ESIL Reflections
Editorial Board: Federico Casolari, Patrycja Grzebyk, Ellen Hey, Guy Sinclair and Ramses Wessel (editor-in-chief)

17 December 2020 Volume 9, Issue 4

Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace

Image by Miriam Espacio (cc)

*Nicholas Tsagourias**
University of Sheffield

Introduction

The COVID-19 pandemic has posed many normative and institutional challenges to the international legal system in both its off-line and on-line dimensions. Certain institutional challenges related to the role of the Security Council, the securitisation of health risks, and the division of powers between the Security Council and the WHO will be examined by Ilja Pavone and Pedro Villarreal in subsequent contributions. This contribution instead focuses on a normative and indeed an on-line challenge, namely the application of general principles of international law, and more specifically the principle of sovereignty, to cyberspace in view of the persistence of malicious cyber operations against health infrastructure during the pandemic. This Reflection uses such malicious cyber operations as a platform to explore the systemic implications of applying the principle of sovereignty to cyberspace, an issue that has divided scholars and governments.

During the COVID-19 pandemic, there has been a significant increase in malicious cyber operations against states' health infrastructure.[1] These include operations against hospitals treating COVID-19

*Professor of International Law and Director of the Sheffield Centre for International and European Law, University of Sheffield, School of Law. nicholas.tsagourias@sheffield.ac.uk

patients,[2] intelligence gain operations against vaccine research centres developing anti-COVID-19 vaccines,[3] as well as operations against governmental health services dealing with COVID-19.[4] Although not all these operations were committed by states, certain operations, in particular those for intelligence gain, were linked to states and provoked stern condemnation. The British Foreign Secretary, for example, called Russia's attacks on vaccine developers in the UK 'unacceptable' and said that international law and the norms of responsible state behaviour must be respected and perpetrators held to account.[5] The Netherlands stated that such operations are 'deplorable examples of irresponsible state behaviour' and that 'in many instances, they constitute violations of international law'.[6] However, even though states condemned such operations as violations of international law, they did not specify which specific rules had been violated.

In view of such legal uncertainty, a number of proposals have been put forward. One proposal envisages the creation of a new norm to protect medical services and facilities from malicious cyber operations during peacetime[7], replicating a similar norm that exists during wartime.[8] Another proposal aims to include the health sector within the protected critical state infrastructure as provided in recommendation 13(f) of the 2015 Report of the United Nations Group of Governmental Experts on

[1] INTERPOL (2020) "Cybercriminals targeting critical healthcare institutions with ransomware" https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware ; Kaspersky, Annex to the second 'Pre-draft' of the report of the Open-Ended Working Group ('OEWG') on developments in the field of information and telecommunications in the context of international security: Kaspersky brief on the threat landscape during the pandemic, June 2020 https://front.un-arm.org/wp-content/uploads/2020/06/kaspersky-annex-on-cyber-threat-landscape-during-covid-19-pandemic-11-june-2020.pdf.

[2] 'L'AP-HP visée par une attaque DDoS' mardi 24 mars 2020 https://www.zdnet.fr/actualites/l-ap-hp-visee-par-une-attaque-ddos-39901161.htm

[3] 'UK National Cybersecurity Centre, Advisory: APT29 targets COVID-19 vaccine development' 16 July 2020 https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf; FBI and CISA, People's Republic of China(PRC) Targeting of COVID-19 Research Organizations 13 May 2020, https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf

[4] U.S. Embassy statement on September 1, 2020 cyberattack against Georgian Ministry of Health https://ge.usembassy.gov/u-s-embassy-statement-on-september-1-2020-cyberattack-against-georgian-ministry-of-health/#.X1H9X59PCsE.twitter

[5] 'UK condemns Russian Intelligence Services over vaccine cyber attacks' 16 July 2020, https://www.gov.uk/government/news/uk-condemns-russian-intelligence-services-over-vaccine-cyber-attacks; 'UK condemns cyber actors seeking to benefit from global coronavirus pandemic' 5 May 2020, https://www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic

[6] 'The Kingdom of the Netherlands' response to the pre-draft report of the OEWG' https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf

[7] ICRC, Statement on agenda item "Norms, rules, and principles" within the open-ended working group on developments in the field of information and telecommunications in the context of international security, 2 July 2020, https://www.icrc.org/en/document/cyberattacks-against-medical-facilities-pose-real-risk-humans-times-pandemics-times. See also *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector* at *https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea*

[8] Article 27 Hague Regulations; Article 19 GCI; Article 18 GCIV; Article 12 API; Article 11 APII.

Developments in the Field of Information and Telecommunications in the Context of International Security (GGE).[9]

Although I have no reason to question the sincerity of such proposals, I am concerned about their systemic effects. Replicating rules that apply during armed conflict introduces a notion of hybrid peace whereas devising new, specifically designed, norms for cyberspace saturates it with norms, leading to normative relativity. More broadly, there is a danger of unnecessarily fragmenting international law through reactive norm creation. One is thus reminded of Judge Easterbrook's 'law of the horse' analogy. As he said, there is no more 'law of cyberspace' than there is 'law of the horse' and that, when faced with new domains and calls for new law, 'the best way to learn the law applicable to specialized endeavours is to study general rules' instead of creating a 'law of the horse'.[10] He then went on to say that what is needed is clarification of the rules.

Before jumping into new endeavours or getting too excited about creating new norms, we need to consider how existing international law principles can address such malicious cyber operations. I contend that the principle of sovereignty is one such general principle that can deal with malicious cyber operations conducted by one state against the health infrastructure of another state.[11]
In what follows I will firstly explain the place and role of the principle of sovereignty in international law and in cyberspace, then I will consider its content and scope and explain how malicious cyber operations against health infrastructure during the pandemic can violate this principle, and finally I will reflect on the systemic implications of applying the principle of sovereignty to cyberspace.

The principle of sovereignty in international law and in cyberspace

Sovereignty is an attribute attached to states and denotes supreme, exclusive, and plenary power and authority.[12] Sovereignty and international law are co-existential. Sovereignty is constitutive of international law because it gives meaning and ontology to international law. Sovereignty operationalises international law because it is the engine behind the creation, application, and enforcement of international law. As the International Court of Justice (ICJ) said, the whole of international law rests upon sovereignty.[13] Sovereignty is also an organising principle in that it

[9] 'The Kingdom of the Netherlands' response to the pre-draft report of the OEWG', supra note 6. UNGA, "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 Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector
[10] Frank H. Easterbrook, "Cyberspace and the Law of the Horse," University of Chicago Legal Forum 207 (1996)
[11] This Reflection focuses on general international law principles applying to inter-state relations and not on specific regimes such as human rights, IP law, or criminal law. It also presumes that said operations are attributable to a state although it will not discuss the attribution criteria for lack of space. For the latter, see for example Nicholas Tsagourias and Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges* 31 *EJIL* 2020
https://academic.oup.com/ejil/advance-article-abstract/doi/10.1093/ejil/chaa057/5897247
[12] Samantha Besson, "Sovereignty" in Rüdiger Wolfrum, ed., *Max Planck Encyclopedia of Public International Law,* OUP, 2012.
[13] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America),* 27 June 1986, ICJ Reports 1986, para 263.

identifies the units of legal and political authority in international law and relations and, at the same time, it defines and delimits their legal competences and powers. In this way it organises their interactions and maintains peace and order by preventing unwelcome interference. Finally, sovereignty ensures participation in the international political and legal process regardless of the state's size and power and, in this regard, it democratises international law and relations.
After the early days of cyber idealism which viewed cyberspace as a new domain cut off from state sovereignty, the 2013 and 2015 UN GGE Reports affirmed that international law, the principle of sovereignty, and the international norms and principles that flow from sovereignty apply to cyberspace.[14] Also, the majority of states that have made their position known recognise the application of the principle of sovereignty to cyberspace.[15]

However, the legal status of the principle of sovereignty in cyberspace has been questioned, with the UK being the arch sceptic. The UK claimed that sovereignty is just a principle and not a rule and, therefore, it does not produce legal consequences.[16] For the UK, a violation of sovereignty does not exist in a legal sense; it only exists in a political sense. Instead, the only rules that apply to cyberspace and produce legal consequences are those on the non-use of force and non-intervention. Applying this line of reasoning to the aforementioned operations means that they did not violate the principle of sovereignty because sovereignty is not a legal rule, they did not violate the rule on the non-use of force because they did not reach the requisite threshold of destruction, and they did not violate the non-intervention rule because they were not coercive.[17]

In my opinion, the view that sovereignty is a non-legally consequential principle is erroneous and I will immediately explain why. I will do this by explaining the legal nature of principles and the relationship between principles and rules before I discuss the legal import of the principle of sovereignty in cyberspace.

---

[14] UNGA '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, paras 19–20. UN GGE 2015 Report, supra, para. 26.

[15] Selectively see République Française, Ministère des Armées, *Droit International Appliqué aux Opérations dans le Cyberespace* (2019) at 1.1. and 1.1.1; 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 Appendix: International law in cyberspace; *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* (July 2020) https://www.aldiplomasy.com/en/?p=20901; Finland, *International law and cyberspace: Finland's national position* (2020) 1-3, at https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859

[16] 'Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.' UK Attorney General's Office, *Cyber and International Law in the 21st Century*, (23 May 2018), available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[17] For a discussion of the scope of the non-intervention and non-use of force rules see the documents mentioned in footnote 15. Whether these malicious operations breached other international law rules such as human rights is outside the scope of this Reflection.

A principle is a general normative proposition containing standards and objectives whereas a rule contains specific prescriptions and proscriptions.[18] When principles enter a legal system, they become legal principles. This is what happened with the principle of sovereignty which, from a political principle, became an international law principle[19] representing the aggregation of rights and duties a state has *qua* state and vis-à-vis other states.[20]

As an international law principle, sovereignty is legally consequential. It can give rise to specific rules such as the rules on the non-use of force or non-intervention.[21] These rules emanate from and protect specific aspects of a state's sovereignty such as its territorial integrity and political independence. This does not mean, however, that the principle of sovereignty becomes redundant. Because of its general character, it remains in the background and can apply to specific facts, producing legal consequences. It should be recalled in this respect that the ICJ attaches legal consequences to principles and, often, uses principles and rules interchangeably.[22] In relation to the principle of sovereignty, for example, the Court held that US overflights violate Nicaragua's sovereignty[23] whereas in *Costa Rica v. Nicaragua* it held that by 'excavating three *carios* and establishing a military presence on Costa Rican territory, Nicaragua has violated the territorial sovereignty of Costa Rica'.[24]

Likewise, states such as France and the Netherlands have affirmed the legal status of sovereignty in cyberspace and recognised that certain cyber operations can violate it.[25] NATO also views sovereignty as being legally consequential.[26] In the same vein, Iran declared that 'the sovereignty of states is not an extra-legal matter'[27] and Finland stated that sovereignty is a primary rule of international law, 'a breach of which amounts to an internationally wrongful act and triggers State responsibility.'28 It can thus be said with reason that, with the exception of the UK, most states that have made public statements on this issue support the view that sovereignty is a legally consequential principle. As far as the USA is concerned, it takes a more nuanced approach. According to a recent iteration, 'States have sovereignty over the information and communications technology infrastructure within their territory' but '[t]he implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there

[18] Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press, 1978), chs 2 and 3.
[19] Declaration on Principles of International Law concerning Friendly Relations & Co-operation among States, UNGA Res. 2625 (XXV), U.N. Doc. A/RES/25/2625 (Oct. 23, 1970).
[20] James Crawford, *Brownlie's Principles of Public International Law,* 8th ed., (OUP, 2012), p. 448.
[21] Article 2(4) of the UN Charter; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America),* [1986] ICJ Rep 14, paras. 202, 204.
[22] *Delimitation of Maritime Boundary in Gulf of Maine Area (Can. v. U.S.)*, [1984] ICJ Rep 246, para 79.
[23] *Nicaragua Case*, supra note 21, para 251.
[24] *Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica Along the San Juan River (Nicaragua v. Costa Rica),* [2015], ICJ Rep 665, para. 229.
[25] *Droit International Appliqué aux Opérations dans le Cyberespace,* supra note 15, 1.1 and 1.1.1; Letter of 5 July 2019 from the Minister of Foreign Affairs, supra note 15. See also the position of New Zealand, The Application of International Law to State Activity in Cyberspace, 01 Dec 2020, paras 11-15, at https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/
[26] AJP-3.20. Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1, January 2020, p.20 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
[27] Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran, supra note 15.
[28] *International law and cyberspace: Finland's national position,* supra note 15, 3.

exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.'[29]

It transpires from this that what is needed is clarification of the content and scope of the principle of sovereignty as it applies to cyberspace. To explain, sovereignty applies to the physical component of cyberspace, for example to cyber infrastructure which is located within a state's territory or jurisdiction. Sovereignty also applies to the social component of cyberspace, that is to persons – nationals or non-nationals – within a state's territory or jurisdiction. As for the logical component of cyberspace, for example the electronics, sovereignty can apply at the point of entry and exit.[30] Since a state can exercise its sovereignty over the physical, social, and logical components of cyberspace, any unauthorised interference by another state will constitute a violation of its sovereignty.[31] It follows from this that cyber operations against hospitals or health services or information-gaining operations against vaccine research centres constitute violations of the targeted state's sovereignty because they are unauthorised intrusions into that state's sovereign domain.

It has been argued that, for sovereignty to be breached, there should be a minimum threshold of harm in the sense of physical effects or that the interference should target governmental functions.[32] In my opinion, the interference does not necessarily need to produce physical harm because the harm is normative; it is the harm to the principle of sovereignty and its bundle of rights. Moreover, the interference should not necessarily target governmental functions; it can target any infrastructure, even a private one, provided that it is within a state's territory or jurisdiction.

At this juncture it is important to note that a degree of flexibility in how states define their sovereignty is to be expected. States define their sovereignty differently by attaching political, security, economic, social, or cultural aspects thereto and they also attach different degrees of importance to them. Consequently, the requisite threshold of harm or the fields protected by sovereignty may differ and, for this reason, a case-by-case assessment may be required.[33] This is in fact inherent in principles which, as I said, are general regarding their content and scope, and their application to a particular set of facts requires interpretation and contextualisation in contrast to rules which, to use Dworkin's expression, apply in an 'all-or-nothing' fashion.[34]

---

[29] DOD General Counsel Remarks at U.S. Cyber Command Legal Conference https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

[30] Nicholas Tsagourias, 'The Legal Status of Cyberspace', in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Elgar, 2015) 13; US Department of Defense, *Cyberspace Operations*, Joint Publication 3-12 (8 June 2018), I-2

[31] The French position is that 'Any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty.' supra note 15, 6. See also the Position of Finland, supra note 15, 2-3.

[32] Michael N Schmitt (ed). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017), 17-27. For New Zealand, see supra note 25, para. 14.

[33] See for example Finland's position, supra note 15, 3 and New Zealand's position supra note 25, paras 14-15.

[34] Dworkin, supra note 18, 24.

Concluding remarks: the systemic role of sovereignty in cyberspace

What are the systemic consequences of applying the principle of sovereignty to cyberspace and recognising its legal import? In the first place, it embeds cyberspace in general international law and triggers its law-creation, law-enforcement, ordering, and participatory potential, all of which are important for peace and order. Otherwise cyberspace will be treated as a *sui generis* domain or a pre-legal domain subject to naked power. Second, sovereignty ensures the comprehensiveness and cohesiveness of legal regulation in cyberspace because it is a unifying general principle. Otherwise, regulation will become *á la carte*, differentiated, or privatised. Third, the principle of sovereignty remedies legal gaps or legal inconsistencies. As explained, it is the background principle that applies when specific rules do not exist but it can also assist in the interpretation of existing rules. Fourth, and following on from this, it closes responsibility gaps. If responsibility is attached to legal obligations and is a mechanism for ensuring international legality, denying the legal import of sovereignty in cyberspace would mean that no responsibility for these or similar malicious operations can be attached to any state. This state of affairs could invite further malicious operations and cultivate a culture of impunity. The consequences will be disorder or dependency on the good will of states or non-state actors to abstain from such operations, in particular during times of emergency. Fifth, the legal void that the rejection of the principle of sovereignty can create may be filled by norms such as the ones mentioned in the introduction. Yet, there is not only confusion about what norms mean and what behaviour they require but norms also have a voluntary and discretionary normative value. The implications of a regulatory regime based solely on norms is that law will not be a determinative or a mandatory ordering tool and therefore any ordering will become voluntary. Of course, norms can give rise to normative claims but these claims can be inconsistent, lack enforceability, or lack ordering consequences. If instead the normative framework is a mixture of law and norms, this can lead to confusion about what is legal and what is illegal and what is expected as a matter of law or what is expected as a matter of politics, good practice, or morality. With that I do not deny the importance of norms; they can play an important role in guiding state behaviour but, in my opinion, they are meant to complement or reinforce existing law than substitute the law.

In conclusion, what the ‘law of the horse’ analogy teaches us is to revert to the principle of sovereignty and to clarify and contextualise its content and scope in cyberspace.

Cite as: Nicholas Tsagourias, ‘Malicious Cyber Operations against Health Infrastructure during the COVID-19 Pandemic and the Renvoi to Sovereignty in Cyberspace’, ESIL Reflections 9:4 (2020).