afford costly subscriptions.⁷⁴ Starting with the headline, blog entries are also often designed for a broader audience beyond the interpretive community.⁷⁵ They themselves are also shorter and usually written in more comprehensible, i. e. less academic, possibly even joking and personal manner and may thus help bridging the gap between scholarship and expert commentary in traditional media.⁷⁶ Going back to Fish, academia is, across all fields, marked not only by its shared interpretive techniques, but also a shared vocabulary and knowledge of rules such as citation standards or of the history and present state of debates. When it comes to blog entries, these features are reduced to a minimum, as there is often no space and need for introductions that primarily serve to show educated readers one's familiarity with the standard texts.

Yet, given that more and more academic content is available online (at least the *Digital Object Identifier* [DOI] numbers of articles and specific passages of lengthy treatises via Google books) and can thus be referred to via hyperlinks (blogs entries may obviously refer to other blog entries), the line between shorter comments in journals and sophisticated blog entries is becoming increasingly fuzzy. This trend directly leads to the question of how one should characterise and handle blogs or even Tweets by academics: As 'nothing more than journalism within the epistemic community concerned'⁷⁷ that should thus not be quoted or otherwise referred to in proper academic work? As somewhere in the grey area between journalism and scholarship,⁷⁸ as a *sui generis* type of text,⁷⁹ or as almost equal to journal articles or book chapters?

⁷⁴ The problem of inequality when it comes to access to resources become more and more apparent in recent years of the Jessup International Law Moot Court, prompting Oxford University Press to make more and more of its content available, see e.g. <<https://www.facebook.com/jessupilsa/posts/our-friends-at-oxford-university-press-have-asked-us-to-share-two-new-content-co/2531738500199611/>>.

⁷⁵ Needless to say, 'clickbait' titles can also be found in traditional journals, e.g. Anthony D'Amato, 'It's a Bird, it's a Plane, it's Jus Cogens!', Conn. J. Int'l L. 6 (1990), 1-6.

⁷⁶ D'Aspremont (n. 12).

⁷⁷ D'Aspremont (n. 12); the author is fully aware of the irony of quoting a blog entry saying that blog entries should not be quoted in scholarly work.

⁷⁸ Birkenkötter (n. 9), 132 f.

⁷⁹ Birkenkötter (n. 9), referring to Alexandra Kemmerer, '(Rechts-)Wissenschaft sui generis?', 11 November 2012, <<https://verfassungsblog.de/>>.

4. Two Practical Examples of the Interaction Between Social Media and International Law

As a final observation to highlight both the pros and cons of the impact of Social Media on international law's interpretive community, this part will conclude with a discussion of two examples of blogs and scholarly interaction, one positive, one negative: the collective effort by scholars connected via Social Media to assess states reactions to the April 2018 strikes in Syria and the hostile debates on recent International Criminal Court (ICC) decisions.

a) The Good: A Blog Survey on the US-Led Strikes against Assad and the Curious Case of Article 2(4)

There exists arguably no other field of international law more prone to academic ivory-towerism as described in the preceding section than the use of force. As scholars produce countless articles on the legality of humanitarian interventions or pre-emptive self-defence no one in states' legal departments, foreign, or defence ministries reads, they indeed risk absorbing themselves in a constructed reality where law actually plays a significant role when powerful states decide whether and how to strike militarily.

Most prominently in recent years, international law largely remained on the sidelines during the war in Syria,⁸⁰ not only (as one may expect) among Assad's allies – Russia and Iran –, but also Western states. By way of example, the first US debate on launching strikes against the government of Bashar al-Assad in Syria after he first used chemical weapons where only one Senator asked about the international legal basis for US strikes.⁸¹ In April 2018, then, the US (along with France and the United Kingdom) proceeded to intervene not only against the so-called 'Islamic State' (ISIS) but also against Syria itself, or, more precisely, the government of Bashar al-Assad. Although legal basis of the former had already been questionable – the US relied on a mixture of generalised national security interests, humanitarian imperatives, and, above all, Iraq's right to (collective) self-defence – the debate remained somewhat muted since no state wanted to be seen as somehow siding with

⁸⁰ See Michael P. Scharf, Milena Sterio and Paul R. Williams, *The Syrian Conflict's Impact on International Law* (Cambridge: Cambridge University Press 2020).

⁸¹ See Julian Ku, 'Syria Insta-Symposium: Does the U. N. Charter Matter to the U. S. Senate's Deliberations on the Use of Force? Nope', 3 September 2013, <<http://opiniojuris.org/>> (on a side note, this title is a good example for nonchalant blog language).

ISIS by openly and repeatedly challenging the legality of strikes against it.⁸² The situation was slightly different after Assad's forces purportedly used chemical weapons against their own population. This time, the target was not a non-state terrorist entity condemned by virtually the entire international community but, strictly speaking, the state of Syria. If there was wide acceptance or endorsement, the content of the prohibition of the use of force could have been changed drastically as allowing states to use force for humanitarian reasons and/or as a reaction to the use of chemical weapons (only).

Taking the possibility of such a far-reaching development seriously, a number of scholars from different regions – namely Alonso Gurmendi Dunkelberg, Rebecca Ingber, Priya Pillai, and Elvina Pothelet – openly called on active participation via Twitter to take a closer look at states' reactions to these strikes. A first blog post published at *OpinioJuris* on 22 April 2018 and thus eight days after the intervention 'canvassed' some 100 states of which 56 had indeed made official comments (going beyond mere state practice they also took two international organisations into account⁸³). Then, with some help by active members of the blogosphere/scholars actively using Twitter, they collected, assessed, and categorised these statements by region and type of reaction (whether they supported – politically and/or legally – rejected, or refrained from clearly assessing the strikes). Some two weeks later, they updated their survey with some additional 23 states, amounting to some 133 countries and 79 reactions.⁸⁴ The result was a staggering example of the possibilities of legal scholarship in the age of Social Media: Ten different types of reactions, from explicitly political and legal support of the strikes to outright condemnations including rejections as illegal. In sum, it turned out that only one state – the United Kingdom – had explicitly defended their legality, namely as a humanitarian intervention in conformity with the wording of article 2(4) of the United Nations (UN) Charter.⁸⁵ On the opposite end, they found that some twelve states had explicitly deemed them as illegal. The vast majority of states, however,

⁸² In addition to Syria, Russia and Iran did nevertheless challenge the legality of strikes against ISIS, albeit in a somewhat restrained manner, see e. g. Michael P. Scharf, 'How the War against ISIS Changed International Law', Case W. Res. L. Rev. 48 (2016), 1-54.

⁸³ Alonso Gurmendi Dunkelberg, Rebecca Ingber, Priya Pillai and Elvina Pothelet, 'Mapping States' Reactions to the Syria Strikes of April 2018', 22 April 2018, <<https://www.justsecurity.org/>>.

⁸⁴ Alonso Gurmendi Dunkelberg, Rebecca Ingber, Priya Pillai and Elvina Pothelet, 'Update: Mapping States' Reactions to the Syria Strikes of April 2018', 7 May 2018, <<https://www.justsecurity.org/>>.

⁸⁵ See the UK government's policy paper, Syria Action – UK Government Legal Position, 14 April 2018, <<https://www.gov.uk>>.

refrained from referring to international law and rather made merely political statements.

On the basis of this research, it seems save to say that there was no change of the legal status quo. A substantial transformation of article 2(4) UN Charter as allowing for military action in situations like these had not occurred. Rather, many states followed a path already trodden in Kosovo: Illegal, maybe, but not necessarily illegitimate. The debates surrounding the inadequacies of the prohibition of the use of force between an outright ban even in cases of mass atrocities and the risk of abusive invocations of human rights protection will thus continue for the unforeseeable future. Yet, as this blog post has also shown, it will be more difficult than ever to claim that a certain rule has changed or evolved into customary international law. The gold standard has been set within days, made possible not only by the laudable endeavours of the blog authors themselves, but also, obviously to a much smaller degree, their open call for suggestions of additional state practice in the initial blog post and via Twitter. There is absolutely no reason why blog entries like this one should not be quoted in academic work. In addition, they also put additional pressure on governments or individual ministers: Their statements will not be overlooked, even if they are made in national television and in their own language.

b) The Bad (and the Ugly?): The International Criminal Court vs. the ‘Blogosphere’

Nevertheless, blog entries also have dark sides. Some practitioners do not necessarily like being watched and being confronted with public reactions by those they accuse of not being familiar with their daily work. A particularly drastic example is the rift within the international criminal law interpretive community and the intense criticism by scholarly ‘outsiders’ via blogs or Twitter⁸⁶ concerning the International Criminal Court’s acquittals of Jean-Pierre Bemba and Laurent Gbagbo, the initial decision to refrain from opening an investigation of the Afghanistan situation (which was later overturned) and, lastly, the Appeal’s Chamber judgement in the Jordan Referral re al-Bashir Appeal.

In the latter, scholars finally received a clear answer as to whether their complaints are being heard or taken seriously. Seemingly enraged

⁸⁶ See, in general, Dov Jacobs, ‘On the Impact of Online Commentary in International Criminal Law: A Vain Pursuit of a Socratic Ideal?’, *LJIL* 32 (2019), 615-623.

by an EJIL:Talk! blog entry by Dapo Akande and comments by other scholars,⁸⁷ the ICC's spokesperson – using his real name – appeared in the comment section to openly accusing Akande of not having read the judgement and refer to the (anonymous) Question and Answer (Q&A) document – apparently written by the spokesperson – where one answer was dedicated to the 'animated discussion in blogosphere'.⁸⁸ It is almost cliché-like criticism of the pitfalls of modern communication is worth quoting at length:

'In the era of social media, it is hoped that observers would properly study the Court's judgments and decisions before rushing to comment on them. Hastily made comments, particularly when made before the commentator has even read the judgment in question, will fail to appreciate the totality and nuances of the Court's reasoning, and may wholly misrepresent the decision or judgment. At the same time, those first comments appearing on social media frequently tend to dominate the ensuing discussion as they are tweeted and retweeted, regardless of their accuracy. Lawyers engaging in public commentary should exercise particular caution and remain mindful of the cardinal principles that guide the conduct of lawyers, including that of honesty, integrity and fairness. This principle adequately covers the need to be fair when criticising courts and judges. Notably, the rules of professional ethics in most legal systems impose special caution on criticism of judges and courts, not because it is wrong to criticise them, but because they are generally not in a position to respond to specific criticisms. It does not mean that judges and courts may not be criticised. It only means that they be criticised fairly. There is an ethical obligation to reflect facts and circumstances accurately and fairly. It is not enough to engage in convenient repeat of the commentaries of others, who may not have been fair to begin with.'⁸⁹

In the subsequent section, the Q&A also emphasises that the accounts of critical experts were also 'properly examined and taken into account'. The document then goes on to address certain points of critique obviously raised by scholars concerning the court's judgement. As these are highly technical issues, one can clearly see the extent to which the author gave his utmost to have the final say on these matters.

⁸⁷ Dapo Akande, 'ICC Appeals Chamber Holds that Heads of State Have No Immunity Under Customary International Law Before International Tribunals', 6 May 2019, and the comments by Göran Sluiter, Leila Sadat, Roger O'Keefe or Dov Jacobs, <www.ejiltalk.org/>.

⁸⁸ The Q&A is available via the blog of Dov Jacobs, <<https://thedovjacobs.files.wordpress.com/>>.

⁸⁹ Q&A (n. 88).

A spokesperson speaking both as an academic and on behalf of an institution is a particularly worrisome example of how online debates may get out of hand if basic principles of interpretive communities are being disregarded.⁹⁰ As Dov Jacobs noted,

‘beyond the discussion on the relationship between traditional scholarship and new modes of communication, what should continue to unite the epistemic communities involved in the study of international criminal law is an attachment to shared values of dialogue, intellectual honesty, methodological rigor and, above all, freedom of expression. These values are crucial to guarantee our independence and academic freedom and any threat to any of these values should be combatted vigorously by everyone, both online and in traditional scholarship, as a threat to the epistemic community as a whole’.⁹¹

For what it is worth, one cannot rule out with certainty that this will not be the last time of failed interaction between practitioners or entire international organisations – i.e. the ICC via a not so anonymous Q&A directly confronting its critiques – and scholars. More Social Media awareness will

⁹⁰ Q&A (n. 88); most importantly, in addition to Akande himself, Marko Milanović and subsequently James Sweeney then addressed the purported writer of the Q&A as follows: ‘I must say that I find it rather odd – even unprecedented – for the official spokesperson of the Court to engage in what is a proper academic debate with scholars like Dapo who have (rightly or wrongly) criticized the Court for the reasoning of its Bashir judgment. I frankly can’t remember ANY spokesperson of any international tribunal acting in that way. I’m not saying necessarily that this is inappropriate, but it is definitely unusual. So, bearing that in mind, could you please answer the following questions:

1) Was your comment on this blog post made in your official capacity as the spokesperson of the Court? Or is it your private view, in your own personal capacity, and if so shouldn’t you have said so?

2) Did you write that comment and the Q&A you referred to on your own initiative, or were you instructed to do so by someone else, e.g. the President of the Court?

[Sweeney’s comment:]

Marko’s point is spot on. Given that elements of the ‘Q&A’ are identical to the comment made here, we can infer that the Q&A is a lengthier reaction to Dapo’s OP.

With that in mind, I find the following elements of the Q&A quite extraordinary:

“Hastily made comments [...] may wholly misrepresent the decision or judgment.”

“Lawyers engaging in public commentary should exercise particular caution and remain mindful of the cardinal principles that guide the conduct of lawyers, including that of honesty, integrity and fairness.”

“There is an ethical obligation to reflect facts and circumstances accurately and fairly.”

Whether one agrees or not with Dapo’s critique of the reasoning of the Appeals Chamber (and I do; and have for a long time on this point generally) the suggestion that commentators making rapid assessments of available materials (and clearly labelling that assessment as provisional) somehow are acting unethically is absurd.

Therefore, for me, it is not just the novelty of the spokesperson commenting here and publishing the Q&A, but also the content of their comments that is profoundly troubling.’

⁹¹ Jacobs (n. 86), 623.

obviously be necessary in the future. At the end of September 2020, the Independent Expert Review Group of the International Criminal Court published its 348 pages final report to multiple International Criminal Court stakeholders where it also briefly touched on the impact of blogs when discussing professional ethics and increased quasi-transparency by new means of communications, thereby putting additional pressure on judges to resign or be disqualified.⁹² The net result was that

‘[s]uch events, whether truly inappropriate behaviour was involved or not, can impact the Court both externally and internally. The Court’s reputation, credibility and trust is eroded, risking lower support by States Parties and civil society. Internally, it can affect staff productivity and welfare, and in some instances can represent a financial risk for the institution. In absence of efficient and effective instruments on ethics and prevention of conflicts of interest, the Court is less able to defend itself against its critics’.⁹³

The consequences of these findings leave the observer with mixed feelings. Positive in the sense that increased accountability may ultimately prove an opportunity for the ICC to learn some lessons. Negative in the sense that, as nothing necessarily stays secret and that rumours about judges and other members of the court can spread like wildfires, it may deal yet another blow to its already tarnished reputation. In the age open defiance of the court by the US and challenges by African states, this would be the last thing the ICC needs.

IV. Conclusion

Twitter and the ‘Blogosphere’ are here to stay. Some Journals, academic associations or even individuals maintain their own blogs, and Twitter has established itself as the go-to platform to stay up to date, share one’s work, or even engage in (heated) debates, at times less about law than about politics.

Assuming the accusations of adopting extreme-relativist positions are correct, a ‘Fisherian’ point of view neither criticises nor endorses these develop-

⁹² Independent Expert Review of the International Criminal Court and the Rome Statute System, Final Report, 30 September 2020, para. 254, <<https://asp.icc-cpi.int>>:

‘Throughout the Experts’ consultations, ethics has been identified as an important topic for all stakeholders. Recent allegations of conflicts of interest, potential ethics violations or inappropriate behaviour from multiple Organs have been publicly covered and speculated upon through various articles and blog posts, and at times surfaced during trials through requests for disqualification of Judges.’

⁹³ Independent Expert Review (n. 92), para. 255.

ments in the digital sphere but rather simply condones them. Interpretive communities are naturally open to change, both when it comes to membership and their respective interpretive strategies.

For better or for worse, Social Media thus has the potential to transform and diversify international law academia. It has already supplemented traditional means of publishing and thereby opened membership in the interpretive community of international law and changed debates among scholars (and practitioners) to a significant degree. States, international organisations, or courts and tribunals face more open and immediate criticism by scholars than ever. Activist and academic stances become intermixed, interpretive communities within interpretive communities develop constantly.

Many of the fears from Social Media's early days have survived until this very day: It may indeed lead (or has already led?) to an inflation of (quasi-) academic production and opinions that could further contribute to the image of international law as an arbitrary and politicised science. Unequal distribution of scholarly influence can also be reflected in the size and reach of Social Media accounts. Academic discussions might end up divided into national, ideological, or regional filter bubbles. In the worst case, they are dominated by biases or *ad hominem* comments.

Be as it may, these negative trends are overshadowed by the benefits of Twitter and Blogs – even more so since they are also present in traditional academic exchanges. In the online realm, however, cooperation has never been easier, scholarship and the global international law debate club are more accessible than ever. The traditional guardrails become increasingly loose. Connecting and interacting with or reading from people you have never met and perhaps never will meet offline is one simple registration away. Those from the global south and with otherwise ‘non-Western’ perspectives in particular have countless possibilities to make themselves heard, at least if they are sufficiently active and well versed to be accepted by other members of international law's interpretive communities. In the Web 2.0, no part of the legal world needs to remain an undiscovered, mystical place.