1

Does International Law Matter in Cyberspace?

We all know that international law matters in the real world, but if and how it matters in the cyber world is an open question. Does international law matter in cyberspace? International law, and in particular the Charter of the United Nations, are the backbone of international relations and are crucial for maintaining international peace and security. Yet, we may wonder whether a State will consider international law as a suitable framework to address a massive cyber operation meddling with its election process, shutting down electricity for thousands of citizens or blowing up an industrial facility on its territory. In recent years, several States have attributed cyber operations to other States, sometimes qualifying them as wrongful acts, but they neither detailed which norms of international law had been breached nor used the international legal framework to respond to these acts. Does this mean that the international legal framework is not suitable to address the threats associated with the exponential development of the internet and information and communication technologies? Or is it because States are not clear on how to apply international law to cyberspace? This book addresses these questions by providing an in-depth analysis of how the norms of international law apply to cyber operations.

The applicability of international law to cyberspace and cyber operations has been a matter of controversy. The contentious question was whether cyberspace constitutes a new 'Wild West' where existing norms of international law, if not international law itself, would not be applicable and thus would not regulate the activities taking place in this 'space'. The question has been settled in both the academic literature and State practice: international law applies to cyberspace and cyber operations. It is worth noting that this had been recognised in the consensual reports of the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of

International Security (UNGGE) in 2013[1] and 2015,[2] and that several States confirmed this position in their comments to the UN Secretary-General[3] and in their national cyberdefence and cybersecurity strategies.[4] Consequently, the question moved on determining the specific interpretation and application of the norms of international law to cyberspace and cyber operations. This does not mean, however, that the application of the norms of international law is an easy task. On the contrary, important issues arise as to how to interpret and apply several norms. There are two main challenges in this regard: on the one hand, given the unique characteristics of cyberspace, interpreting the application of international law to cyber operations may require a certain level of adaptation. On the other, the subjects of international law, and particularly States, may have different if not divergent interpretations of certain specific norms of international law.

[1] UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98, para 19.

[2] UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174, para 24.

[3] UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (9 September 2013) UN Doc A/68/156/Add.1; UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 June 2014) UN Doc A/69/112; UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (18 September 2014) UN Doc A/69/112/Add1.

[4] See, for instance: Australia, 'Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity' (Department of Home Affairs 2016) 7, 28, 40–41 https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf; France (SGDSN), 'Stratégie nationale de la Cyberdéfense [*Revue stratégique de cyberdéfense*]' (Secrétariat général de la défense et de la sécurité nationale (SGDSN) and Economica 2018) 82, 85 and 87 www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/; France, 'International Law Applied to Operations in Cyberspace [*Droit international appliqué aux opérations dans le cyberespace*]' (ministère des Armées 2019) https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf; The Netherlands, 'Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace' and 'Appendix: International Law in Cyberspace' (Ministry of Foreign Affairs 2019) https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; Russian Federation, 'Doctrine of Information Security of the Russian Federation' (2016) para 34 www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163; United Kingdom, 'National Cyber Security Strategy' (2016) 63 www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

International law is often perceived as the Holy Grail for ensuring the peace and stability of cyberspace. For instance, the 'Paris Call for Trust and Security in Cyberspace' launched by French President Emmanuel Macron at the 2018 Internet Governance Forum,[5] the two resolutions on 'Developments in the field of information and telecommunications in the context of international security' adopted by the UN General Assembly in autumn 2018,[6] the norms adopted by the Global Commission on the Stability of Cyberspace in November 2018,[7] plus Microsoft's campaign 'Digital Peace Now',[8] have one thing in common: besides speaking to the diversity of initiatives and processes on cybersecurity at the international level, a general recognition that international law is one of the key pillars in the discussion about stability in cyberspace.

The question of the suitability of international law and the question of its applicability and application to cyberspace must be distinguished. By dissecting the question of the application of international law to cyber operations throughout its chapters, this book ultimately demonstrates whether international law is suitable, even whether it constitutes a panacea, for the peace and stability of cyberspace.

The introduction of this book is comprised of four sections: the first dissects the question of the applicability of international law to cyberspace and offers the reader an introduction to the challenges regarding its application (1.1); the second details the scope of the book (1.2); the third demonstrates the contribution of the book to the scholarship on cyber operations and international law (1.3); and the fourth roadmaps the content of the book by introducing the main aspects of each of its chapters (1.4).

[5] France, 'Paris Call for Trust and Security in Cyberspace' (2018) www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in. A dedicated website was launched at the one year anniversary of the 'Paris Call': https://pariscall.international/.

[6] 'Developments in the field of information and telecommunications in the context of international security', UNGA Res 73/27 (11 December 2018) UN Doc A/RES/73/27; 'Advancing responsible State behaviour in cyberspace in the context of international security', UNGA Res 73/266 (2 January 2019) UN Doc A/RES/73/266.

[7] GCSC, 'Norm Package Singapore' (Global Commission on the Stability of Cyberspace 2018) https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf; see also the final report of the GCSC: 'Advancing Cyberstability' ((Global Commission on the Stability of Cyberspace 2019), https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf.

[8] Microsoft, 'Digital Peace Now' (2018) https://digitalpeace.microsoft.com.

1.1 Cyber International Law: New Challenges for International Law?

Before detailing the scope, contribution and content of the book, it is important to reflect on the development of cyber international law, namely the norms of international law that apply to cyberspace.

The development of cyberthreats occurs at a time when norms of international law, and more generally the international legal order, are questioned and challenged. Since the end of the Cold War, after a period of rise and development, international law is increasingly challenged by States and other actors.[9] Recent practice on the use of force offers a good illustration: an increasing number of States are using force outside the cases prescribed by the UN Charter. In recent times, various events have demonstrated the increasing challenges affecting international law, such as the conflicts in Ukraine and Syria, the relative defiance of the US administration toward international law since the election of President Donald Trump,[10] Chinese actions in the South China Sea, plus the growing critique vis-à-vis the International Criminal Court.[11]

In addition to the general challenges to international law, specific norms of international law are being challenged in their application by new realities and obstacles, such as the development of new technologies. Professors Heike Krieger and Georg Nolte have rightly identified that the development of cyberspace may create new challenges for international

[9] See, generally: Heike Krieger and Georg Nolte, *The International Rule of Law – Rise or Decline? Points of Departure* (KFG Working Paper Series No 1 2016); Alison Pert, 'International Law in a Post-Post-Cold War World – Can It Survive?' (2017) 4 Asia & the Pacific Policy Studies 362. See also, for instance, the discussion on this question in the *EJIL: Talk! Contributing Editors' Debate*: Andreas Zimmermann, 'Times Are Changing – and What about the International Rule of Law Then?' (*EJIL: Talk!*, 5 March 2018) www.ejiltalk.org/times-are-changing-and-what-about-the-international-rule-of-law-then/; Monica Hakimi, 'International Law in "Turbulent Times"', (*EJIL: Talk!*, 6 March 2018) www.ejiltalk.org/international-law-in-turbulent-times-part-i/; Christian Tams, 'Decline and Crisis: A Plea for Better Metaphors and Criteria' (*EJIL: Talk!*, 7 March 2018) www.ejiltalk.org/decline-and-crisis-a-plea-for-better-metaphors-and-criteria/; Lorna McGregor, 'The Thickening of the International Rule of Law in "Turbulent" Times' (*EJIL: Talk!*, 8 March 2018) www.ejiltalk.org/the-thickening-of-the-international-rule-of-law-in-turbulent-times/.

[10] Harold Hongju Koh, 'The Trump Administration and International Law' (2017) 56 Washburn Law Journal 413; Clare Frances Moran, 'Crystallising the International Rule of Law: Trump's Accidental Contribution to International Law' (2017) 56 Washburn Law Journal 491; Jack Goldsmith, 'The Trump Onslaught on International Law and Institutions' (Lawfare, 17 March 2017) www.lawfareblog.com/trump-onslaught-international-law-and-institutions.

[11] Zimmermann (n 9).

law.[12] This observation can, arguably, be further developed. More specifically, I believe that the relationship between the norms of international law and the development of cyberspace should be analysed under three headings.

Firstly, international law has already been challenged and even sometimes contested in recent years. This situation results in a certain level of uncertainty in the way that the norms of international law are, or will be, applied.

Thus, and secondly, the development of cyberspace and cyber operations challenges norms of international law that already face a certain level of uncertainty and contestation in both their content and their application.

Thirdly, this twofold challenge regarding the application of the norms of international law to cyberspace and cyber operations is visible in the difficulty for States to discuss and agree on the matter. The same difficulty is observed in the academic literature.

The work of the UNGGE[13] is particularly illustrative. Most notably, it demonstrates the different positions defended by States on the norms-making process, and their preference for non-binding norms, mainly norms of behaviour and confidence-building measures. In this complex context, the successive UNGGE managed to reach consensus and produce reports. The 2013 and 2015 reports were particularly significant because they acknowledged the applicability of international law and the UN Charter to cyberspace.[14] In June 2017, however, the fifth UNGGE failed to reach a consensus on its final report. Some States contest the applicability of entire branches of international law to cyberspace, such as the law of armed conflict, self-defence and countermeasures. This situation poses a particular challenge to international law and there is a risk of geographical fragmentation of international law norms applicable to cyberspace.

[12] Krieger and Nolte (n 9) 12.

[13] The first UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was appointed by the UN General Assembly in 2004 (UNGA Resolution 58/32), but it failed to adopt a consensus report. It was followed by three successful UNGGE appointed in 2009 (UNGA Resolution 60/45), 2012 (UNGA Resolution 66/24) and 2014 (UNGA Resolution 68/243) which adopted consensus reports respectively in 2010 (UN Doc A/65/201), 2013 (UN Doc A/68/98) and 2015 (UN Doc A/70/174). A fifth UNGGE was appointed by the UN General Assembly in 2016 (UNGA Resolution 70/237), but it failed to adopt a final consensual report in June 2017.

[14] UN Doc A/68/98 8, para 19; UN Doc A/70/174 12, para 24 *et seq.*

By analysing the application of the existing norms of international law to cyber operations as well as identifying their limits, this book provides a lens to study accurately, on the one hand, how international law is challenged, and, on the other, how and to what extent it evolves. Before delving into the application of norms of international law to States' behaviour in cyberspace, it is necessary to analyse the applicability of international law to cyberspace.

1.1.1 International Law Is Applicable to Cyberspace and Cyber Operations

The first question arising with the development of cyber threats is whether international law is applicable to cyberspace and cyber operations. It is only by answering this first question that we can move to the subsequent and more interesting one of the actual application of specific norms of international law to cyberspace and cyber operations.

In that sense, the humankind creation of cyberspace is comparable to the conquest of the air at the beginning of the twentieth century and that of outer space in its middle period. Each time human activities were deployed in a new area, the same question was asked: is international law applicable? And, subsequently, how does it apply?

This section, first, shows that, for the purposes of international law, cyberspace does not constitute a new territory, area or domain, conversely to land, the air, the seas and outer space; second, it demonstrates that nothing prevents international law from applying to cyberspace. The section is comprised of three parts: the first two are dedicated to international air law (1.1.1.1) and international space law (1.1.1.2). The rationale for these analyses is that while considering whether we should adopt a new treaty dedicated to cyberspace and cyber operations,[15] comparisons with the development of the law of the seas, international air law and international space law are frequently used. The argument often put forward is that we need a cyber-specific treaty similar to the

[15] See, for instance: John Markoff and Andrew E Kramer, 'U.S. and Russia Differ on a Treaty for Cyberspace', *The New York Times* (27 June 2009) www.nytimes.com/2009/06/28/world/28cyber.html; Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations' in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (2012); Ido Kilovaty and Itamar Mann, 'Towards a Cyber-Security Treaty' (*Just Security*, 3 August 2016) www.justsecurity.org/32268/cyber-security-treaty/; Mette Eilstrup-Sangiovanni, 'Why the World Needs an International Cyberwar Convention' (2018) 31 Philosophy & Technology 379.

United Nations Convention on the Law of the Sea, the Convention on International Civil Aviation and the Outer Space Treaty. Drawing from this observation, this section provides an introduction to the development of international air and international space law before moving to its third part, showing why cyberspace is different from air and outer space and how it affects the applicability of international law and the development of new norms (1.1.1.3).

1.1.1.1 International Air Law

On 21 November 1783, the first manned hot air balloon flight took place in Paris. The use of hot air balloons developed continuously during the nineteenth century. The first controlled, sustained flight of a powered, heavier-than-air aircraft was performed by Orville and Wilbur Wright on 17 December 1903. The development and multiplication of aircraft, particularly regarding transborder flights, was a growing subject of concern in the late nineteenth century and early twentieth, notably during the First World War.

The status of airspace and human activities taking place in the airspace according to international law was heavily debated. Peter H Sand, Jorge de Sousa Freitas and Geoffrey N Pratt, in an article on the history of international air law, identify four categories of publicists of international air law: 'authors in favour of absolute freedom of air navigation, those in favour of absolute State sovereignty in the air, those accepting a vertical limitation ("zones") to sovereignty, and those accepting a functional limitation by international law'.[16] Despite various attempts of multilateral conferences and conventions on the matter, international air law mainly developed through bilateral agreements.[17]

It was only in 1919, with the adoption of the Paris Convention Relating to the Regulation of Aerial Navigation,[18] that the question of the extension of State sovereignty over airspace was solved. Article 1 reads:

> The High Contracting Parties recognise that every Power has complete and exclusive sovereignty over the air space above its territory.
>
> For the purpose of the present Convention, the territory of a State shall be understood as including the national territory, both that of the mother country and of the colonies, and the territorial waters adjacent thereto.

[16] Sand, de Sousa Freitas and Pratt, 'An Historical Survey of International Air Law before the Second World War' (1960) 7 McGill Law Journal/Revue de droit de McGill 24, 28 (footnotes omitted).
[17] *ibid* 29–31.
[18] 'Convention Relating to the Regulation of Aerial Navigation, Signed at Paris on 13 October 1919, and Its Additional Protocol, Signed at Paris on 1 May 1920' [1922] LNTSer 99; 11 LNTS 173.

This Article codified State practice existing prior to the First World War.[19] The Convention solved the question of the status of airspace regarding State sovereignty as well as establishing various principles that became the basis of international air law. It laid the ground for the future international instruments adopted on this matter, and more generally for the development of international air law.

1.1.1.2 International Space Law

The development of human activities in the airspace made clear that it was only a matter of time before humankind conquered the next frontier, outer space. Consequently, decades before the launch on 4 October 1957 of Sputnik 1, the first man-made object sent into outer space, State representatives and scholars started to think about the legal regime of outer space and of potential human activities that could take place there. In addition to the question of the status of outer space, there was also a question regarding the status of celestial bodies and whether they may be subject to State appropriation. As highlighted by Peter Jankowitsch, '[t]he most powerful drive towards creating such a new branch of international law finally came from geopolitical considerations, namely the opening, in outer space, of a new field of competition and possibly confrontation of the two superpowers of the day, the United States and the Soviet Union'.[20]

This situation led to the adoption of the first resolution of the United Nations General Assembly related to outer space on 13 December 1958, Resolution 1348(XIII) entitled 'Question of the Peaceful Use of Outer Space',[21] that *inter alia* created the ad hoc Committee on the Peaceful Uses of Outer Space (COPUOS), which became permanent with the adoption of Resolution 1472(XI) of 1959.[22] The 1958 resolution was followed by several subsequent resolutions on questions relating to outer space. Resolution 1962(XVIII) entitled 'Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space'[23] marked an important milestone in this process since it laid the

[19] Sand, de Sousa Freitas and Pratt (n 16) 32–33.
[20] Peter Jankowitsch, 'The Background and History of Space Law' in Frans von der Dunk, *Handbook of Space Law* (Elgar 2015) 2.
[21] 'Question of the Peaceful Use of Outer Space', UNGA Resolution 1348(XIII) (13 December 1958) (adopted without vote).
[22] 'International Co-operation in the Peaceful Uses of Outer Space', UNGA Resolution 1472 (XI) (12 December 1959) (adopted without vote).
[23] 'Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space', UNGA Resolution 1962(XVIII) (13 December 1963) (adopted without vote).

foundation of international space law and marked the starting point of the process that led to the adoption of the first multilateral treaty on outer space in 1967.

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,[24] which may be seen as the founding text of international space treaty law, was adopted as an annexe to Resolution 2222 (XXI) of 1966. It was subsequently open to signature simultaneously in London, Moscow and New York in January 1967 and entered into force on 10 October 1967.[25] The Outer Space Treaty, as well as the subsequent Agreement Governing the Activities of States on the Moon and Other Celestial Bodies,[26] established *inter alia* that neither outer space nor celestial bodies may be 'subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means'.[27]

It is today unquestioned that international law applies in both airspace and outer space, including any human activities taking place there. These brief introductions to the development of international air law and international space law show how the applicability of international law to airspace and outer space was slowly settled and became widely accepted – the primary objective was to identify the main features of the specialised regimes relating to specific areas that are often considered as potential models for international cyberspace law. The next section will analyse the main features of cyberspace and identify whether it is relevant to refer to these models for the development of international cyberspace law.

1.1.1.3 International Cyberspace Law

The question of the applicability of international law to cyberspace was based on the assumption that cyberspace constitutes a new area for human activities similarly to land, air, the seas and outer space. This section demonstrates that the assumption is irrelevant, since cyberspace

[24] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, UNGA Resolution 2222 (XXI) (19 December 1966) (adopted without vote) [hereafter Outer Space Treaty].
[25] *ibid*, 18 UST 2410, 610 UNTS 205, 6 ILM 386 (1967).
[26] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies [hereafter Moon Agreement] (adopted by the General Assembly in its Resolution RES 34/68 of 5 December 1979 without vote, and entered into force on 11 July 1984) 1363 UNTS 21, 18 ILM 1434 (1979), 18 UST 2410.
[27] Outer Space Treaty, Article 2; Moon Agreement, Article 11.

does not constitute a new legal domain (A), and nothing prevents international law from applying to cyberspace and cyber operations (B).

A Cyberspace Is Not a New Legal Domain Cyberspace is not a technical term created by computer scientists or engineers. It first emerged in science fiction literature.[28] William Gibson is considered to be one of the first writers to employ and popularise the term cyberspace.[29] He used it for the first time in July 1982 in 'Burning Chrome', a short story published in the magazine *Omni*.[30] In his 1984 novel *Neuromancer*, he portrayed the notion of cyberspace thus:

> A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding.[31]

Initially, cyberspace had no clearly defined 'semantic meaning'.[32] Slowly and incrementally, however, the term cyberspace migrated from the realm of science fiction and became pivotal elsewhere. For instance, a debate emerged, and continues today, on whether cyberspace constitutes the fifth domain for military activities alongside the existing domains of land, sea, air and outer space.[33] Likewise, it is debated whether it constitutes a 'global common',[34] which is a domain or area that lies outside the

[28] Jeff Prucher (ed), 'Cyberspace', *The Oxford Dictionary of Science Fiction* (OUP 2006).
[29] See, for instance, Scott Thill, 'March 17, 1948: William Gibson, Father of Cyberspace', *WIRED* (17 March 2009) http://archive.wired.com/science/discoveries/news/2009/03/dayintech_0317.
[30] William Gibson, 'Burning Chrome', *Omni* (July 1982) 72.
[31] *ibid*, *Neuromancer* (Ace Books 1984) 69.
[32] In 2000, Gibson commented on the origins of the term and criticised it in a documentary on his work, stating, 'All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.' See Mark Neale, *No Maps for These Territories* (Docurama 2000).
[33] 'Cyberwar: War in the Fifth Domain', *The Economist* (1 July 2010) www.economist.com/node/16478792; see also: Christy Marx, *Battlefield Command Systems of the Future* (The Rosen Publishing Group 2005) 14; Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfection of International Law* (Brill & Martinus Nijhoff Publishers 2015) 13.
[34] Jean-Jacques Lavenue, 'Cyberespace et Droit International : Pour Un Nouveau Jus Communicationis' [1996] *Revue de la Recherche Juridique: Droit prospectif* http://droit.univ-lille2.fr/fileadmin/user_upload/enseignants/lavenue/cyberart.pdf, Part II(B); Joanna Kulesza, *International Internet Law* (Routledge 2012) 145–146; Scott J Shackelford,