# SOVEREIGNTY IN CYBERSPACE. HOW STATES ARE TAKING BACK CONTROL

Edoardo Maria Landoni

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather".

With these words at Davos in 1996, the libertarian John Perry Barlow opened his famous *Declaration of the Independence of Cyberspace*, crystallizing the widespread imaginary of the time: cyberspace as a purely virtual domain, beyond the reach of states and the logic of territorial sovereignty. It was portrayed as a space of individualism and private agency, where the singular prevailed over the collective. A realm imagined to transcend territorial constraints and to be indifferent to borders. Cyberspace, in this vision, did not end at the frontiers of the nation-state, it connected the entire world, challenging the very plausibility, and legitimacy, of applying geographically rooted legal and political authority. Karl Schlögel captured this intuition by giving a name to this "home of the mind": *Cyberia*, an imagined community, a digital nation that went beyond the limitations of local authorities and territorial attachments, and therefore inherently at odds with a traditional Westphalian conception of sovereignty grounded in territorial borders, exclusive jurisdiction, and the possibility of drawing a clear line between an "inside" and an "outside".

This image of cyberspace did not emerge in a vacuum. It both embodied and helped to sustain some of the most powerful myths of that era. It was the era of globalization, widely interpreted as a byproduct of the distinctive American unipolar moment after the Cold War, and marked by liberal optimism in the expectation that openness and interconnectivity – left largely to market forces – would deliver global prosperity and stability. Reinforced by computer-mediated communication, this vision promised an epochal transformation of human experience that would transcend time (the end of history), space (the end of geography), and power (the end of politics). This was evident even in early definitions of cyberspace, which focused primarily on its immaterial aspects, rendering it an a-geographical and a-political new reality. Even the term "cyberspace" itself, some argue, was coined to distance it from the materiality of the "Internet", understood more narrowly as the physical interconnection of networks. Here, physicality was deliberately put aside and cyberspace was framed as a realm of "pure spirit", a place where humanity might unite under the banner of freedom.

This vision however, was not as simplistic or naive as it may appear from this brief reconstruction, it reflected serious attempts to grasp the magnitude of the transformations underway. This should not be taken to mean that security concerns were absent, or that states ignored the infrastructures sustaining the digital realm. Skeptics were

tnote
TORINO WORLD AFFAIRS INSTITUTE

A technician inspecting server racks inside a modern data center. *Source: Wikimedia Commons*

critical of cyber-optimism and warned early on about systemic vulnerability, cascading failure, and the possible strategic uses of the new interdependence. Yet, it must be acknowledged that this narrative contributed to a wider misreading of power relations in the cyber domain. The more consequential point was in fact that the idealized narrative of a borderless, self-regulating cyberspace shaped deeply early approaches to cybersecurity as well as governance. Even as threats began to materialize, responsibility for security was often treated as something best delivered by private actors and market incentives, with the state expected to remain relatively marginal. A stance that would be revised only gradually, as cyberspace was increasingly recognized not as an *exceptional* domain, but as a strategic environment – akin to land, sea, air, and space – shaped by rivalry, coercion, and contestation.

From the early 2000s the change in cybersecurity discourse was also, more fundamentally, a change in the language on sovereignty. The liberal premise of the 1990s began to erode as states were forced to relearn a basic fact: with the emergence of this new domain, the effective exercise of political authority also depends on who controls the communications backbone and who holds jurisdiction over data; two functions that, in much of the West, telecommunications liberalization had largely shifted into private hands. Moreover, as digital interconnection deepened, it became harder to sustain the assumption that integration would automatically yield cooperation and security. Interdependence increasingly came to be seen as a source of leverage, something that could be weaponised by exploiting the vulnerabilities it creates.

As threats proliferated and cyber operations became more entangled with interstate conflict, the problem of (re)asserting state sovereignty moved to the center of Western debates. The 2013 *Tallinn Manual* offers a revealing marker of this shift, starting from its very first rule on sovereignty. It is hardly accidental that the *Manual* emerged as a direct consequence of the 2007 attacks on Estonia's networks, a crisis that pushed NATO to create the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in order to strengthen Allied and partner capability and cooperation in cyber defense. One of the Centre's most important outputs was, in fact, the *Tallinn Manual*, which remains a crucial reference point for understanding the broader conceptual reorientation towards cyber governance, anchoring it to the principle of sovereignty: "A State may exercise control over cyber infrastructure and activities within its sovereign territory. [...] States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure [...] cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State". Thus, sovereignty returns in its most traditional form through territorial control and enters cyberspace through the material infrastructure that anchors it to the ground and ultimately makes it function. Cables land somewhere, data fall under a jurisdiction, and access is mediated by operators and infrastructures that states can regulate, constrain, or even disconnect.

If this discursive and political trajectory is true in most western countries, for Russia and China, sovereignty in cyberspace was never an afterthought. This domain was read from the very beginning through a state-centric lens, as an arena in which external influence could penetrate domestic order. With these lenses, the "open internet" appeared less as a neutral public good than as an infrastructure shaped by western – and US in particular – influence, and therefore as a potential instrument of intrusion. The Arab Spring and the Snowden revelations reinforced this view, strengthening the claim that control over the information environment was inseparable from regime security and political stability. Russia and China did not merely look at cyberspace through a sovereignty lens but they tried to build sovereignty directly into the architecture (normative and infrastructural) of their domestic networks. In Russia, this has meant a long-running effort to insulate the national information space through the project of a sovereign RuNet (Russian Network): a mix of regulation and infrastructural measures meant to manage traffic within national boundaries and tighten control over data routing and key points of international interconnection. China, for its part, has explicitly framed its approach to cyber governance through the notion of "cyber sovereignty", understood as the principle that each state has the right to independently choose its path of digital development and its model of internet regulation, and to exercise administrative and judicial authority over cyber infrastructure, data, and online activities within its jurisdiction.

As seen, this logic is no longer confined to the so called "revisionists powers". Western countries have increasingly moved in the same direction, even if under different vocabularies and legal frameworks. In the EU, "digital sovereignty" has become a pivotal policy agenda centered on tighter data governance, stronger platform regulation, and the development of trusted infrastructures meant to reduce critical dependencies, including through the reshoring (or friend-shoring) of sensitive segments of digital supply chains. In the United States, a similar strategic impulse has taken shape through a national security-oriented regulation combined with industrial policy, and supply-chain strategies intended to secure leverage over foundational technologies.

> **What is often described as "virtual" is being brought back under territorial logics, through control over where data are stored and processed, which infrastructures and providers are considered trustworthy, and how cross-border connectivity is governed.**

Overall, these trends unequivocally indicate that the digital domain has become a space in which states increasingly seek to reassert sovereignty. The multistakeholder ideal has not disappeared as a normative reference, but it is increasingly subordinated to state power and strategic competition. What is often described as "virtual" is being brought back under territorial logics, through control over where data are stored and processed, which infrastructures and providers are considered trustworthy, and how cross-border connectivity is governed. The utopia of a global borderless and interconnected cyberspace has largely lost its appeal and in its place, a growing "sovereignty fever" is pushing states to reassert jurisdiction and control, contributing to the political and technical fragmentation of the global internet.

**Edoardo Maria Landoni** *is PhD Candidate in Political Science at the University of Milan. His research focuses on geopolitics and strategic studies, with particular attention to how information and communication technologies reshape power, security, and international competition.*