The Legacy of the Law of the Sea for Cyberspace Peacetime Regulation: Moving from Imitation to Methodology

Abstract

During the last decade the international decision-makers increasingly struggled to find suitable analogies to frame the regulatory scenario of the 'cyberspace'. The emergence of an increasingly contested and dynamic *aterritorial* dimension – only partially overlapping with the traditional 'domains' falling within the scope of international law provisions – urged both academic and political community to provide a coherent jurisdictional framework to establish legal certainty in cyberspace.

Ranging different disciplinary fields and often subjected to unwarranted sensationalism and 'hype', we argue that regulating the multi-layered patchwork of cyberspace activities requires a more nuanced approach able to build on analogies with existing international framework while emphasizing the need for new legal and policy solutions to cyberspace inherent *diversity*. The Law of the Sea – in particular the 1982 'Montego Bay Convention' – and the Outer Space Law may serve as a methodological blueprint for a thorough international debate and appraisal of international cyberspace regulation.

International Law; Cyberspace Regulation; Law of the Sea; Cyber Domain; Heterotopian Space

Words count: 3306

I. INTRODUCTION: ADDRESSING CYBERSPACE LEGAL VACUUM

The cyber domain – because of its unique features – is 'a perfect breeding ground for political disorder and strategic instability.[1] Global computer-based communications cut across territorial borders, creating a new realm of human activity and "undermining the feasibility – and legitimacy – of laws based on geographical boundaries."[2]

States and relevant stakeholders - facing the challenges raised by the astonishing pace of increase in cyber actors', data flows and technical vulnerabilities in the new domain – could no simply 'embrace uncertainty'[3] abandoning any attempt to develop treaties to regulate the new domain.

Cyberspace cannot be deemed a legal lacuna:[4]it is broadly acknowledged the need to establish a common ground to promote rule of law compliance and to strike a balance between several principles at stake, such as internet freedom, privacy, law enforcement, and interstate cooperation.

The utopia of a non-territorial or aterritorial internet expressed in 1996 Barlow's *Declaration of Independence of Cyberspace* - that may sound odd nowadays - has gradually evolved in even more puzzling jurisdictional quandaries, leaving cyberspace legal regime caught between the forces of local territorialism and the new rational of commercial efficiency.[5]

Concurring with eminent scholars, we argue that the question should not be "*whether* to regulate cyberspace [and cybersecurity issues], but rather *how* to do so – within which forum, involving which actors and according to which of many competing values."[6]

Though nostalgic of absolute States' sovereignty still advocate for a 'Cyber Westphalia'[7] arguing that "[international] law that can be applied to cyberspace without far-reaching modifications"[8]it is manifest that cyberspace 'heterotopian' spatiality necessitates a paradigmatic shift in how we conceptualize the exercise of jurisdiction and the related relevant provisions and norms.[9]

---

1 Kello, L. (2013) The meaning of the Cyber Revolution. *International Security* 38(2), 7-40: 32

2 Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 1367

3 Murray, A. (2007). *The regulation of cyberspace: control in the online environment.* Routledge: 252-256

4 Ziolkowski, K. (Ed.). (2013). Peacetime regime for state activities in cyberspace, NATO Cooperative Cyber Defence Centre of Excellence: XIII

5 Schultz, T. (2008). Carving up the Internet. *European Journal of International Law*, 19(4), 800

6 Deibert, R. & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy:* 56

7 Demchak, C., & Dombrowski, P. (2013). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs*, 29-38.

8 von Heinegg, W. H. (2012). Legal implications of territorial sovereignty in cyberspace. In 2012 *4th International Conference on Cyber Conflict* (CYCON 2012), 1-13.

9 See: Fehlinger P. & De La Chapelle B. (2016) Jurisdiction on the Internet: from Legal Arms Race to Transnational Cooperation, *Global Commission On Internet Governance Paper Series*:

No. 28 — April 2016, Chatham House; and Ryngaert, C., & Zoetekouw, M. “The End of Territory? The Re-Emergence of Community as a Principle of Jurisdictional Order in the Internet Era” in Kohl, U. (Ed.) (2017) *The Net and the Nation State,* Cambridge: Cambridge University Press, 185-201; for a thorough analysis see the suggestions advanced by Easterbrook: “the best way to learn the law applicable to specialized endeavors is to study general rules.” In Easterbrook, F. H. (1996), “Cyberspace and the Law of the Horse”, *University of Chicago Legal Forum.*, 207.

II. THE INTERNATIONAL REGULATION OF MARITIME DOMAIN AS A METHODOLOGY

The idea of a global "all-encompassing Internet treaty that would harmonize relevant laws and solve the full range of cyber-cooperation issues" presents severe political and technical shortfalls.[10] Nevertheless, the parallel to decades-long efforts of international negotiations resulting in the 1982 Montego Bay Convention (UNCLOS) could provide a useful starting ground as long as it is
conceived not as a mere analogical transfer of principles, but as a valuable model on how to engage different actors and strike a balance among opposite interests.

Moreover, it is noteworthy to emphasize how a conventional instrument such a treaty – unlike soft-law measures – could help the generation of customary international law norms. Finally, on the following analysis of how the International Law of the Sea drafting process - particularly the 1982's UNCLOS - could serve as a paradigm for the birth of a cyberspace international treaty law, we should bear in mind the following caveats.

Firstly, law of the seas' milestone attempt of regulation dates to early XVII century (Dutch Jurist Grotius wrote the seminal *Mare Liberum* in 1609)[11] and its codification has been lengthy and unwieldy due to conflicting States' interests, whereas the cyberspace has quickly emerged as a new -military and civilian - domain only in the most recent decades.

Moreover, even if severe divergences among States[12] on how to cope with cybersecurity were overcome, the range of actors involved ought to be broadened in order to shift the focus from international cooperation to transnational cooperation among all stakeholders.[13]

Even though several provisions of IL treaties on the law of the sea (mainly the UNCLOS and the 1994 *San Remo Manual*) could have a say in cyberspace, we will not push too forward the equivalence. The feasibility of the 'cyber sea' metaphor - which suggest to "apply the navigational regimes of the UNCLOS to the medium of cyberspace[14] – remains questionable. The main analytical focus will be instead on the methodological and diplomatic takeaways of the UNCLOS drafting process. The International community should engage all the relevant stakeholders and build upon the cumbersome, but successful pattern of the maritime domain regulation process to create a set of binding treaties able to develop common rules, a shared lexicon and, possibly, a Court.

---

[10] Fehlinger P. & De La Chapelle B., *op.cit.,* 11.

[11] See e.g. Chapter 4 in Brownlie, I. B. (1990). *Principles of public international law*. Oxford University Press.

[12] Kilovaty, I. & Mann, I. (2016), Towards a Cyber-Security Treaty, *Just Security*, August 3, 2016.
[13] Fehlinger P. & De La Chapelle B. (2016) Jurisdiction on the Internet.
[14] Stavridis, J. G., & Parker III, E. C. (2012). Sailing the cyber sea. *Joint Force Quarterly*, (65): 61.

III. BUILDING ON UNCLOS PROVISIONS: THE BEST WAY FORWARD?

In the present essay, we will not focus on the *jus ad bellum* and *jus in bello*[15], rather we will examine the 'peacetime regime for cyberspace. However, it is worth mentioning that notable efforts have been made to develop an international common regulation of the 'fifth domain of warfare'. Nevertheless, the agreements failed to deliver tangible results since cyberattacks 'defy the simple categorization of traditional weaponry under international law'[16] and the definition itself vary widely.[17]

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is a non-binding academic document developed under NATO CCDCOE overview, it provides little help in developing a consistent treaty on peacetime activities. Similarly, the Council of Europe's Convention on Cybercrime – the only multilateral, legally binding instrument that address criminal activities in cyberspace[18] could not constitute a starting point for a 'cybersecurity convention'

because of its negligible impact on States' jurisdictional claims and the shortfalls in effectiveness.[19] "If members of the international community were able to develop a convention structured after UNCLOS III, mandating international cooperation on cybersecurity […] the benefits would be palpable."[20] Nonetheless, despite some shared features of maritime and cyber domain[21], the seas have more-or-less well-defined boundaries related to topographically defined jurisdictions in physical space, while cyberspace has only weak connectivity to physical space[22] and its inherently expansive in nature. Finally, both UNCLOS and space treaty were developed 'at a time of greater trust of international bodies to assist in the management of distrust between sovereign nations'.[23] Furthermore, cyberspace is both cross-cutting deep-rooted in all the physical domains: [24]the overwhelming array of phenomena that may occur at physical or intangible level made it ill-suited to an all-encompassing treaty.

---

15 Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*.

16 Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: T. *Duke L. & Tech. Rev*.: 21

17 An intense debate is under way about the applicability of UN Charter provisions such as 'use of force' (art.2.4), 'legitimate self-defense' (art. 51) to cyberattacks Hathaway, O. et al. (2012) "The law of cyber-attack." *California Law Review*; Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press.

18 Jurich, J. P. (2008). Cyberwar and customary international law. *Chi. J. Int'l L., 9,* 275: 283

19 See Stahl, W. M. (2011). Uncharted Waters of Cyberspace. *Ga. J. Int'l & Comp*. L., 40, 247: 263-264 and Weber, A.
M. (2003). Council of Europe's Convention on Cybercrime, *The. Berkeley Tech. LJ,* 18, 425.

20 Stahl, W. M. (2011): 270

21 "Both are expansive domains in which humans can operate using specially designed and developed technologies". Ryan, J. J., Ryan, D. J., & Tikk, E. (2010). Cyber Security Regulation. *International Cyber Security: Legal & policy Proceedings*, CCDCOE: 82.

22 Ibid.: 82.

23 Weitzel, D. S. (2001). Where No Lawyer Has Gone Before-What a Cyberspace Attorney

Can Learn from Space Law's Legacy. *Comm. Law Conspectus,* 10, 191: 192.

[24] CEIS (2014), "Les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ?" Ministère de la défense Délégation aux Affaires Stratégiques: 11.

IV. CONTENT ANALOGIES: FOOD FOR THOUGHT, DESPITE DISSIMILARITIES

Nowadays – like during the protracted drafting process of UNCLOS– international stakeholders are called to deal with the "void created by the rampant technological revolution in this area"[25].

A sound policy that balances international freedoms in cyberspace with legitimate concerns about national security with legitimate concerns about national security[26] may be achieved drawing upon UNCLOS' drafting process and adapting the principles stated in its Preamble to cyber domain.[27]

Nevertheless, 'applying [altogether] the navigational regimes to the medium of Cyberspace'[28], would be a 'conceptual stretching' since cyberspace's borders are blurred and contested.

A high-sea-like regime (part VII UNCLOS) would give rise to further jurisdictional confrontation; likewise, the proposed model of harbour and 'cabotage' to regulate transborder data flows[29] would be unfeasible because of cyberspace's unique mechanisms such as anonymization, ubiquity, data divisibility and data partioning.[30] Similar conundrums thwart the application of the right of innocent passage (art. 52 UNCLOS) and cast doubts on the smooth running of the hazy parallel between 'archipelagic waters' (art. 49 UNCLOS) and the Cloud.

Furthermore, it should be underscore that cyberspace cannot be classified neither as 'common heritage of mankind' (art. 136 UNCLOS) nor as a *res nullius*: even if cyberspace in its entirety is not subject to the sovereignty of a single State or of a group of States[31], they retain a high degree of control on it. The different jurisdictional claims and the lack of a shared vocabulary on the definitions of cybercrime and cybersecurity itself constitute a critical hurdle in developing a consistent basis to address serious threats taking cue from UNCLOS' provisions on piracy (art. 101).

The development of a universal jurisdiction in cyberspace is unlikely if States will be unable (or unwilling) to come together and agree on common definitions and thresholds as to fundamental features of cybersecurity environment.[32] The hopeful prospect of UNCLOS' adaptation to cyber domain pertains mainly to the Governance *of* the Internet -i.e. the governance of protocols and the

---

25 Evensen, J. (1986) "Working Methods and Procedures in the Third UNCLOS",199 *Receuil des Cours,* 436. See also: Harrison, J. (2011). *Making the Law of the Sea,* Vol. 80, Cambridge University Press.

26 Barney, S. M. (2001) "Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of cyberspace." *Naval Law Review.* Vol. 48.: 61.

27 "Prompted by the desire to settle, in a *spirit of mutual understanding and cooperation*, all issues relating to the Law of the Sea"; "Recognizing the desirability of establishing [..], with *due regard for the sovereignty* of all States, a *legal order* […]"

28 Barney, S. M. (2001) "Innocent Packets?": 61.

29 Jiménez, W. G., & Lodder, A. R. (2015). Analyzing approaches to internet jurisdiction based on a model of harbors and the high seas. *International Review of Law, Computers & Technology*, 29(2-

3), 266-282.
[30] Daskal J., (2016) The Un-Territoriality of Data, *Yale Law Journal:* 368-369.
[31] von Heinegg, W. H. (2012). Legal implications of territorial sovereignty in cyberspace: 1.
[32] See Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press.

evolution of the technical architecture.[33] The 98% of all international internet traffic is on submarine cables[34] that constitute the backbone of the international telecommunication system[35]: therefore, UNCLOS art. 113 constitutes a vital provision to regulate cyberspace's physical layer.

It is not unreasonable to take cue from the International Tribunal for the Law of the Sea (ITLOS) to develop a forum to settle disputes, nevertheless the discussion on the issue have been limited to academic *exercises de style*[36] or it have become bogged down by unbridgeable jurisdictional divides and opposite principles among countries and stakeholders involved.

Moreover, a set of agreements that would shape a framework of shared definitions and jurisdictional rules thereof is a prerequisite for the development of an effective cyberspace IL arising from Law of the Sea's exemplum. Finally, a Tribunal for Cyberspace should be grounded in several treaties since no single UN treaty could simultaneously regulate cyberwarfare, counter cybercrime and protect the civil liberties of Internet users.[37] The creation of an international cyberspace tribunal – ideally granting to international organizations a *locus standi* and not the mere right to file amicus curiae briefs (ITLOS Rule 84) and cautious of avoiding overlapping competences with ICJ and ICC[38] – 'would go a long way toward encouraging cooperation on the development of international norms' on cybercrime and cybersecurity while allowing nations to retain some level of autonomy in domestic cybersecurity policies.[39]

---

[33] de La Chapelle, B. (2007). "The Internet Governance Forum: How a United Nations Summit Produced a New Governance Paradigm for the Internet Age." In *Governing the Internet*. OSCE: 27

[34] Presentation by the International Cable Protection Committee (ICPC), (2015) "UN Open-Ended Informal Consultative Process on Oceans and the Law Of The Sea", *16th meeting Oceans and Sustainable Development*

[35] See e.g. "Oceans and the law of the Sea", Report of the Secretary-General, A/70/74, 30 March

2015

[36] Stein Schjolberg advocated for a ‘an International Court or Tribunal for Cyberspace’ established through a set of
United Nations’ treaties. Schjolberg, S. (2011). A global treaty on cybersecurity and cybercrime. *Cybercrime Law*, 97.

[37] Patrick, S. (2014). Unruled World. *Foreign Aff.,* 93, 58: 71

[38] With regard to Law of the Sea conflicts: Treves, T. (1998). Conflicts between the ITLOS and ICJ. *NYUJ Int'l L. & Pol.*, *31*, 809.

[39] Stahl, W. M. (2011). Uncharted Waters of Cyberspace: 273

V. CONCLUSION: SHARING LANGUAGE AND PRINCIPLES TO DEVELOP INTERNATIONAL LAW

Several authors argued that the UNCLOS cannot constitute a usable model for policy for the global cyberspace security due to the latter's newness, volatility and rapid pace of innovation in the digital realm.[40] Nevertheless, despite the emphasized dissimilarities, UNCLOS drafting process could provide a spark to develop – through a lengthy, but necessary international dialogue - a common lexicon on global cybersecurity and a starting ground to engage all relevant stakeholders, moving from pure intergovernmental treaties to policy standards based on transnational cooperation.[41] Reverting the UNCLOS process – prior agreement on joint definitions and principles during a series of international conferences – could then lead to the consolidation of a shared *opinio juris* that would trigger a consistent *State practice* helping in generating a cyberspace customary international law.[42]

[40] Nye, J. (2014). The Regime Complex for Managing Global Cyber Activities. *Governance Paper Series No.1*: CIGI.

[41] Fehlinger P. & de La Chapelle B. (2016) Jurisdiction on the Internet: 13

[42] See e.g. D'Amato, A. (1970). Manifest intent and the generation by treaty of customary rules of international law. *American Journal of International Law,* 64, 892; Baxter, R. R. (1965). Multilateral Treaties as Evidence of Customary International Law. *Brit. YB Int'l L.*, 41, 275.

BIBLIOGRAPHY

Barney, S. M. 2001. "Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of cyberspace." *Naval Law Review.* Vol. 48., 61.

Baxter, R. R. 1965. Multilateral Treaties as Evidence of Customary International Law. *Brit. YB Int'l L.*, 41, 275.

Brenner, S. W. 2009. *Cyberthreats: The emerging fault lines of the nation state.* Oxford University Press.

Brownlie, I. B. 1990. *Principles of public international law*. Oxford University Press.

CEIS. 2014. “Les droits maritime et de l’espace peuvent-ils inspirer un droit du cyberespace ?” *Ministère de la défense Délégation aux Affaires Stratégiques,* 11.

D'Amato, A. 1970. Manifest intent and the generation by treaty of customary rules of international law. *American Journal of International Law,* 64, 892.

Daskal, J. C. 2015. The Un-Territoriality of Data. *Yale Law Journal*, *2016*.

Deibert, R., & Rohozinski, R. 2010. Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43-57.

de La Chapelle, B. 2007. “The Internet Governance Forum: How a United Nations Summit Produced a New Governance Paradigm for the Internet Age.” In *Governing the Internet*. OSCE, 27

Demchak, C., & Dombrowski, P. 2013. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs*, 29-38.

Easterbrook, F. H. 1996. “Cyberspace and the Law of the Horse”, *University of Chicago Legal Forum*, 207.

Evensen, J. 1986. *Working methods and procedures in the Third United Nations Conference on the Law of the Sea*. Martinus Nijhoff.

Fehlinger P. and De La Chapelle B. 2016. Jurisdiction on the Internet: from Legal Arms Race to Transnational Cooperation, *Global Commission On Internet Governance Paper Series*: No. 28 — April 2016, Chatham House.

Harrison, J. 2011. *Making the Law of the Sea,* Cambridge University Press.

Hathaway, O. et al. 2012. The law of cyber-attack. *California Law Review*: 817-885.

Johnson, D. R., & Post, D. 1996. Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 1367-1402.

Jurich, J. P. 2008. Cyberwar and customary international law: The potential of a bottom-up approach to an international law of information operations. *Chi. J. Int'l L.*, *9*, 275.

Kello, L. 2013. The meaning of the Cyber Revolution: perils to theory and statecraft. *International Security*, 38(2), 7-40.

Kilovaty, I. & Mann, I. 2016. , Towards a Cyber-Security Treaty, *Just Security*, August 3, 2016.

Murray, A. 2007. *The regulation of cyberspace: control in the online environment.* Routledge.

Nye, J. 2014. The Regime Complex for Managing Cyber Activities, The Global Commission on Internet Governance, *Global Commission on Internet Governance Paper Series*, No. 1

Ophardt, J. A. 2010. Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duke L. & Tech. Rev*., 21.

Patrick, S. 2014. Unruled World: The Case for Good Enough Global Governance, *Foreign Aff.*, *93*, 58.

Ryan, J. J., Ryan, D. J., & Tikk, E. 2010. Cyber Security Regulation. *International Cyber Security: Legal & policy Proceedings*, Tallinn, CCDCOE.

Ryngaert, C., & Zoetekouw, M. "The End of Territory? The Re-Emergence of Community as a Principle of Jurisdictional Order in the Internet Era" in Kohl, U. (Ed.) (2017) *The Net and the Nation State., Multidisciplinary Perspectives on Internet Governance,* Cambridge: Cambridge University Press, 185-201

Schjolberg, S., & Ghernaouti-Helie, S. 2011. A global treaty on cybersecurity and cybercrime. *Cybercrime Law*, 97.

Schmitt, M. N. 2013. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Schultz, T. 2008. Carving up the Internet: jurisdiction, legal orders, and the private/public international law interface. *European Journal of International Law*, *19*(4), 799-839.

Stahl, W. M. 2011. Uncharted Waters of Cyberspace. *Ga. J. Int'l & Comp*. L., 40, 247.

Stavridis, J. G., & Parker III, E. C. 2012. Sailing the cyber sea. *Joint Force Quarterly*, (65), 61.

Treves, T. 1998. Conflicts between the ITLOS and ICJ. *NYUJ Int'l L. & Pol.*, *31*, 809.

Jiménez, W. G., & Lodder, A. R. 2015. Analyzing approaches to internet jurisdiction based on a model of harbors and the high seas. *International Review of Law, Computers & Technology*, 29(2-3), 266-282.

Weitzel, D. S. 2001. Where No Lawyer Has Gone Before-What a Cyberspace Attorney Can Learn from Space Law's Legacy. *CommLaw Conspectus,* 10, 191.

Ziolkowski, K. (Ed.). 2013. *Peacetime regime for state activities in cyberspace: international law, international relations and diplomacy*. NATO Cooperative Cyber Defence Centre of Excellence.

MAIN DOCUMENTS

Council of Europe Convention on Cybercrime. 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Oceans and the law of the Sea, Report of the Secretary-General, A/70/74, 30 March 2015. Available at: http://cil.nus.edu.sg/wp/wp-content/uploads/2015/12/Ses7-2.-A.70.74-Oceans-and-the-Law-of-the-Sea-in-%E2%80%98Report-of-the-Secretary-General-Report-of-UNSG%E2%80%99-30-March-2015-paras.-53-55..pdf

Rules of the International Tribunal for the Law of the Sea 2009. Available at: https://www.itlos.org/fileadmin/itlos/documents/basic_texts/Itlos_8_E_17_03_09.pdf

United Nations Convention on the Law of the Sea. 1982. Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf