**Taťána Jančárková**
Palacký University in Olomouc
tatiana.jancarkova@gmail.com
ORCID: 0000-0003-1520-7162

https://doi.org/10.26881/gsp.2023.2.09

# Sovereignty as a Factor in Securing, Securitizing, and Fragmenting Cyberspace

We live in a globalized world. In its evolution from a system of distinct economic and political entities to an interconnected and interdependent society where geographic boundaries appear blurred and a multitude of actors interact in fluid relations, information and communication technologies (ICT) have been a major catalyst. In enabling a universal exchange of data between any and all devices willing to receive them, the internet has proven to be of major societal, political, and economic value. It has also given rise to a new domain where human activity takes place – cyberspace.

Globalized society has posed a serious challenge, however, to the notion of sovereignty as the cornerstone of the modern legal and political order. Many have considered sovereignty an obsolete concept while others have defended it or introduced innovative views to allow for a plausible interpretation of the new reality where states no longer seem to hold the monopoly of authority and control, but can be forced instead to cede them to or share them with supranational structures or non-state actors.

Nevertheless, if cyberspace has become the epitome of the challenges globalization brings to sovereignty, the threats associated with cyberspace and the use of ICT have actually elevated the sovereignty debate to a new level. This article looks at three possible ways sovereignty, or how the concept is understood, is reflected in and impacts cyberspace – affecting its security, contributing to its securitization, and, possibly, to its fragmentation – to show that sovereignty is by no means an irrelevant concept in cyberspace.

## Sovereignty – one notion, multiple understandings

The popular wisdom has it that sovereignty is the pillar of the modern international legal order as formed by the Peace of Westphalia in 1648 and dating back to the writings of Jean Bodin. In fact, the notion has been challenged and interpreted in multiple ways ever since its conception, and it has often acquired different meanings depending on the lens; law, political science, international relations, and economics are but a few

disciplines offering their distinct perspectives on sovereignty. Multiple sovereignties can thus be said to co-exist, often expressed in dichotomies: legal/political, internal/external, absolute/limited, or unitary/divided.[1] Many definitions refer to sovereignty's internal dimension, and they comment on the authority or the power of a state within its own territory.

The oft-cited 1928 definition of sovereignty by Judge Huber, formulated in the Island of Palmas arbitration case, adds an external dimension when it stipulates that "[s]overeignty in the relation between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State, [making it] the point of departure in settling most questions that concern international relations."[2]

Another well-known interpretation is that of Stephen Krasner who, in his study of sovereignty as "organized hypocrisy," breaks the concept down into four categories: domestic sovereignty, interdependence sovereignty, international legal sovereignty, and Westphalian sovereignty.[3]

Whichever definition of sovereignty we choose, there are always the elements of state authority, control exercised by the state, and the state's territory. Cyberspace, by default, defies them all.

The core infrastructure is mostly owned and controlled by non-state actors. For instance, private companies, academic institutions, or NGOs manage ten of the thirteen name root servers. Online services are mostly offered by corporations that also provide technical solutions used by states in performing their functions. States, in turn, act as clients with a limited degree of control over infrastructure or services. Cyberspace is not organized geographically, either. No state can thus purport to have exclusive jurisdiction and authority over a part of cyberspace. How then does sovereignty project in cyberspace?

## Securing cyberspace

States for long ignored cyberspace. Coming late to digital development, governments did not consider the internet beneficial to advancing their political and economic interests, nor did they find it important for national security.

With time, it turned out that activities in cyberspace had impacts in the physical world and could inflict harm on persons or cause material damage. States had to acknowledge that it was desirable to regulate certain manifestations of those activities in

---

1 S. Besson, *Sovereignty* [in:] *Max Planck Encyclopedia of Public International Law*, OUP 2011, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=MPIL [accessed: 2022.10.09].

2 Permanent Court of Arbitration, Island of Palmas Case (The Netherlands v United States), case no. 1925-01, award, available at https://pcacases.com/web/sendAttach/714 [accessed: 2022.10.09].

3 S. Krasner, *Sovereignty. Organized Hypocrisy*, Princeton 1999.

their territory, or regulate how persons within their jurisdiction behaved in cyberspace in order to fulfil the state's commitments in other domains.

That is how first legislation pertaining to cyberspace came about, criminalizing online child pornography and computer fraud and protecting intellectual property.[4] In the digital world dominated by US-based companies, however, much of the online activity remained protected by the umbrella of the freedom of speech, which is protected by the first amendment of the US constitution.

Therefore, when the French courts ruled against Yahoo! in 2000[5] and ordered it to "take all necessary measures to dissuade and make impossible" French residents' visits to its auction sites selling Nazi memorabilia, and when the US-based internet giant complied, it constituted a breakthrough. Effectively, the ruling introduced geographic identification of internet traffic and geoblocking,[6] and proved that states could exercise some degree of control over cyberspace.

The first manifestation of state sovereignty in cyberspace was one of a normative authority at the domestic level. Following legislation protecting individual rights and economic interests, attention turned toward protecting assets necessary for the delivery and running of important societal services such as energy production and distribution, healthcare, and transportation.[7] Along with the concept of critical infrastructure, the early 2000s and 2010s saw the advent of rules concerning the critical information infrastructure. By according a special status under the law to certain types of infrastructure, states have been able to impose security requirements contributing to greater security of information systems and networks and, consequently, of cyberspace.

These efforts were already motivated by the growing perception of threats from state actors who were capable of delivering cyber effects affecting the capacity of victim states to decide freely on their internal affairs. Cyberspace had become another domain of operations and cyber security a component of national and international security. Thus, securing cyberspace became a corollary to its securitization.

---

4 See, for instance, the US Computer Fraud and Abuse Act of 1986 or the Communications Decency Act of 1996.

5 LICRA et UEJF v. Yahoo! Inc., Tribunal de Grande Instance de Paris, RG 05308 (22 May 2000).

6 M. Lasar, *Nazi hunting: How France first 'civilized' the Internet*, "Ars Technica", 22 June 2011, https://arstechnica.com/tech-policy/2011/06/how-france-proved-that-the-internet-is-not-global/ [accessed: 2022.10.09].

7 It is held that the first software-induced damage of physical infrastructure dates to as early as 1982 when a gas pipeline in Siberia exploded because of a Trojan horse hidden in software allegedly stolen by Soviet industrial espionage from Canada, with knowledge of the US.

## Securitizing cyberspace

Securitization is a term coined by political scientists[8] to describe the process of shifting an issue to become a security concern, justifying thus the extraordinary attention and resources allocated to the matter. The process begins with "speech acts." References to a "cyber Pearl Harbor,"[9] the declaration by NATO of cyberspace as a domain of operations,[10] or the Obama administration's reaction to the SONY hack[11] can be considered as such.

The securitization of cyberspace, however, began with the introduction, by Russia in 1998, of the discussion on the "Developments in the Field of Information and Telecommunications in the Context of International Security," which was included in the UN agenda. Since then, several iterations of groups of governmental experts have contemplated threats originating in cyberspace, norms of responsible state behavior therein, and confidence building measures to avoid a cyber conflict.

In 2013, states agreed that existing international law applied to cyber operations.[12] The modern international legal order is based on the prohibition of the use or threat of force and the principle of non-intervention in internal affairs of states. The latter are considered as equal sovereigns, which is reflected in the relevant clauses of the UN Charter. Sovereignty has thus re-entered the discussion, this time in its external dimension, as the principle underpinning all international legal norms.

Nevertheless, not only it is unclear as yet how international law applies in cyberspace; the states have not reached a consensus on whether sovereignty itself is a rule the breach of which constitutes an internationally wrongful act and entails state responsibility. They have agreed, however, that cyber attacks can, by their effects, amount to the use of force. For those states that recognize sovereignty as a rule, cyber operations against information infrastructure on the territory of another state that does not reach the threshold of the use of force represents a violation of sovereignty. Sovereignty, thus, becomes useful for assessing the international wrongfulness of cyber operations and for informing response options, including self-defense.

Further, sovereignty and its defense have become a handy internal bargaining chip in developing state cyber capabilities. To date, over 60 states have institutionalized

---

8 B. Buzan, O. Waever, J. de Wilde, *Security: A New Framework for Analysis*, London 1998.

9 E. Bumiller, T. Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, "New York Times", 11 October 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-ofcyberattack.html [accessed: 2022.10.09].

10 NATO, *Warsaw Summit Communiqué*, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm [accessed: 2022.10.09].

11 A. Viswanatha, J. Menn, *Obama's Response to the Sony Hack Says a Lot about US Cyber Policy*, "Business Insider", 14 January 2016, https://www.businessinsider.com/r-in-cyberattacks-such-as-sony-strikeobama-turns-to-name-and-shame-2015-1 [accessed: 2022.10.09].

12 United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, 24 June 2013, https://documentsdds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement [accessed: 2022.10.09].

their cyber security and defense in the form of a cyber command, with many of them openly admitting to building offensive cyber capabilities.[13] Cyber warfare has become an integral part of national security and defense doctrines and growing resources are being allocated both to national cyber security and cyber defense.

On the other hand, international law can only be breached by states. How relevant and helpful is it to contemplate violations of international law and argue by sovereignty when most cyber attacks come from non-state actors? Could sovereignty in fact be just an excuse for governments to clamp down on their domestic opponents or simply to stay in power at the expense of individual rights, international cooperation, and economic freedoms?

## Fragmenting cyberspace

As mentioned above, cyberspace is not organized on a territorial basis, neither technologically nor administratively. Its governance is rather a complex network of state, commercial and non-governmental/academic entities. States took a long time to acknowledge the economic and societal potential of information and communication technologies and almost exclusively considered cyberspace in its technological dimension. When they joined in the exploitation, it was too late to impose the traditional model used, for instance, for postal and telecommunication services. Those services had been organized territorially and functioned under state license/concession, which was not a workable model in ICT where voluntarily interconnected autonomous systems are the basic organizational unit.

Internet governance thus relies on a web of organizations and individuals who, often voluntarily, contribute to the maintenance and stability of core internet infrastructure and the formulation of policies, in order to ensure global interconnectivity. This has not been without controversy. For instance, the US government had, for historical reasons, exclusively controlled certain aspects of internet functioning for a long time. The decision-making processes in the key governing bodies such as ICANN left much to be desired in terms of transparency. Projecting frictions from the physical world, some states tried to tilt the balance in favor of an intergovernmental model of governance by shifting the responsibility for internet governance to specialized bodies of the International Telecommunication Union or the UN. Such moves might have also been motivated by the ambition and perceived need to control information and access to cyberspace on the part of states with a more authoritative inkling.

Those states have used the authority granted by internal and external sovereignty to control internet traffic in their territory. In practice, that has led to internet shutdowns,[14] forcing providers to process clients' data in the state's territory and even

[13] J. Blessing, *The Global Spread of Cyber Forces, 2000–2018* [in:] *13th International Conference on Cyber Conflict: Going Viral*, eds. T. Jančárková, L. Lindström, G. Visky, P. Zotz, Tallinn 2021.

[14] Access Now reports up to 182 internet shutdowns in 34 countries in 2021 alone. See Access Now,

the obligation to cooperate with law enforcement bodies. Some of them have used national sovereignty and ensuing security concerns as a justification for creating "national segments" of cyberspace.[15] Such activities negate the founding premise of the internet– universal connectivity – leading in the extreme to the splintering of the internet. At the same time, they show that sovereignty provides an impetus for political and technical decisions impacting and transforming cyberspace and its stability.

Against the background of growing state competition, creating an "open, free, secure, and stable cyberspace" has proven to be an ever greater challenge.

## Conclusion

Any debate on sovereignty and cyberspace eventually involves quoting from John P. Barlow's Declaration of Independence of Cyberspace. In 1996, Barlow excluded governments from the governance of the new, artificial domain.[16] Little did he know that thirty years later, states would ascertain their authority in and over cyberspace in all kinds of contexts. Today, even Western companies seem to have grown to accept some forms of cyber sovereignty. The statement of France's former president, Sarkozy, that the internet "is not a parallel universe which is free of rules of law or ethics or of any of the fundamental principles that must govern and do govern the social lives of our democratic states"[17] has found its extreme confirmation in Russia's information security doctrine of 2016 and its law on the "sovereign internet" of 2019.

While national security concerns can justify a certain level of restriction, the basic premise of internet, however, which is freedom of information and communication, inevitably suffers. Nevertheless, in principle it makes sense to regulate human behavior in cyberspace, a human-made environment.

Sovereignty in cyberspace therefore is not a myth; it is rather what one makes of it. It is, as in other domains, a multi-faceted concept, the flexibility of which has allowed it to remain relevant over time, but also most dependent on the prevailing interests of its subjects.

## Literature

Access Now, *Internet shutdowns in 2021: The return of digital authoritarianism*, 28 April 2022, https://www.accessnow.org/wp-content/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

---

*Internet shutdowns in 2021: The return of digital authoritarianism*, 28 April 2022, https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf [accessed: 2022.10.09].

15 Among them, China with its Great Firewall and Russia with its "sovereign internet".

16 J.P. Barlow, *A Declaration of the Independence of Cyberspace*, 8 February 1996, https://www.eff.org/cyberspace-independence [accessed: 2022.10.09].

17 M. Lasar, *Nazi hunting…*

Barlow J.P., *A Declaration of the Independence of Cyberspace*, 8 February 1996, https://www.eff.org/cyberspace-independence.

Besson S., *Sovereignty* [in:] *Max Planck Encyclopedia of Public International Law*, OUP 2011, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472?rskey=eOob0X&result=1&prd=OPIL.

Blessing J., *The Global Spread of Cyber Forces, 2000–2018* [in:] *13th International Conference on Cyber Conflict: Going Viral*, eds. T. Jančárková, L. Lindström, G. Visky, P. Zotz, Tallinn 2021.

Bumiller E., Shanker T., *Panetta Warns of Dire Threat of Cyberattack on U.S.*, "New York Times", 11 October 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-ofdire-threat-of-cyberattack.html.

Buzan B., Waever O., de Wilde J., *Security: A New Framework for Analysis*, London 1998.

Krasner S., *Sovereignty. Organized Hypocrisy*, Princeton 1999.

Lasar M., *Nazi hunting: How France first "civilized" the Internet*, "Ars Technica", 22 June 2011, https://arstechnica.com/tech-policy/2011/06/how-france-proved-that-the-internetis-not-global/.

LICRA et UEJF v. Yahoo! Inc., Tribunal de Grande Instance de Paris, RG 05308 (22 May 2000).

NATO, *Warsaw Summit Communiqué*, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Permanent Court of Arbitration, Island of Palmas Case (The Netherlands v United States), case no. 1925-01, award, https://pcacases.com/web/sendAttach/714.

United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, 24 June 2013, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement.

Viswanatha A., Menn J., *Obama's Response to the Sony Hack Says a Lot about US Cyber Policy*, "Business Insider", 14 January 2016, https://www.businessinsider.com/r-incyberattacks-such-as-sony-strike-obama-turns-to-name-and-shame-2015-1.

## Summary

***Taťána Jančárková***

**Sovereignty as a Factor in Securing, Securitizing, and Fragmenting Cyberspace**

Information and communication technologies have played an important role in shaping the globalized world we live in today. While it is an accepted fact that globalization has challenged the understanding of the concept of sovereignty, the link between sovereignty and cyberspace is often not thought of at all. There are, however, multiple ways in which sovereignty has affected cyberspace as we know it. This article looks at how the notion of sovereignty contributes to the security, securitization, and, eventually, the possible fragmentation of cyberspace.

**Keywords:** sovereignty; cyberspace; securitization; fragmentation of cyberspace.

## Streszczenie

*Taťána Jančárková*

**Suwerenność jako czynnik zabezpieczający, sekurytyzujący i fragmentaryzujący cyberprzestrzeń**

Technologie informacyjne i komunikacyjne odegrały ważną rolę w tworzeniu zglobalizowanego świata, w którym dziś żyjemy. Podczas gdy faktem jest, że globalizacja podważyła rozumienie pojęcia suwerenności, związek między suwerennością a cyberprzestrzenią jest często w ogóle pomijany. Istnieje jednak wiele sposobów, w jakie suwerenność wpłynęła na cyberprzestrzeń, jaką znamy. Autorka analizuje, w jaki sposób pojęcie suwerenności przyczynia się do bezpieczeństwa, sekurytyzacji, a w końcu możliwej fragmentacji cyberprzestrzeni.

**Słowa kluczowe:** suwerenność; cyberprzestrzeń; sekurytyzacja; fragmentacja cyberprzestrzeni.