TOWARDS THE NEXT "GROTIAN MOMENT": FORMING THE CONSENSUS ON CYBER SOVEREIGNTY THROUGH CUSTOMARY INTERNATIONAL LAW

By: Jiatai Zhang

Abstract:

The burgeoning advancements in information technology and cyberspace have prompted a global imperative for nations to engage in regulating the internet. These endeavors stand for an extension of traditional sovereignty principles, leveraging state authority for their implementation. Across the international landscape, nations are asserting varying degrees of sovereignty in cyberspace, reflecting diverse interpretations of the concept. This plurality underscores the multiple interests that different regimes prioritize in response to the challenges posed by internet technologies. However, this diversity of perspectives has engendered a proliferation of uncertainty within global cyber governance frameworks, impeding the coherent application of international law in cyberspace. Customary International Law (CIL) serves as a pivotal mechanism capable of transcending this hermeneutic variability in cyber governance. By institutionalizing the minimum consensus among states as a foundation for international norms, CIL offers a pathway to navigate the complexities surrounding the notion of cyber sovereignty and delineate the normative rights and obligations of states in the realm of international cyber governance. This paper aims to dissect the contemporary "Grotian Moment" concerning cyber sovereignty, a moment characterized by the rapid evolution of CIL about cyberspace. Through an analysis of influential international non-binding policy documents and the cyber governance

practices of key nations, the paper endeavors to illustrate the existence of a foundational consensus and behavioral norms governing cyber sovereignty within the international community. It interrogates whether the prevailing international consensus and state practices can catalyze the emergence of a new "Grotian Moment" in international law. In pursuit of expediting the realization of this customary law, the paper proposes a two-pronged strategy: first, the formulation of a binding declaration of principles by the United Nations, predicated on a foundational consensus regarding cyber sovereignty; and subsequently, the collaborative development of international internet norms by diverse nations based on their respective governance frameworks.

Keywords: Customary International Law; Cyber Sovereignty; Grotian Moment; Internet Governance

Contents:

INTRODUCTION

The internet transcends geographic boundaries, facilitating information and resource flow while challenging regulatory authorities. Early internet optimists predicted governments would "…have no sovereignty where we gather."[1] Yet, as the internet expands, regulators are trying to manage and constrain its development.

Major countries recognize the applicability of international law in cyberspace, based on State sovereignty and sovereign equality from the UN Charter. However, there's no consensus on how to apply international law in cyberspace. Different concepts of cyber sovereignty and varying internet management approaches undermine global governance. Current international law lacks a universal standard for interpreting cyber sovereignty.

While varied national positions on cyber sovereignty hinder codified norms, they help identify international customs. The "Grotian moment" describes the rapid formation of customary international law (CIL). New practices in emerging areas can quickly become international customs due to global consensus and changing environments.

This paper will begin by outlining the evolving landscape of cyberspace and the challenges posed by diverse national interpretations of cyber sovereignty. It will introduce the concept of cyber sovereignty and define its dual manifestations—both as an active exercise of state power and as a protective measure against external interference. The study will then examine how CIL is anticipated to form in cyberspace,

[1] John Perry Barlow, "A Declaration of the Independence of Cyberspace" (2019) 18:1 Duke Law & Technology Review 5.

focusing on emerging state practices and the development of *opinio juris*. Drawing on historical examples of rapid legal crystallization or "Grotian Moments," the paper will forecast how similar dynamics might shape international law in the digital era. It will also propose a future strategy, including a UN-led declaration and collaborative efforts among nations, to establish a binding framework that will guide cyber governance in an increasingly interconnected world.

By developing a consensus on cyber sovereignty through CIL, this study aims to predict a robust framework for regulating state conduct and ensuring that digital interactions are governed within a coherent legal structure. Such a framework is essential for safeguarding national security, fostering international stability, and upholding the rights and responsibilities of states as well as people in an increasingly interconnected world. Therefore, the research proposes a roadmap that may facilitate enhanced global cooperation and contribute to greater legal certainty in the digital age.

1. CYBER SOVEREIGNTY IN THE CONTEMPORARY WORLD

Traditional sovereignty denotes a state's supreme authority within territorial boundaries. However, the advent of ICT challenges these notions in cyberspace, where cyber sovereignty emerges. Diversified practices in internet sovereignty have caused fluctuations in countries' positions on internet governance.

1.1 Definition

The term "sovereignty" conveys a variety of meanings but generally refers to the supremacy of power within a state over other political entities.[2] Sovereignty, in its legal dimension, is the ability to set and enforce laws within a jurisdiction to achieve social control and goals.[3] The principle of sovereign equality in international relations confers on states the right to freely choose and develop their political, economic and cultural affairs while respecting their territorial integrity and political independence.[4] Transnational constraints, like UN sanctions and military actions, partially negate sovereignty by citing human rights and international peace as legal considerations, constituting legitimate interference.[5]

Cyber sovereignty, also referred to as internet sovereignty or network sovereignty, emphasizes the applicability of state sovereignty in cyberspace. Applying the concept of sovereignty to cyberspace can justify state control over the network.[6] The

---

[2] Daniel Philpott, "Sovereignty: An Introduction and Brief History" (1995) 48:2 J.Int'l Aff. 353. Also see Samantha Besson, "Sovereignty" (April 2011), online: <opil.ouplaw.com>.

[3] Jonathan Law, ed, *A Dictionary of Law*, Tenth edition. (Oxford, United Kingdom: Oxford University Press, 2022). DOI: <https://doi.org/10.1093/acref/9780192897497.001.0001>.

[4] *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UNGA, 25th Sess, UN Doc. A/RES/2625(XXV).

[5] Carrie Booth Walling, "Human Rights Norms, State Sovereignty and Humanitarian Intervention " (2015) 37:2 Hum Rts Q 383. DOI: <https://doi.org/10.1353/hrq.2015.003>.

[6] Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist" (2009) 64:1 AF L Rev 1 at 14. DOI:

information and communication technology (ICT)-based internet empowers users to cross traditional boundaries, leading the traditional definition of national sovereignty through territorial boundaries is greatly challenged in cyberspace.[7]

The 2013 United Nations Group of Governmental Experts report on Information and Telecommunication Technologies identifies "[i]nternational law, and in particular the Charter of the United Nations" as the fundamental norms that states should adhere to when engaging in information technology governance.[8] This report further clarifies that "[s]tate sovereignty and international norms and principles that flow from sovereignty" are equally applicable in the context of state regulation of ICTs.[9] The principle of sovereign equality, as a fundamental principle of the Charter of the United Nations, empowers states to conduct their domestic affairs autonomously.[10] A series of national consensus declarations affirms the reasonableness of the principle of national sovereignty in the governance of cyberspace.[11]

Principles of national sovereignty in cyberspace underpins the authority of states to regulate and protect digital domains within their territorial boundaries. This concept extends traditional notions of sovereignty to include the control over digital infrastructure, data flows, and online content. States exercise this sovereignty through legislative frameworks that govern cybersecurity, data protection, and the regulation of

---

<https://doi.org/10.4324/9781003344124-3>.

[7] Milton L. Mueller, “Against Sovereignty in Cyberspace” (2020) 22:4 Rev. Int'l Stud. 779. DOI: <https://doi.org/10.1093/isr/viz044>.

[8] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGA, 68th Sess, UN Doc. A/68/98 (2013) at 8.

[9] Ibid.

[10] *UN Charter*, 26 June 1945, Can TS 1945 No 7 at art 2.1.

[11] Sean Kanuck, "Sovereign Discourse on Cyber Conflict under International Law" (2010) 88:7 Tex L Rev 1571 at 1575. DOI: <https://doi.org/10.1177/09646639100190020506>.

cross-border cyber activities. In this context, national sovereignty not only empowers governments to combat cybercrime and espionage but also mandates the safeguarding of critical information infrastructures against external interference. Additionally, it facilitates the enforcement of domestic laws in the virtual realm, enabling states to maintain order and secure digital markets. However, the dynamic nature of cyberspace challenges the traditional applications of sovereignty, necessitating adaptive policies that balance state control with the inherently borderless nature of the internet.

Sovereignty is a combination of rights and obligations possessed by a state.[12] The internet blurs sovereignty boundaries, leading to conflicting jurisdictions and varying levels of state interference. States differ on cybercrime definitions and international responsibilities. While sovereign equality and respect for sovereignty are promoted for security and stability, the exercise of cyber sovereignty remains controversial and contradictory.

1.2 Application of Cyber Sovereignty

Diverse practices of cyber sovereignty have expanded its implementation. Different countries' approaches reveal various aspects of the concept, influenced by interests and strategies, leading to multiple variants in cyber governance.[13] These actions of exercising sovereignty in the process of network governance can be simply divided into two categories: active pursuit and passive response.[14]

In active pursuit, sovereignty reflects the ability of a state to proactively pursue

---

[12] Supra note 4.
[13] Anupam Chander & Haochen Sun, “Introduction: Sovereignty 2.0”, in Anupam Chander & Haochen Sun, ed, *Data Sovereignty: From the Digital Silk Road to the Return of the State*, (New York: Oxford University Press, 2023) at 7. DOI: <https://doi.org/10.1093/oso/9780197582794.003.0001>.
[14] Paul W. Kahn, "The Question of Sovereignty" (2004) 40:2 Stan J Int'l L 259 at 260.

specific purposes through its own behavior in governance.[15] This power lets states shape industry models, norms, and conduct for internet entities as they wish. Examples include the EU's Horizon 2020 and Horizon Europe programs,[16] which support technological progress through EU regulations, and China's Digital Silk Road, which enhances its internet industry and oversea construction through international cooperation.[17] South Africa's ICT and Digital Economy Action Programme outlines government roles in regulation, implementation, financing, and planning for economic development.[18]

Sovereignty could also be actively exercised to achieve non-economic purposes. The EU's General Data Protection Regulation (GDPR), implemented in 2018, imposes higher requirements on online services regarding data processing and the safeguarding of personal data rights. Due to the size of the EU market and the broad extraterritorial effect of GDPR regulations, the EU governance model is widely adhered to by internet participants in the international arena, allowing this sovereign act to evolve from EU legislation to a quasi-norm international governance.[19] Beyond defining modes of

---

[15] Robert H Jackson, *Quasi-States: Sovereignty, International Relations and the Third World*. (Cambridge: Cambridge University Press, 1991). at 27-9. DOI:<https://doi.org/10.1017/CBO9780511559020>. Also see Miriam Ronzoni, "Two conceptions of state sovereignty and their implications for global institutional design", (2012) 15:5 Critical Review of International Social and Political Philosophy 573 at 577. DOI:<doi.org/10.1017/CBO9780511559020>.

[16] EU, *Regulation* 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006 Text with EEA relevance, [2013] OJ L, 347/81. Also see EU, *Regulation* 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance) [2021] OJ L, 170/1.

[17] Marta Majcherczyk & Bai Shuqiang, "Digital Silk Road - The Role of Cross-Border E-Commerce in Facilitating Trade" (2019) 9:2 J WTO & China 106.

[18] South Africa, Department of Communications & Digital Technologies, *National Digital and Future Skills Strategy Originality, agility, critical thinking and problem-solving for digital inclusion* (2020).

[19] Annegret Bendiek & Magnus Römer, "Externalizing Europe: the global effects of European data

governance, state regulation of networks can also help fulfill socio-cultural purposes. In 2017, China implemented a cybersecurity law that empowers administrative authorities to advocate for online governance, guide online public opinion and require online users to comply with national laws and the vaguely worded "public order and social morality"[20].

Sovereignty in passive response represents the right of sovereign states not to suffer external interference and the obligation not to intervene in other states.[21] ICT advancements have lowered the cost of cross-border hostile actions, from espionage to physical attacks.[22] The US National Cybersecurity Strategy 2023 identifies threats like economic blackmail and technological espionage, emphasizing international collaboration and legal measures to address these issues.[23] Similarly, the EU is developing a cyber governance model with the NIS Directive and Cybersecurity Regulation to set security standards for private entities.[24]

Cyber fraud, theft, commercial espionage, disruption of hardware and software systems and invasion of privacy are some of the many destructive behaviors associated

protection" (2019) 21:1 Digital Policy, Regulation and Governance 32. DOI:<https://doi.org/10.1108/DPRG-07-2018-0038>.

[20] *Cybersecurity Law of People's Republic of China*, art 6,12.

[21] *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, UNGA, UN Doc.A/RES/2131(XX), (1965).

[22] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" (2012) 17:2 Journal of Conflict and Security 211 at 227. DOI:<https://doi.org/10.1093/jcsl/krs014>.

[23] United States, the White House, *National Cybersecurity Strategy* (2023) at 3-4.

[24] EU, *Regulation* 2023/2841 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, [2023] OJ L, 2023/2841, 18.12.2023. Also see EU, *Directive* 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [2022] OJ, L 333/80.

with cybercrime that can adversely affect a wide range of social actors.[25] Despite different perceptions of the nature of the offense, its elements, and jurisdictional scope, all states regard countering cybercrime as an important task in the field of criminal law in the age of the internet.[26] The UN Cybercrime Convention is a manifestation of this trend at the level of international law.[27]

Traditional sovereignty grants a state supreme authority to enforce laws within its territory and maintain equality in international relations. With the advent of ICT, cyber sovereignty has emerged, pushing state regulation into cyberspace. States now actively shape digital norms and governance models while also defending against external interference.

Establishing widely accepted standards in cyber sovereignty is key to creating clear, consistent cross-border governance frameworks. Such uniformity minimizes legal ambiguities, fosters international cooperation, and enables effective countermeasures against cyber threats—all while safeguarding individual rights. In turn, these standards enhance the interoperability of digital systems and balance national security with global information exchange. A cohesive regulatory environment bolsters trust, stability, and predictability in the cyber domain, paving the way for a secure and resilient digital future.

---

[25] Graeme R. Newman, "Cybercrime" in Marvin D. Krohn, Alan J. Lizotte & Gina Penly Hall (eds) *Handbook on Crime and Deviance,* (New York: Springer 2009). DOI:<https://doi.org/10.1007/978-1-4419-0245-0>.

[26] Jonathan Clough, "Cybercrime", (2011) 37:4 Commonwealth Law Bulletin 671 at 671-2. DOI:<https://doi.org/10.1080/03050718.2011.621277>.

[27] *Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, UNGA, 79th Sess, UN Doc. A/RES/79/243 (2024).

2. CUSTOMARY INTERNATIONAL LAW IN CYBER GOVERNANCE

In cyberspace, customary international law (CIL) can also evolve through two essential components: state practice and *opinio juris*. This section explores how diverse national actions and cautious expressions of legal obligation are reshaping customary norms in today's interconnected global environment.

2.1 Components of CIL in Cyber Governance

The translation of social customs into international legal norms requires certain prerequisites. A 2018 report from the International Law Commission summarizes two key elements of CIL: general practice and *opinio juris* (the opinion of law).[28] In the emerging cyberspace, both practice and *opinio juris* are undergoing transformation. Existing legislative efforts made in international arena are mostly commercial and not comprehensive.[29] Meanwhile, diverse state practices in governance create space for CIL, offering an alternative approach to applying international law in cyberspace.[30]

2.1.1 *State Practice in Cyber Governance*

State practice involving cyber governance is common and has been increasing as the internet expands exponentially. The proliferating practices of states and international organizations in governing various aspects such as the cyber economy, data protection, and cybercrime are crucial for determining customs related to cyber sovereignty.[31]

---

[28] *Identification of customary international law*, UNGA, UN Doc. A/RES/73/203 (2019) at 2.
[29] Warren B. Chik, "'Customary internet-ional law': Creating a body of customary law for cyberspace. Part 1: Developing rules for transitioning custom into law", (2010) 26:1 C.L.S.Rev. 3 at 14-5. DOI:<https://doi.org/10.1016/j.clsr.2009.11.005>.
[30] Gary Brown & Keira Poellet, "The Customary International Law of Cyberspace", (2012) 6:3 Strategic Studies Quarterly, 126 at 129.
[31] Paul Przemysław Polański, "Cyberspace: A new branch of international customary law?" (2017) 33 C.L.S.Rev 371 at 373. DOI: <https://doi.org/10.1016/j.clsr.2017.03.007>.

According to the ILC, state practice includes multiple forms of action by the sovereign in the executive, legislative, judicial, and other spheres, as well as, under specific circumstances, the sovereign's inaction.[32] Traditional state practice is often time-consuming and dominated by the sovereign, whereas in cyberspace it is not only instantaneous but also accompanied by many practices and regularities of previous non-state actors. Concurrently, cyber activities in virtual spaces are instantaneous and decentralized. While cyber technology facilitates the use of the internet by states to take measures or express their positions, it also creates challenges in determining state practice.

State practices contain regulation and governance of e-commercial activities in the cyber age. The norms adopted by domestic governance include both binding conventions and non-binding model laws and consensual international agreements.[33] While the World Trade Organization responds slowly into the regulation of e-commerce, the work programme on e-commerce under its sponsorship, and the model of state behavior derived from this programme, initially define the current policies of WTO members towards e-commerce.[34] In the domestic commercial sector, the states prefer to adopt uniform standards of behavior among private commercial entities to ensure information security and combat illegal content.[35] These internal rules of behavior stem from the general standards and customs of private individuals that have

[32] Supra note 30, at 3.
[33] UNCITRAL, *United Nations Convention on the Use of Electronic Communications in International Contracts*, (New York: 2007)
[34] WTO, *Work Programme on Electronic Commerce*, WTO Doc WT/L/274 (1998) online: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/274.pdf&Open=True>.
[35] Supra note 31 at 374.

arisen from the application of network technologies in commercial activities.[36]

On the other hand, state practice also includes those governance patterns in which the use of cybertechnology to commit crimes and invasions of privacy have been considered as cybercrime since the very beginning of the development of cyberspace and have been regulated through national legislation.[37] Due to the borderless nature of the internet, the potential supranational nature of cybercrime has similarly attracted the attention of sovereigns.[38] The Cybercrime Convention, developed under the leadership of the European Union and the United States, as well as the International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, currently in draft form within the United Nations framework and initiated mainly by developing countries, reflect the attributes of Western and non-Western models of cybercrime governance and state response.[39]

Surprisingly, some disreputable state practices in cyber governance also attest to the customary status of some malicious behavior. Due to the anonymity of the internet, it is rare to identify official participation or support in cyberattacks or espionage. Nevertheless, all countries prefer that others refrain from engaging in the same kind of malicious behavior that they have engaged in.[40] The disjunction between actual practices and stances has led to mutual accusations among states, further contributing

---

[36] Ibid.
[37] Martin Wasik, "The emergence of computer law", in Yvonne Jewkes & Majid Yar, ed, *Handbook of Internet Crime*, (Routledge: Milton Park, Abingdon, Oxon 2011) at 401-2. DOI:<https://doi.org/10.4324/9781843929338>.
[38] Michael McGuire, *Hypercrime: The New Geometry of Harm*, 1st ed (Routledge-Cavendish: London 2007). DOI:<https://doi.org/10.4324/9780203939529>.
[39] *Further revised draft text of the convention*, UNGA, UN Doc. A/AC.291/22/Rev.2 (2024).
[40] Supra note 29 at 141.

to the deadlock in rule formation and the continuation of practices involving cyber warfare.

Sovereigns' concerns about cyberspace insecurity and the risk of self-management by cyber entities contribute to the growth of state practice in the cyber age.[41] The dynamics generated by the paradigm of sovereignty to achieve effective control in various social spheres also incorporate cyber technology and encourage the continued expansion of state practices.

2.1.2 *Opinio Juris* in Cyber Governance

The legal nature of international custom derives from the sense of legal obligation that actors have concerning their practice. Prior crystallization of CIL indicates that *opinio juris* plays an important role in identifying whether a norm is CIL.

The expression of *opinio juris* in cyberspace has not increased proportionately with growing state practices but rather has stalled. Compared to the diversity of state practices, the expression of *opinio juris* tends to rely on official statements and declarations. While this feature facilitates the recognition of *opinio juris*, it also reinforces the caution of states in articulating their positions. The lack of *opinio juris* in cyber governance reflects this caution.[42] Numerous obstacles, such as technological inferiority, political conflicts, strategic considerations, or confidentiality requirements, can prevent states from taking a position.[43] So far, 30 countries have published national

[41] James A. Lewis, "Sovereignty and the Role of Government in Cyberspace" (2010) 16:2 Brown J World Aff. 55 at 63.
[42] Michael N. Schmitt & Sean Watts, "The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare" (2015) 50:2-3 Tex Int'l L J 189 at 230.
[43] Kubo Mačák, “From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers” (2017) 30 LJIL 877 at 881. DOI:<https://doi.org/10.1017/S0922156517000358>.

positions on cyber governance, including a position statement from the African Union.[44] National position statements address principles like sovereignty, non-intervention, and the applicability of international human rights and humanitarian law in cyberspace. While these statements represent *opinio juris*, few states have made their positions public.[45] Quasi-consensus exists in documents like the UN documents and the Tallinn Manual, which influence specific contexts and support broader national consensus. However, these non-binding documents are not official government expressions, lacking definitive status for *opinio juris*.

Determining the *opinio juris* of states on cyber governance remains challenging. Even among the few states that have disclosed their positions, there are disparities in understanding and standards applied. This reality highlights that constructing new CIL related to the internet through state practice and *opinio juris* still requires further contributions in interpreting and explaining national positions.[46]

2.2 Exercising CIL by Interpretation in Cyberspace

Applying CIL to cyber governance has been controversial. Some states interpret existing CIL to apply traditional principles to the internet. While this highlights the importance of established international law sources, traditional governance and legal customs are often criticized for their relevance in cyberspace.

Interpreting and applying CIL in the context of cyber governance is contentious.[47]

---

[44] Cooperative Cyber Defence Centre of Excellence, "List of articles" (last modified 11 July 2024) at part 5, online:< https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions>.
[45] Ann Väljataga, *Tracing opinio juris in National Cyber Security Strategy Documents* (Taillin: NATO Cooperative Cyber Defence Centre of Excellence, 2018).
[46] Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace" (2017) 42 Yale J Int'l L Online 1 at 20.
[47] Michael Schmitt & Liis Vihul, "The nature of international law cyber norms." (2014) NATO

In national position statements, states that invoke CIL rules to express their views follow a similar reasoning path: the existence of established customary rules in each subject area, combined with fact that cyber behaviors resemble the characteristics of that subject area, means that the relevant customary rules should also apply to those cyber behaviors. This trilogical interpretation implies the precondition that CIL can be applied to similar situations through interpretation.[48] Japan and the Netherlands, in their position papers, cite the customary law rule prohibiting infringement of sovereignty identified by the International Court of Justice in Nicaragua v. United States, arguing that attacks on critical infrastructure or interference in the normal performance of governmental functions through cyber means may constitute an infringement of sovereignty.[49] Instead of focusing on specific state practices or *opinio juris*, this approach emphasizes the historical importance of CIL for cyber behavior. States recognize the controversy due to divergent practices and social contexts. While the formation time for custom has been relaxed, state practice and general recognition remain key in determining the existence of a custom.[50]

Controversial approaches to interpreting CIL in cyberspace do not reject the application of customary rules entirely. When the attributes of cyber activities meet the requirements for applying a customary rule, the application of a particular rule stands

Cooperative Cyber Defence Centre of Excellence, The Tallinn Papers 5.

[48] Ori Pomson, "Methodology of identifying customary international law applicable to cyber activities", (2023) 36 LJIL 1023 at 1028. DOI:<https://doi.org/10.1017/S0922156523000390>.

[49] Japan, Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, (16 June 2021) at 2-3. Also see Netherlands, Government of the Kingdom of the Netherlands, *Appendix: International law in cyberspace*, (26 September 2019) at 1-3.

[50] North Sea Continental Shelf (Germany *v* Netherlands), [1969] ICJ Rep 4 at para 74.

alone, independent of any interpretative technique. This paradigm of applying customary law in cyberspace is evident in the field of international humanitarian law. For example, under the Geneva Conventions, medical units in armed conflict are always protected from attack if they do not violate their humanitarian purpose.[51] The International Humanitarian Law rules, which protect medical units from attack, regulate any act of destroying these units.[52] When a conflicting party obstructs the functioning of a medical unit through a cyberattack, this behavior constitutes a violation of the Geneva Conventions. This approach relies on the content and scope of a particular customary rule and therefore only addresses the cyber variant of a specific issue, failing to provide comprehensive behavioral norms for a broader range of cyber practices.

Complex state practices and unclear positions hinder the interpretation of customary law, and existing customary rules are limited in their application to cyber behavior. The elements of practice and consensus in cyberspace do not have an adequate basis in traditional patterns of the generation of customary international law.

---

[51] *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 12 August 1949, 75 UNTS 31 at art 19. [Geneva I]; *Geneva Convention relative to the Protection of Civilian Persons in Time of War*, 12 August 1949, 75 UNTS 287 at art 18. [Geneva IV]; *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*, 8 June 1977, 1125 UNTS 3 at art 11-2. [Protocol I].

[52] Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law Volume I: Rules*, (Cambridge University Press: Cambridge 2009) at 96. DOI:<https://doi.org/10.1017/CBO9780511804700>.

3. RAPID CRYSTALLIZATION OF CIL: IDENTIFYING "GROTIAN MOMENT"

Beyond the traditional patterns generated by customary international law, the "Grotian moment" offers a way forward. This concept refers to a specific instance of law-making where international rules, legal doctrines, and customary law can be rapidly established due to inadequate State practice and *opinio juris*, under conditions of significant changes in societies and rapid evolution of international governance paradigms.[53] The concept, although not formally recognized, has garnered increased attention in academic field.[54]

3.1 The Grotian Moment in History

Several academically recognized "Grotian Moments" can reflect dynamics of this concept. These four historical instances can be categorized into two types based on their origins.[55]

3.1.1 By Judicial Bodies

International courts and tribunals primarily identify and recognize CIL. The establishment of the international war tribunals after World War II, as well as the International Criminal Tribunal for the Former Yugoslavia reveal the importance of international judicial bodies in a Grotian Moment.[56]

The Charter of the International Military Tribunal, which served as the basis for the Nuremberg Trials, is now recognized as a source of customary law regarding

---

[53] Michael P. Scharf, "Seizing the Grotian Moment: Accelerated Formation of Customary International Law in Times of Fundamental Change" (2010) 43:3 Cornell Int'l LJ 439 at 440.

[54] Burns H. Weston, et al., *International Law and World Order: A Problem-Oriented Coursebook*, 3rd ed, (West Academic Publishing: St. Paul 1997) at 1369.

[55] Milena Sterio, "Grotian Moments and Statehood" (2022) 54 Case W Res J Int'l L 71 at 74.

[56] Frédéric Mégret, "The 'Grotian Style' in International Criminal Justice", (2021) 42 Grotiana 304.

accountability for international crimes.[57] The Nuremberg Charter, which enabled accountability for international crimes despite no prior state practice or *opinio juris*, has since been acknowledged as a source of customary law. Shortly after, the Tokyo Charter, which provided the foundation for the International Military Tribunal for the Far East, was also established.[58] Following the Nuremberg Trials, United Nations Resolution 95/I unanimously affirmed the principles of international law enshrined in the Charter, thereby forming the basis for *opinio juris* among United Nations members.[59] The UN Secretary-General's interpretation of the second natural paragraph of UNSC Resolution 808, included the Charter of the International Military Tribunal as part of CIL.[60] The rapid formation of international customary law in this field facilitated by the emerging *opinion juris*, bypassing traditional State practice.

The ICTY marked another Grotian moment in the accountability for individual crimes. Although the UN Charter does not explicitly grant the power to establish international tribunals, the Security Council's resolution established the ICTY, demonstrating a departure from existing precedents and relatively weak *opinio juris*.[61] Statute of the International Criminal Tribunal for the former Yugoslavia, adopted by the Security Council in Resolution 827,[62] contributed to the evolution of CIL in the

---

[57] *The Charter and judgment of the Nürnberg Tribunal : history and analysis: memorandum / submitted by the Secretary-General*, UNGA & International Law Commission, 1949, UN Doc. A/CN.4/5.
[58] *Charter of the International Military Tribunal for the Far East,* 26 April 1946, Treaties and Other International Acts Series 1589.
[59] *Affirmation of the Principles of International Law Recognized by the Charter of The Nürnberg Tribunal*, UNGA, 11 December 1946, UN Doc. A/RES/95(I).
[60] *Report of the Secretary-General pursuant to paragraph 2 of Security Council resolution 808*, UNSG, UN Doc. S/25704 (1993) at para 42-4.
[61] Ibid, at para 22.
[62] *Resolution 827*, UNSC, 3217th meeting, 1993, UN Doc S/RES/827.

realm of international ad hoc tribunals, expanding customary international humanitarian law to cover both domestic and international spheres and serving as a precedent for the creation of the Special Tribunal for Rwanda and its Statute.

Grotian moments are mainly observed by judicial bodies in international humanitarian law, often set against the backdrop of serious and urgent humanitarian crises.[63] These situations necessitate rapid responses and rely on the *opinio juris* of States to formulate rules in the absence of legal foundations and precedents.

3.1.2 By Countries

Spatial and socio-economic changes can also trigger a Grotian moment. Unlike court-based practices, Grotian moments resulting from extra-legal factors typically manifest as inter-State consensus and often culminate in international conventions or agreements with a broader scope.[64]

Expansive interpretations of sovereignty adopted by a single State because of scientific and technological developments can be rapidly accepted as international custom.[65] In September 1945, the United States claimed its ownership of the resources of its continental shelf. Prior discussions on seabed jurisdiction had been limited and regarded only as exceptions rather than constituting new rules. The national position of the U.S. was based on advances in drilling technology and the marine scientific research capabilities. In the decade following this claim, numerous countries followed suit,

[63] Boutros Boutros-Ghali, "A Grotian Moment" (1994) 18:5 Fordham Int'l L.J. 1609 at 1616.
[64] Omri Sender & Michael Wood, "Between 'Time Immemorial' and 'Instant Custom': The Time Element in Customary International Law" (2021) 42 Grotiana 229.
[65] Snjólaug Árnadóttir, "Emerging State Practice on Maritime Limits: A Grotian Moment Unveiling a Hidden Truth?" (2023) 44 Grotiana 4.

prompting the International Law Commission (ILC) to prioritize continental shelf legislation. This eventually led to the 1958 Convention on the Continental Shelf and the United Nations Convention on the Law of the Sea. Despite the involvement of many states, H. Lauterpacht argued that the U.S. stance significantly influenced the evolution of continental shelf norms into CIL.[66] The U.S. position shaped the global understanding and application of the continental shelf concept and influenced maritime jurisdiction guidelines.[67]

For norms of behavior in an entirely new international space, the United Nations can provide the institutional basis for consensus-building to accelerate the formation of international customs. From 1957 to 1963, only the U.S. and the Soviet Union had the capability to launch artificial satellites and conduct human spaceflights. In 1963, the UN General Assembly adopted the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, providing basic consensus for peaceful exploration of outer space. While this declaration was not binding and was not cited by judicial bodies, it was recognized by the UN General Assembly as a source of principles of statutory law principles.[68] The emergence of outer space law illustrates the gradual process of legal principles gaining *opinio juris* through international practice. Given the limited State practice, UN member states were able to quickly establish CIL by generating *opinio juris* at the international level

---

[66] Hersch Lauterpacht, "Sovereignty over Submarine Areas" (1950) 27 Brti YB Int'l L 376 at 394.
[67] Michael P. Scharf, *Customary International Law in Times of Fundamental Change: Recognizing Grotian Moments*, 1st ed, (Cambridge University Press: Cambridge 2013) at 122. DOI:<https://doi.org/10.1017/CBO9781139649407>.
[68] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 21st Sess, UNGA, 1967, UN Doc A/RES/2222(XXI).

through consensus.

The Grotian moment in history reveals its complexities. There is no fixed pattern to the socio-historical context and legal elements that constitute new customary rules. Creating challenges in identifying new Grotian moments.

3.2 Conditions for Forging the Grotian Moment

Analyzing historical cases of rapid customary rule formation reveals new Grotian moments. These rules arise from swift changes in social or technological conditions and the quick emergence of universal *opinio juris*.[69]

Four recognized Grotian Moments reveal an interesting distinction between international judicial institutions, which play a leading role in the generation of customary law at a time of dramatic changes in socio-political factors, and inter-state consensus mechanisms, represented by the United Nations, which play a leading role in the generation of customary law at a time of changes in non-social, natural factors.[70]

These historical moments also demonstrate the important role of *opinio juris* in the formation of customary law. The Nuremberg Charter, established by the victorious World War II nations, was recognized through unanimous UN General Assembly resolutions. The ICTY similarly relied on unanimous Security Council resolutions to establish norms for war crimes trials. These principles were applied before any extensive State practice existed. Continental shelf principles and outer space norms of conduct also rely on a rapidly emerging consensus among States and United Nations

[69] Michael P. Scharf, "Hugo Grotius and the Concept of Grotian Moments in International Law" (2022) 54 Case W Res J Int'l L 17.
[70] Supra note 55.

resolutions. While there were instances of State practice regarding the continental shelf and outer space (e.g., U.S. mining and space missions by the U.S. and Soviet Union), they were not sufficiently extensive or enduring to constitute customary law. It is obvious that in a Grotian Moment, the value of state practice under customary law is of a lower order than *opinio juris*.

Resolutions and declarations within the United Nations structure were the primary sources of *opinio juris* during the Grotian moments.[71] Besides international judicial bodies such as international courts and tribunals, *opinio juris* can also be established by the United Nations. Three of the four historical events accelerating the crystallization of CIL mentioned above were directly based on consensus in United Nations General Assembly and Security Council resolution or declarations. Prior to the formation of the Convention on the Continental Shelf and the United Nations Convention on the Law of the Sea, the principle of the continental shelf though not yet codified by a United Nations resolution, implied widespread acceptance among United Nations member States.[72]

In summary, a Grotian moment in history necessitates the emergence of a rapidly evolving customary international law rule, triggered by an unprecedented social event or the establishment of a new international domain. This rule is further shaped by the formation of inter-State *opinio juris*, often through United Nations resolutions or declarations. The role of State practice in this process is secondary.

---

[71] Milena Sterio, "Humanitarian Intervention Post-Syria: A Grotian Moment?" (2014) 20:2 ILSA J Int'l & Comp L 343.

[72] Lorenzo Gasbarri, "(Meta) Grotian Moment: International Organizations and the Rapid Formation of Customary International Law" (2022) 43 Grotiana 113.

4. CHASING THE CHARACTERISTICS OF THE "GROTIAN MOMENT" IN CYBER SOVEREIGNTY

Predicting a Grotian moment is more complex than identifying it historically, as future predictions involve speculation and assumptions. Past conditions offer a framework for making such predictions more plausible and provide guidelines for policymakers aiming to foster the rapid development of CIL. While creating international law rules is challenging and traditional CIL development is reluctant, identifying a Grotian moment in cyber sovereignty could help regulate state actions in cyberspace through international law.

4.1 New External Conditions in Cyber Sovereignty

As a recently created international space, the internet has brought revolutionary changes to human civilization, impacting every aspect of society. To predict the Grotian moment, it is essential to recognize that cyberspace is novel to state sovereignty and that there is a need for legal rules concerning sovereignty within it.

While there has been some legal practice of transnational cyber governance, state sovereignty in the cyber world remains amid disordered international governance.[73] ICTs, particularly internet technologies, challenge the application of traditional sovereignty components in cyberspace. A widely cited constructivist approach considers population, territory, authority and national recognition as the four constituent elements of a sovereign state.[74] This combination of components can be

[73] Supra note 46.
[74] Michael Ross Fowler & Julie Marie Bunck, "What Constitutes the Sovereign State?", (1996) 22:4 Rev. Int'l Stud at 381. DOI:< https://doi.org/10.1017/S0260210500118637>.

seen in the formation of the Principles on the Continental Shelf and the Legal Principles on Outer Space. By interpreting the continental shelf as a natural extension of a state's geographical territory, its nature shifted from being a new international space to national territory, thus applying traditional rules of sovereignty along with the other parts of the territory. On the other hand, outer space could hardly fulfill any of the four elements, and the 1963 Declaration of Legal Principles rejected the application of the concept of sovereignty in outer space.

The features of internet technology complicate the determination of sovereignty.[75] While most network participants belong to different states in terms of population, the anonymity of the technology allows a significant number of internet users to operate without being limited by their identity. For the state, network participants are only subject to jurisdiction when their behavior interferes with the real order. Anonymous users in cyberspace do not constitute a national population. The greatest technical challenge to sovereignty posed by cybertechnology, as noted earlier, is borderlessness. While managing physical equipment and infrastructure is a power of the state by virtue over its traditional sovereignty, control of equipment does not imply the establishment of substantive boundaries on network activity and data. States cannot exercise effective control over each part of the network.[76] Any cyber behavior across traditional borders is possible if internet service itself is not cut off. The decentralized and fragmented governance of network activities makes it difficult for authorities to monopolize on

[75] Michael N. Schmitt & Liis Vihul, "Respect for Sovereignty in Cyberspace" (2017) 95:7 Tex L Rev 1639.
[76] Noam Neuman, "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality" (2021) 97 INT'L L. STUD. 765.

regulation. The formation of technical standards and network community norms often depends on the common practices of all network participants, with state constraints on the network accounting for only a small part of the equation. Therefore, the traditional concept of sovereignty is not directly applicable to the internet. In terms of sovereignty, cyberspace represents an entirely new international space.

Effective governance of cyberspace requires sovereign rules.[77] Unlike outer space, cyberspace directly impacts both international relations and state-citizen interactions. Cyberattacks and state regulation of internet content interfere with other states' sovereignty and affect citizens' rights and obligations. As a fundamental principle guiding the exercise of state power and delineating the boundaries of public authority, the principle of sovereignty retains significant normative value in the digital era. The establishment of a sovereignty principle broadly accepted by the international community would contribute to reconciling diverse and fragmented national positions and behaviors in cyberspace, thereby promoting convergence and normative order at the international level.

4.2 Identifying *Opinio Juris* on Cyber Sovereignty

The rapid emergence of *opinio juris* is a central component of the Grotian moment. Recognition by states of international legal rules in the internet age and the creation of a sense of legal obligation require an objective carrier. National position statements, academic perspectives with an official background, and documents from international

[77] Guiguo Wang, "Are There International Rules Governing Cyberspace?" (2021) 8:2 J Int'l & Comp L 357.

organizations form the basis of the current common *opinio juris* on cyber sovereignty between states.

4.2.1 National Position Statements

Countries and interstate organizations that express their positions on cyber sovereignty are not the majority in the international community. However, these countries, due to their technological capabilities, market size and international influence, have enabled their cyber activities and practices to impact the development of the internet and the formation of norms. The understanding of cyber sovereignty encompasses both the protection of sovereignty and the exercise and limitation of sovereignty.

States protect their sovereignty by defining what kind of cyber behavior violates the principle of sovereignty. The most cited violation is an attack on infrastructure.[78] This understanding extends traditional territorial sovereignty, treating cyber infrastructure within the territory as a physical part protected by the state's sovereignty. Cyberattacks on the normal functioning of governments are also cited as violations of sovereignty, as they jeopardize normal economic, political, and cultural management activities. Beyond traditional sovereignty, some states consider that a cyber operation with serious consequences violates sovereignty even if the operation occurs entirely in cyberspace.[79] The more radical position asserts that no cyber operations from other states may occur within a state's cyberspace without consent. Conversely, the milder position recognizes that under certain conditions, cyber operations infringe on

[78] Cooperative Cyber Defence Centre of Excellence, "Sovereignty" (last modified 17 June 2024) at part 5, online:<https://cyberlaw.ccdcoe.org/wiki/Sovereignty> at part 2.1, 2.3, 2.6, 2.15.
[79] Ibid, at 2.16

sovereignty but argues that not all unauthorized cyber activities are wrongful.[80]

The exercise of sovereignty involves the state's ability to participate in governance in cyberspace. The power to legislate and legally bind network users and infrastructures under sovereign jurisdiction and to advocate for technical norms consistent with security objectives is seen by some states as the embodiment of internal sovereignty in network governance. Beyond legal norms, internal sovereignty also underpins policies for internet industry development.[81] The exercise of sovereignty in cyberspace is constrained by treaty obligations, rules of CIL and general principles of law. International human rights and humanitarian law norms are key binding constraints on sovereignty, limiting its overreach in internal governance and external communication.[82]

Expressions of national positions on sovereignty in cyberspace include both traditional and cyber-age characteristics. Cyberattacks on infrastructure, people, and government functions are understood to constitute a violation of sovereignty based on the principle of territorial sovereignty. Some states advocate for a legitimate presence in extraterritorial cyberspace for innocuous or minor cyber behavior, reflecting the transformation of sovereignty by the borderlessness and anonymity of cyberspace.

4.2.2 Tallinn Manual

The Tallinn Manual, initially focused on cyberattacks, has expanded in its second edition to cover a broader range of international cyber behaviors. NATO included non-

[80] Ibid, at 2.9, 2.20, 2.30.
[81] Ibid, at 2.9.
[82] Ibid, at 2.37.

NATO experts to reduce Western bias. While it remains an academic resource without official recognition, countries like Canada, Germany, and the Netherlands have endorsed its criteria for defining sovereignty violations. The Manual is valuable for countries with scholars or institutions engaged in its research.

The Tallinn Manual follows the traditional approach of defining cyber sovereignty based on territorial considerations.[83] States may exercise sovereignty over cyber infrastructure and activities within their territorial boundaries and under special conditions, over facilities and activities outside their territory. Due to cyberspace's decentralized nature, experts have ruled out categorizing it as globally common, like outer space. However, they found that states cannot claim sovereignty over cyberspace itself.[84] The Manual focuses on cyber infrastructure under the state's absolute control as central to cyber sovereignty.

Regarding the exercise of sovereignty in cyberspace, states have the power to take necessary measures concerning infrastructure and individuals participating in cyber activities within their territory and to engage equally in international cyber governance. Internally, sovereignty involves controlling infrastructure, while at the cyber-logical level, states can require specific internet protocols or cryptographic certificates.[85] At the cyber-social level, states can regulate participants in cyber activities. States must ensure their territories are not used for cyber-attacks against other states. Externally, sovereignty empowers states to govern cybercrime without external interference,

---

[83] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017) at 11. DOI:<https://doi.org/10.1017/9781316822524>.
[84] Ibid, at 13.
[85] Ibid, at 13-7.

allowing them to join international cybercrime treaties or state their positions without coercion. Both internal and external sovereignty are bound by international human rights and humanitarian law treaties, the rules of customary law, and general principles of law.

The Tallinn Manual focuses on cyber violations of sovereignty, considering only infringements resulting from a state's cyber behavior as violations. An act may lead to a sovereignty breach if it can be traced back to a state. The injured parties are the state itself, persons, or entities within the state's territory. The panel debated cyber-espionage, with many scholars viewing it as a violation, while realist scholars argue it is tacitly tolerated. Breaches of sovereignty are divided into substantive breaches and attacks on authority. Substantive breaches involve remote cyber behavior causing physical damage or dysfunction, such as damage to network equipment or interference in critical facilities. Attacks on authority damage government functions.

The Tallinn Manual consolidates the consensus of scholars from major internet-participating countries, defining state sovereignty in cyberspace without departing from the existing sovereignty framework while adapting to cyber technology's characteristics.

4.2.3 Documents of United Nations

Currently, two consensus-building bodies in the United Nations address cyberspace governance: namely the Group of Governmental Experts (GGE) and the Open-ended Working Group (OWEG). Both are part of the UN Office for Disarmament Affairs, but their membership scope differs; the GGE limits participation to specific countries, while

the OEWG is open to all UN member states. Both bodies address the application of sovereignty in their cyber governance reports.

The GGE has produced four reports: the 2010 report did not mention sovereignty; the 2013 report first acknowledged sovereignty in the context of cyber activities, but only at the macro level, without specific issues. The 2015 report refined the application of sovereignty, identifying states' responsibility to mitigate cyberattacks from their territory as an obligation to respect other states' sovereignty.[86] The 2021 report further clarified national jurisdiction over network facilities and highlighted ICT technology infrastructure.[87] Though specific rules remain unclear, the consensus on sovereignty in cyber activities in the working report, indicates governmental recognition of the concept. The norms suggested could serve as evidence of *opinio juris* for customary law.

The OEWG's work aligns with the 2015 GGE report but does not further describe sovereignty in networks. The 2021 final report only considers attacks on cyber infrastructure with serious consequences as breaches of state sovereignty.[88] These UN mechanisms, reflecting consensus among many states, incorporate rules and principles of sovereignty as international legal norms for cyber activities. Although documents

---

[86] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General*, UNGA, 70th Sess, UN Doc. A/70/174 (2015) at 8.

[87] *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: note / by the Secretary-General*, UNGA, 76th Sess, UN Doc. A/76/135 (2021) at 17.

[88] *Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report*, UNGA, UN Doc. A/AC.290/2021/CRP.2 (2021) at 4.

from international organizations do not directly constitute customary law, they can serve as evidence of an *opinio juris* and contribute to the formation of customary law.

This section examines the complexities of predicting a Grotian moment in cyber sovereignty. It highlights how cyberspace's borderless nature creates new external conditions that challenge traditional state sovereignty. The discussion further identifies *opinio juris* through national position statements, the Tallinn Manual, and UN documents, underscoring their role in shaping emerging customary international law.

5. CONCLUSION: TOWARDS THE NEXT "GROTIAN MOMENT"

Meeting the described conditions does not automatically lead to a Grotian moment. A specific international event is needed to formally express the rapid emergence of a customary law rule. Historically, such principles have been codified through General Assembly resolutions, international treaties, or legal interpretations. For cyber sovereignty, a UN General Assembly resolution declaring binding legal principles would be the most favorable route for its rapid crystallization into customary international law.

Customary rules on cyber sovereignty should include three key elements about the current *opinio juris*. First, the traditional concept of territorial sovereignty should apply to parts of cyberspace. Despite cyberspace's borderlessness and anonymity, its infrastructure and participants are physically found in real-world territories, emphasizing the importance of cyber infrastructure among States. Applying territorial sovereignty can help hold States accountable and impose international law constraints on their cyber behavior. Second, acknowledge the modification of sovereignty in cyberspace due to its unique features and adjust the threshold for sovereign interference. While traditional territorial rules consider unauthorized exercise of power as a sovereignty violation, cyberspace's lack of clear borders and instantaneous actions suggest that minimal cyber activities, like accessing publicly available information, might not constitute interference. Lastly, recognize that international human rights and humanitarian law, along with other treaties, customs, and principles, apply to state sovereignty in cyberspace.

This study does not claim the emergence of a new Grotian moment, as customary rules only become established law upon explicit recognition. Given the challenges in forming statutory norms and customary law for cyberspace, the study suggests that current cyber sovereignty rules meet the conditions for a Grotian moment based on previous CIL developments. The proposed solution is to leverage rapidly crystallizing CIL to achieve international law governance of state behavior in cyberspace. Drawing on past examples, States could use customary law as a foundation for creating codified cyber governance laws, enhancing international regulation of state cyber activities.

Bibliography

Legislation: International

- *UN Charter*, 26 June 1945, Can TS 1945 No 7.
- *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 12 August 1949, 75 UNTS 31. [Geneva I];
- *Geneva Convention relative to the Protection of Civilian Persons in Time of War*, 12 August 1949, 75 UNTS 287. [Geneva IV];
- *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*, 8 June 1977, 1125 UNTS 3. [Protocol I].
- *Charter of the International Military Tribunal for the Far East*, 26 April 1946, Treaties and Other International Acts Series 1589.

Legislation: Foreign

- China P.R., *Cybersecurity Law of People's Republic of China*, art 6,12.
- EU, *Regulation* 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006 Text with EEA relevance, [2013] OJ L, 347/81.
- EU, *Regulation* 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and

dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance) [2021] OJ L, 170/1.

- EU, *Regulation* 2023/2841 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, [2023] OJ L, 2023/2841, 18.12.2023.
- EU, *Directive* 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [2022] OJ, L 333/80.

Jurisprudence

- *North Sea Continental Shelf (Germany v Netherlands)*, [1969] ICJ Rep 4.

Secondary Material: Monographs

- Chander, Anupam & Haochen Sun, *Data Sovereignty: From the Digital Silk Road to the Return of the State*, 1st ed (New York: Oxford University Press, 2023).
- Jackson, Robert H, *Quasi-States: Sovereignty, International Relations and the Third World*. 1st ed (Cambridge: Cambridge University Press, 1991).
- Henckaerts, Jean-Marie & Louise Doswald-Beck, *Customary International Humanitarian Law Volume I: Rules*, 1st ed (Cambridge University Press: Cambridge 2009).

- Jewkes, Yvonne & Majid Yar, *Handbook of Internet Crime*, 1st ed (Routledge: Milton Park, Abingdon, Oxon 2011).
- Krohn, Marvin D., Alan J. Lizotte & Gina Penly Hall et al, *Handbook on Crime and Deviance*, 1st ed (New York: Springer 2009).
- Law, Jonathan, *A Dictionary of Law*, 10th ed (Oxford, United Kingdom: Oxford University Press, 2022).
- McGuire, Michael, *Hypercrime: The New Geometry of Harm*, 1st ed (Routledge-Cavendish: London 2007).
- Scharf, Michael P., *Customary International Law in Times of Fundamental Change: Recognizing Grotian Moments*, 1st ed, (Cambridge University Press: Cambridge 2013).
- Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017)
- Weston, Burns H., et al., *International Law and World Order: A Problem-Oriented Coursebook*, 3rd ed, (West Academic Publishing: St. Paul 1997).

Secondary Material: Articles

- Árnadóttir, Snjólaug, "Emerging State Practice on Maritime Limits: A Grotian Moment Unveiling a Hidden Truth?" (2023) 44 Grotiana 4.
- Barlow, John Perry, "A Declaration of the Independence of Cyberspace" (2019) 18:1 Duke Law & Technology Review 5.
- Bendiek, Annegret & Magnus Römer, "Externalizing Europe: the global effects of European data protection" (2019) 21:1 Digital Policy, Regulation and

Governance 32.

- Boutros-Ghali, Boutros, “A Grotian Moment” (1994) 18:5 Fordham Int'l L.J. 1609.
- Brown, Gary & Keira Poellet, “The Customary International Law of Cyberspace”, (2012) 6:3 Strategic Studies Quarterly, 126
- Buchan, Russell, “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?” (2012) 17:2 Journal of Conflict and Security 211.
- Chik, Warren B., “‘Customary internet-ional law’: Creating a body of customary law for cyberspace. Part 1: Developing rules for transitioning custom into law” (2010) 26:1 C.L.S. Rev. 3.
- Clough, Jonathan, “Cybercrime” (2011) 37:4 Commonwealth Law Bulletin 671.
- Fowler, Michael Ross & Julie Marie Bunck, “What Constitutes the Sovereign State?”, (1996) 22:4 Rev. Int'l Stud 381.
- Franzese, Patrick W., "Sovereignty in Cyberspace: Can It Exist" (2009) 64:1 AF L Rev 1.
- Gasbarri, Lorenzo, “(Meta) Grotian Moment: International Organizations and the Rapid Formation of Customary International Law” (2022) 43 Grotiana 113.
- Kahn, Paul W., "The Question of Sovereignty" (2004) 40:2 Stan J Int'l L 259.
- Kanuck, Sean, "Sovereign Discourse on Cyber Conflict under International Law" (2010) 88:7 Tex L Rev 1571.
- Lauterpacht, Hersch, "Sovereignty over Submarine Areas" (1950) 27 Brti YB Int'l L 376.

- Lewis, James A., "Sovereignty and the Role of Government in Cyberspace" (2010) 16:2 Brown J World Aff. 55.
- Mačák, Kubo, "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers" (2017) 30 LJIL 877.
- Majcherczyk, Marta & Bai Shuqiang, "Digital Silk Road - The Role of Cross-Border E-Commerce in Facilitating Trade" (2019) 9:2 J WTO & China 106.
- Mégret, Frédéric, "The 'Grotian Style' in International Criminal Justice", (2021) 42 Grotiana 304.
- Mueller, Milton L., "Against Sovereignty in Cyberspace" (2020) 22:4 Rev. Int'l Stud. 779.
- Neuman, Noam, "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality" (2021) 97 INT'L L. STUD. 765.
- Philpott, Daniel, "Sovereignty: An Introduction and Brief History" (1995) 48:2 J.Int'l Aff. 353.
- Polański, Paul Przemysław, "Cyberspace: A new branch of international customary law?" (2017) 33 C.L.S.Rev 371.
- Pomson, Ori, "Methodology of identifying customary international law applicable to cyber activities"(2023) 36 LJIL 1023.
- Ronzoni, Miriam, "Two conceptions of state sovereignty and their implications for global institutional design" (2012) 15:5 Critical Review of International Social and Political Philosophy 573.
- Scharf, Michael P., "Seizing the Grotian Moment: Accelerated Formation of

Customary International Law in Times of Fundamental Change" (2010) 43:3 Cornell Int'l LJ 439.

- Scharf, Michael P. "Hugo Grotius and the Concept of Grotian Moments in International Law" (2022) 54 Case W Res J Int'l L 17.
- Schmitt, Michael, "Grey Zones in the International Law of Cyberspace" (2017) 42 Yale J Int'l L Online 1.
- Schmitt, Michael & Sean Watts, "The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare" (2015) 50:2-3 Tex Int'l L J 189.
- Schmitt, Michael & Liis Vihul, "Respect for Sovereignty in Cyberspace" (2017) 95:7 Tex L Rev 1639.
- Sender, Omri & Michael Wood, "Between 'Time Immemorial' and 'Instant Custom': The Time Element in Customary International Law" (2021) 42 Grotiana 229.
- Sterio, Milena, "Humanitarian Intervention Post-Syria: A Grotian Moment?" (2014) 20:2 ILSA J Int'l & Comp L 343.
- Sterio, Milena, "Grotian Moments and Statehood" (2022) 54 Case W Res J Int'l L 71.
- Walling, Carrie Booth, "Human Rights Norms, State Sovereignty and Humanitarian Intervention" (2015) 37:2 Hum Rts Q 383.
- Wang, Guiguo, "Are There International Rules Governing Cyberspace?" (2021) 8:2 J Int'l & Comp L 357.

Other Materials: International Documents

- UNCITRAL, *United Nations Convention on the Use of Electronic Communications in International Contracts*, (New York: 2007).
- UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, 25th Sess, UN Doc. A/RES/2625(XXV).
- UNGA, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, UN Doc.A/RES/2131(XX), (1965).
- UNGA, *Identification of customary international law*, UN Doc. A/RES/73/203 (2019) at 2.
- UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 68th Sess, UN Doc. A/68/98 (2013) at 8.
- UNGA, *Further revised draft text of the convention*, UN Doc. A/AC.291/22/Rev.2 (2024).
- UNGA & International Law Commission, *The Charter and judgment of the Nürnberg Tribunal : history and analysis: memorandum / submitted by the Secretary-General*, 1949, UN Doc. A/CN.4/5.
- UNGA, *Affirmation of the Principles of International Law Recognized by the Charter of The Nürnberg Tribunal*, 11 December 1946, UN Doc. A/RES/95(I).
- UNGA, *Treaty on Principles Governing the Activities of States in the*

Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 21st Sess, 1967, UN Doc A/RES/2222(XXI).

- UNGA, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General*, 70th Sess, UN Doc. A/70/174 (2015) at 8.
- UNGA, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: note / by the Secretary-General*, 76th Sess, UN Doc. A/76/135 (2021) at 17.
- UNGA, *Open-ended working group on developments in the field of information and telecommunications*
- *in the context of international security Final Substantive Report*, UN Doc. A/AC.290/2021/CRP.2 (2021) at 4.
- UNSC, *Resolution 827*, 3217th meeting, 1993, UN Doc S/RES/827.
- UNSG, *Report of the Secretary-General pursuant to paragraph 2 of Security Council resolution 808*, UN Doc. S/25704 (1993) at para 42-4.
- WTO, *Work Programme on Electronic Commerce*, WTO Doc WT/L/274 (1998).

Other Materials: Foreign Documents

- Japan, Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations,* (16 June 2021).
- Netherlands, Government of the Kingdom of the Netherlands, *Appendix: International law in cyberspace*, (26 September 2019).

- South Africa, Department of Communications & Digital Technologies, *National Digital and Future Skills Strategy Originality, agility, critical thinking and problem-solving for digital inclusion* (2020).
- United States, the White House, *National Cybersecurity Strategy* (2023).

Other Materials: Online Resources

- Besson, Samantha, "Sovereignty" (April 2011), online: <opil.ouplaw.com>.
- Cooperative Cyber Defence Centre of Excellence, "List of articles" (last modified 11 July 2024) at part 5, online:< https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions>.
- Cooperative Cyber Defence Centre of Excellence, "Sovereignty" (last modified 17 June 2024) at part 5, online:<https://cyberlaw.ccdcoe.org/wiki/Sovereignty> at part 2.1, 2.3, 2.6, 2.15.
- Schmitt, Michael & Liis Vihul, "The nature of international law cyber norms." (2014) NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Papers 5.
- Väljataga, Ann, Tracing opinio juris in National Cyber Security Strategy Documents (Taillin: NATO Cooperative Cyber Defence Centre of Excellence, 2018).