Freuler, Juan Ortiz

Article

Infrastructural power: State strategies for internet control

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Freuler, Juan Ortiz (2025) : Infrastructural power: State strategies for internet control, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 14, Iss. 2, pp. 1-27, https://doi.org/10.14763/2025.2.2009

This Version is available at:
https://hdl.handle.net/10419/321976

INTERNET POLICY REVIEW

Volume 14 **Issue** 2

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Infrastructural power: State strategies for internet control

Juan Ortiz Freuler *University of Southern California*

DOI: https://doi.org/10.14763/2025.2.2009

Published: 20 May 2025
Received: 28 May 2024 **Accepted:** 1 October 2024

Funding: The author did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Ortiz Freuler, J. (2025). Infrastructural power: State strategies for internet control. *Internet Policy Review*, *14*(2). https://doi.org/10.14763/2025.2.2009

Keywords: Internet governance, Points of control, Digital sovereignty, Infrastructural turn, internet fragmentation

Abstract: This article explores the implications of the infrastructural turn in internet governance, a policy shift where nation-states increasingly assert sovereignty through material interventions in the internet's physical and technical architecture. I propose a typology of six strategies that nation-states deploy over key locations and levers within the internet infrastructure, referred to as points of control. These strategies include subsidising new network edges to circumvent certain nodes, adding a neutralising layer around points of control, breaking up key nodes, diversifying governance, hijacking the point of control, or creating smaller local nodes. Each strategy is illustrated by an example of how a nation-state deployed it within a particular context. The typology provides scholars with a novel analytical framework for examining internet governance preferences, while offering policymakers a practical roadmap for advancing digital strategic autonomy and resisting coercion, and shaping initiatives like the Non-Aligned Tech Movement. By focusing on how governments exercise infrastructural power, the article contributes to debates on sovereignty and digital decolonisation, while challenging the paralysing narrative of internet fragmentation.

ACKNOWLEDGEMENTS

The author extends gratitude to Hernan Galperin, Lucia Bosoer, Francesca Musiani, Nathalia Foditsch, Carolina Batista Israel, and Frédéric Dubois for their insightful comments on an early draft of this article. The author also thanks participants of the Pacific Telecommunications Conference (PTC) and the Digital Non-Alignment Workshop at the Freie Universität Berlin, as well as the Internet Policy Review team for their constructive feedback that significantly strengthened the final manuscript.

Introduction

> *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.*
> – John Perry Barlow

In February 1996, from Davos, Switzerland, the co-founder of the Electronic Frontier Foundation and former Grateful Dead songwriter, John Perry Barlow, released the Declaration of Independence of Cyberspace (Barlow, 2016). Through it, he called on governments to stand back and allow cyberspace to evolve without their control. In Barlow's declaration, the concept of cyber-*space* is taken quite literally to refer to a separate space, a manoeuvre which is then leveraged to claim "governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you…Cyberspace does not lie within your borders." The declaration was a direct response to the US Congress' Telecommunications Act, which sought to establish a broad set of rules governing the internet, and which would be (mostly) struck down by the Supreme Court months later.

Four years after Barlow's declaration, in March 2000, while speaking at John Hopkins University on international trade, then US President Bill Clinton claimed that it would not be possible for the Chinese government to control the internet, stating that it would be like "nailing Jello to a wall" (C-Span, 2000). While Barlow's position was a normative one, arguing that the government *should not* get involved in regulating the internet, Clinton's was a descriptive statement according to which there was nothing the governments *could* do to regulate the internet. The growing

field of internet governance is one where experts seek answers to both questions: what *can* be done, and what *should* be done. This article builds on the work of a varied set of internet governance scholars to address these questions and seeks to move the debate forward by placing the focus on *how* governance is being exercised through infrastructures.

This article builds on the notion that the infrastructural turn in internet governance requires a similar analytical turn in scholarly analysis of internet governance. One which focuses on the analysis of network architectures (Musiani, 2013). The article begins by illustrating how internet governance scholars have come to recognise that governments *can* shape information flows through infrastructural design. Then, I build on the work of Julia Pohle and others (Pohle & Thiel, 2020; Pohle & Santaniello, 2024) to argue that the rise of the sovereignty narrative over the past decade reflects a growing belief that governments *should* intervene. These shifts move public debate beyond the notion that such interventions pose an unacceptable risk of fragmenting the internet. Consequently, it is reasonable to expect an increased interest among policymakers to reorganise information and communication infrastructures and explore new architectures.

This article contributes to the internet governance scholarship and debates by presenting a typology of government strategies targeting points of control, key locations and levers within the internet infrastructure that influence the flow of information. The typology shows how government action can consolidate or redistribute power. Each of the six strategy archetypes is illustrated through the examination of real-world interventions. The article concludes that the shift towards localised control mechanisms reflects the shortcomings of the global multistakeholder governance model. Some of the strategies described could help peripheral nation-states protect their strategic digital autonomy in a world where interdependence has been abused for coercion by the most powerful governments and companies.

Conceptual framework

Internet governance: descriptive accounts

In observing the degree of unplanned interconnectedness that societies were achieving, Helen Margetts and others have underlined the “political turbulence” such new technological arrangements would bring forth (Margetts et al., 2015). An understanding of the underlying architecture has led academics like Carolina Aguerre to argue that governance over the internet is inherently polycentric, where

"governance is diffuse and complex across multiple sites and layers" (Aguerre et al., 2024). Rather than *turbulence*, Aguerre and colleagues argue that "polycentrism involves both the 'chaos' of multitudinous actors and the 'order' of social structures" (p. 7). Others, such as Joseph Nye, have chosen to refer to this challenge in terms of a "Regime Complex" (Nye, 2014), a formula developed by political scientists seeking to make sense of areas of international relations where "things were generally working but for which there was no existing international law" (DeNardis et al., 2020).

Indeed, as the aforementioned authors suggest, the inherent complexity of the internet architecture, and particularly the fact that it is in constant evolution, make it difficult to provide a full description of how power is exercised over and within it. However, evidence suggests that governments, notably the US government as revealed by Snowden in 2013, have exerted indirect control over information flows in systematic ways. Thus, while mapping the entire system may be elusive, observing inputs and outputs traversing the network offers insights into the effects of various levers. Laura DeNardis, David Clark, and Jonathan Zittrain highlight the resurgence of established power dynamics, as actors seek to identify and manage these levers as 'points of control' across the network (Clark, 2012; DeNardis, 2012; Zittrain, 2003). While the internet may exhibit polycentric governance, certain centres wield disproportionate power. Recognising and understanding these points of control is a crucial step towards ordering elements within the polycentric governance framework.

After years of analysis, DeNardis, alongside Francesca Musiani and others, contend that there is a growing focus on infrastructures within internet governance circles (Musiani et al., 2016). This shift entails a redirection of efforts from global governance forums and standard-setting arenas towards physically controlling critical network components. Examples include enforced data localisation to ensure adherence to local laws, backed by the threat of taking physical control over servers or operators. Within a framework of polycentric internet governance, as characterised by Aguerre, the authors would argue that the absence of central authority enables actors to leverage points of control to pursue specific agendas.

In synthesis, because the boundaries of the internet itself are unclear and constantly shifting, defining internet governance becomes a complicated task. This answer creates discomfort because it points to known-unknowns that, given the importance of the question, the public expects answers to. Rather than seeking complete answers at the systems level, some scholars argue that we should focus on points of control, which can be defined as the discrete mechanisms and junctures

within the internet's architecture and governance that enable those who control them to modulate, restrict or shape information flows. These points of control, which can be managed through technical, economic, and policy-based levers, have become central to the strategies of governments and incumbent corporations seeking to protect their interests, and they are the centrepiece of this article.

Internet governance: sovereignty and the normative accounts

Within the normative frameworks that are developed to advocate for government intervention in digital infrastructure, the concept of digital sovereignty stands out, particularly in relation to the infrastructural turn. Pohle and Thiel (2020) define digital sovereignty as the "idea that a nation or region should be able to take autonomous actions and decisions regarding its digital infrastructures and technology deployment" (p. 8). Cutting through abstract obfuscations like 'the cloud', this conceptualisation of digital sovereignty places the focus on material infrastructures, uncovering how these infrastructures are tethered to territories where nation-states have historically exercised their authority (Lespinois, 2017).

In this context, therefore, digital sovereignty refers to a desire by national governments to shape the way in which the internet operates within their territory. Given the displacement of the nation-state in dominant globalisation narratives of the 1990s and 2000s (Castells, 2009), the rising interest in digital sovereignty since the 2010s is often discussed as marking a resurgence of the nation-state, which in turn contributes to the fragmentation of the globalised system (Pohle & Santaniello, 2024, p. 13).

As Couture and Toupin (2019) note, however, variations of the term digital sovereignty are employed to convey a broad spectrum of meanings, often displacing the state from the centre and coalescing around some notion of individual or collective control. Pohle and Santaniello (2024) also acknowledge that within the nation-state-centric models, both democratic and authoritarian regimes have embraced the concept and suggest that such diversity might strengthen the concept's prospects of gaining traction, with its definition evolving as the discourse surrounding it matures.

Confronting this process of change are a variety of stakeholders, including those who perceive such changes as a threat to the dominant positions they have secured within the existing network (Avila, 2018). These actors often deploy variations of the precautionary principle, arguing that infrastructural modifications risk irreversible harm to the internet 'as we know it.' Within this discourse, the narrative

of fragmentation functions as a rhetorical tool, framing state-led interventions as unacceptable threats to the internet's unity rather than legitimate acts of sovereignty

The fragmentation narrative

Traditional conceptualisations of internet *fragmentation* refer to the breakdown of the paths between platforms, territories, or companies[1]. In a 2016 report, Drake, Cerf, and Kleinwächter observed that prevailing conceptualisations of internet fragmentation predominantly centred on the absence of technical interoperability between information technologies. Nonetheless, they contended that such definitions were incomplete and proceeded to delineate three distinct manifestations of fragmentation: technical, governmental, and commercial (Drake et al., 2016). This article primarily contributes to discussions associated with the governmental elements: "Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources" (p. 7)[2]. However, while useful for describing surface-level disconnections, the term "fragmentation" is part of a narrative that is facing an existential crisis.

The resurgence of the nation-state as a central actor in internet governance has destabilised the once-dominant fragmentation narrative. This sovereignty-centred discourse reframes state intervention not as a threat to the internet's unity, but as a legitimate assertion of autonomy coming from within the network, a rhetorical shift that directly challenges the precautionary principle's reliance on narratives of *loss*. These narratives of loss, which portray continuity as inherently positive, implicitly defend the power asymmetries embedded in the existing network. This tension is illustrated by the US government's reversal as its own dominant position within the network is weakening (Winseck, 2019): once a vocal critic of state-led interventions (e.g., condemning India's early data localisation proposals [Basu, 2020]), the US then began to openly advocate for governments to exclude Chinese companies from global networks under the guise of "purity" and "freedom" (US Department of State, 2020, 2022). This pivot reflects a broader recognition among powerful states that reducing exposure to adversaries, once decried as unacceptable fragmentation, can serve strategic interests. Indeed, the same data localisa-

1. Other scholars have preferred the term *splintering* (Greenstein, 2012, p. 15), which I believe has the same problems as fragmentation, while a third group has referred to this phenomenon as *balkanization,* which should be rejected since it glosses over the Balkan's complicated history.
2. Many scholars believe there has been no technical fragmentation, and there is minimal evidence to suggest that countries will attempt to disrupt the interoperability of the various networks that comprise the internet (see Mueller, 2017; Pohle & Voelsen, 2022; Pohle & Santaniello, 2024).

tion policies that the US previously framed as problematic are proliferating globally (Ferracane & van der Marel, 2024), underlining how geopolitical competition and a quest for digital sovereignty are reshaping norms and expectations.

Given that the same phenomenon of connection is perceived to have different impacts by different actors at different moments in time, it makes sense to separate the processes and procedures implied by *fragmentation* from either positive or negative connotations. By zooming into the activity surrounding the network's "points of control" this article moves beyond the paralysing narrative of internet fragmentation to analyse the strategies deployed by the nation-states reshaping the internet's topography. To facilitate this step beyond fragmentation, I propose the term *re-networking*. This term underlines the internet is *always and only becoming*; that change can, and often is, guided by human decisions that merit discussion, and that the overall number of connections is generally increasing (there is no net loss), even when some specific connections are being degraded or cut.

Having established that the shape of the internet is in constant flux, it becomes clearer that actors will try to ensure the network adopts a shape that advances their corporate, community or state interests. The typology developed throughout the next sections underlines the variety of ways in which governments are re-networking the internet, and the different impacts it can have.

Managing internet points of control: a typology of strategies

In the previous sections, I established that although internet governance is polycentric or diffused, there are a variety of mechanisms through which governments can seek to advance their policy goals. Scholars often highlight the difficulty of portraying internet governance as a formal and coherent system. Meanwhile, as this section illustrates, governments have taken an *infrastructural turn* to modulate how people within their territories interface with global networks. Governments identify and target what Laura DeNardis refers to as *points of control*: discrete mechanisms that enable shaping information flows. Recognising that "arrangements of technical architecture have always inherently been arrangements of power" (DeNardis, 2012, p. 721), policymakers are re-networking infrastructure into architectures that better align with their policy goals.

As the infrastructural turn continues to be fuelled by attempts to advance digital sovereignty, policymakers will increasingly be expected to manage points of control, either to leverage them or diffuse the power others can exercise through

them. This article offers policymakers a tool to explore possible infrastructural interventions. It is a response to Musiani's (2022) call to analyse the critical spaces where sovereignty is contested and, zooming in to trace re-arrangements, identify "what particular loci of power are constituted by material activities of infrastructuring" (p. 792).

To examine this process and shape it, I begin by identifying points of control within the network and strategies that can be leveraged to advance distinct governance agendas and reshape the power dynamics around them. Each of the six strategies is illustrated by iconic examples of their deployment, which are examined through a political economy lens: For each example, I trace how different interests and state power intersect within a specific context, and how this results in a reshaping of infrastructural control. The discussion section synthesises the process visually (Figure 1) and explores the themes emerging from the analysis. This historical and structural analysis shows how power can be wielded within what was described as complex, polycentric governance networks.

While this typology is not exhaustive, it provides a structured framework for understanding and exploring strategies towards infrastructural re-networking. The selection criteria for the six examples used to illustrate the strategies were prominence, diversity and representativity. Prominence allows examples to be presented without needing to offer a more detailed account of the context. The second criteria were diversity both in terms of geography, which shows that the infrastructural turn is a global phenomenon, and in terms of the layer of the internet stack where the point of control is located, which helps understand the breadth of interventions. Future research could expand this compendium to include less visible cases or non-state interventions.

Subsidising new edges to reduce the relevance of a point of control: the EU-Brazil undersea cable circumventing US landing points

Governments can develop infrastructure that allows internet traffic to bypass the point of control, thereby reducing the ability of that specific node to be leveraged as a point of control against them. Rather than focusing on policy development, this strategy relies on deploying infrastructure. For example, Brazil's construction of a new undersea cable intended to reduce its dependence on US infrastructure.

Over the past decades, Brazil has risen to become the 9th-largest economy by GDP (World Bank, 2024), while maintaining good relations with the US, EU, and China, in line with a Constitutional mandated foreign policy of self-determination, often

construed as non-alignment (Hughes & Bridi, 2023; Stuenkel, 2020). Internet governance, however, is an arena where Brazilian interests and policies have clashed directly with those of US companies and institutions.

In 2013, Edward Snowden showed how the National Security Agency (NSA) was leveraging private corporate infrastructure for espionage. Among the many areas of the network that Snowden revealed to be compromised were a series of cable landing points in the US through which Brazil routed most of its traffic to the EU (Greenwald, 2014a; Snowden, 2019). The only existing cable connecting South America and the EU directly at the time was the Atlantis-2 cable; a 40 gigabytes per second cable built by a consortium of EU and Latin American companies in the year 2000 (Telegeography, 2013). To put this bandwidth in perspective, US-EU cables at the time had a bandwidth of over 500 gigabytes per second, meaning that traffic from South America to the EU would be organically and typically routed through the US, as it was the fastest route. In fact, one of the slides revealed by Snowden shows the NSA explaining how the existing undersea cable architecture meant that traffic between Brazil and Iran would be routed through the US, where data could be extracted (NSA, 2012, p. 6).

The NSA grouped these access methods under the codename Fairview, the most expensive of the programmes revealed by Snowden, at US$ 189 million in 2011. This price-tag is cheap considering it gave the NSA access to an estimated billion or more messages from Brazilian users (Greenwald, 2014b), and the processing of 60 million foreign emails daily by 2012 (NSA, 2012). Following the revelations, Brazilian President, Dilma Rousseff, stated her outrage at the UN, saying “[w]ithout respect for [a nation's] sovereignty, there is no basis for proper relations among nations” (L. Clark, 2013).

The Brazilian government saw the Snowden revelations as an opportunity to discuss changes to the internet governance system as a whole, establishing NetMundial in 2014, a conference that sought a political way forward (Almeida, 2014). Meanwhile, beyond seeking to shape the internet governance system at a global level, Brazil also sought to identify and target the points of control that directly threatened its sovereignty. In the immediate aftermath of the Snowden revelations, Brazil, with financial support from the EU, expedited the construction of a direct link to the EU, the EllaLink, initially planned in 2012. This cable provided much needed capacity, while allowing traffic to circumvent the US landing points that had been used to intercept critical information exchanged between these regions (Reuters, 2014). The new EllaLink offers 3125 gigabytes per second through each of its four fibre pairs (Knight et al., 2016; Submarine Networks, n.d.), or 78

times the bandwidth of the pre-existing cable. In 2015, during press interviews at the project's launch, the Brazilian government official overseeing the initiative explained its significance by highlighting the risks of routing internet traffic through the US, referencing Snowden's revelations (Boadle, 2015).

Adding a neutralising layer around the point of control: India's Open Network for Digital Commerce

Governments can develop protocols that neutralise the power an actor can exercise over a point of control. This approach consists of reorganising how existing physical infrastructures can operate by relying on a combination of software and regulation. This strategy, for example, was deployed by India to manage the risks of a highly consolidated e-commerce sector.

While in 2025 India accounted for around 16% of the world's internet users, only around 55% of its population was using the internet (Statista, 2025). Government officials seem to recognise that capturing value locally is critical to minimising economic disruption as internet penetration expands. According to GitHub, the most popular platform for programming tasks, India has 9.75 million users, and added 2.5 million users in 2022 alone, which led the platform to project that by 2025 India will have equalled the US in number of GitHub developers (GitHub, 2023). However, and in contrast with China, India still cannot boast major global platforms, like TikTok. While China put a firewall around its territory and developed homegrown technologies under tight state scrutiny, in India the multinational tech companies came first, and regulatory scrutiny later. In 2025, for example, the web layer of the internet was controlled by US companies like Google, which had over 89% of the Web browser market and 97% of the search engine market in India (StatCounter, 2025). These percentages were higher than the world average, and higher than in other large emerging economies, like Indonesia or Brazil. Perhaps this explains why the government is seeking to create space for local businesses in the app layer often referred to as web 2.0. A way in which the government seems to be approaching this challenge of capturing value locally involves leveling the playing field through competition-enhancing policies against established companies[3].

India has deployed this neutralising strategy to shape e-commerce, a sector which

3. Another argument is that the population's low levels of disposable income mean consumption is still relatively low and the value of their data for the ad-targeting systems is minimal. Thus, the government sought to create a system where the data adds value for the citizen instead of the platform, which is where the account aggregator model comes in, placing a point of control under tight government scrutiny, as opposed to a multinational company.

is growing rapidly. Whereas it represented US$ 30 billion in 2020, it reached US$ 123 billion in 2024 and is projected to reach US$ 300 billion by 2030 (Statista, 2025). Meanwhile, Amazon and Flipkart together control over 70% of the e-commerce market (Statista, 2023). This degree of consolidation fuels concerns that, as internet use grows, it might further consolidate wealth and create joblessness (Khan, 2017). Since medium and small enterprises generate 60% of employment in India, Prime Minister Modi has repeatedly underlined the need for "equitable competition between large and small sellers" (Economic Times, 2023). The government of India has developed a set of government-centric building blocks that neutralise the existing points of control in e-commerce while increasing the government's ability to modulate their operations. These blocks are identity, data, and payments, through which the government has created an Open Network for Digital Commerce (ONDC).

In terms of identity, India developed Aadhaar, a system of biometric identification that enables the government to assume a role often played by platforms in certifying a person's identity and characteristics (e.g. authenticating identity on new online service by using Facebook credentials). While streamlining online trust by creating offline traceability for online interactions, Aadhaar has raised concerns regarding privacy and state surveillance (Jujjavarapu, 2017).

Meanwhile, through the Digital Personal Data Protection Act (2023) and data localisation policies, the government took steps to have multinational companies build infrastructure to localise data, stating that this would increase economic growth, boost employment, prevent foreign surveillance and secure access for local law enforcement (Grover et al., 2024, Burman & Sharma, 2021). The government announced it seeks to increase the sharing of anonymised data with homegrown companies, assuming their growth is in the national interest as they would be better aligned with national goals (Pandai & Samdub, 2024). Lastly, the government created a new layer of infrastructure to facilitate such sharing, through standardised open systems. This includes account aggregators that, relying on Aadhaar authentication, operate with fiduciary duties towards the user, intermediating with other applications to navigate consent and permissions, and which seek to reassure users that data exchanges across sectors and platforms are secure and consent-based (India Stack, n.d).

The third bloc is the Unified Payments Interface (UPI), launched in 2016. This is an open source, interoperable payments system managed by the Reserve Bank of India. It facilitates digital payments while diffusing the point of control in the hands of incumbent players, such as credit card payment processing companies. UPI has

become the preferred mode of payment in India and is the global leader in terms of volume of transactions, ahead of its Chinese equivalent (WEF, 2023).

These building blocks converge in the Open Network for Digital Commerce (ONDC), a government-led initiative that neutralises the existing point of control in e-commerce. The ONDC shores up competition by unshackling the hold platforms exercise over key elements such as identity (simplified through Aadhaar), which is central to the reputation building that allows buyers and sellers to trust each other. The government created an open protocol that unbundles these data from the platforms and allows sellers on one platform (e.g. Amazon) to engage with buyers who have set up a profile through other platforms (e.g. Flipkart), while also allowing them to move their identities and reputations across platforms (Dash et al., 2022).

The ONDC thus creates the equivalent of a meta-marketplace that is managed by a nonprofit created by the government with the purpose of enabling cross-platform interoperability and reducing user lock-in. Physical shops, in turn, are already using digital payments, which allows them to quickly operate through virtual commerce platforms. The system therefore increases the number of marketplace players, reducing the power any of them can exercise over the market, while placing the government-designed nonprofit as a gatekeeper that defines which actors get access to the meta-marketplace. In this way, the government neutralised the existing points of control managed by payments operators and e-commerce platforms, while increasing its own ability to modulate the operations within this sector through a combination of software, infrastructure, and policy.

Breaking up points of control: the EU mandating operating systems allow sideloading of apps

Governments can develop legislation and regulations that break up existing points of control by deeming the power being exercised at such nodes to be illegal and redistributing such power across the network. This strategy has been deployed by the European Union (EU), which through the Digital Markets Act (DMA) disrupted the control app stores exercised over the mobile ecosystem. Although the EU has few corporations operating as global market leaders in the internet economy (Bradford, 2023), its regulatory power over a large and affluent consumer market allows it to shape global corporate standards, a phenomenon referred to as the "Brussels Effect" (Bradford, 2015). By leveraging this power, EU policymakers destabilise the dominance of the US-based incumbents, indirectly creating more favourable conditions for homegrown companies to compete globally.

In the EU, as in most countries besides China, the market for operating systems is consolidated around Apple's iOS (32% share), and Alphabet's Android (67% market share) (StatCounter, 2024a). Whereas Android allows its users to rely on a variety of app stores, Apple vertically integrated the iPhone device, the iOS operating system, and the app store (Ortiz Freuler, 2023). In this way, it created an extremely effective point of control over what apps people download onto their devices. Apple defends a hefty 30% commission on app purchases and in-app transactions by citing a complex and costly app-vetting system, which they argue is key to user trust and a seamless experience that ultimately benefits app-makers (Marsden & Brown, 2023). In short, Apple acknowledges it created a point of control, but argues it is leveraged to advance the interests of users and app-makers.

App-makers, including prominent ones such as Epic Games, accused Apple of abusing its market power and this point of control to extract value from users and developers alike. In a show of its effectiveness as a point of control, Apple blocked the Fortnite app after it tried to enable payments that would circumvent the app store tax (Sriram et al., 2024). A US court ordered Apple to allow app developers to inform users about alternatives to Apple's in-app purchase system (Robertson, 2021). In contrast, in 2022, the EU took a legislative approach, creating a general rule within the Digital Markets Act (DMA) which, in the context of Apple's app store, forced the company to allow users to download apps from outside the Apple app store, a practice often referred to as side-loading (Pierce, 2024; Diaz, 2024).

In this way, EU legislators reduced the power Apple can exercise at this point of control by breaking it open, creating a new set of nodes through which app developers and users can connect: the web. In contrast with the ONDC strategy put forward by the Indian government, the EU did not develop government-centric building blocks. Instead, the EU expects the private sector to develop trust-enabling alternatives to those developed by Apple, and which Apple argued justified the large fees it extracted at the point of control.

Diversifying governance over points of control: the example of ICANN

Governments can diversify governance over points of control by transitioning authority from single actors to multi-stakeholder institutions. This approach redistributes decision-making power, mitigating risk of abuse over a point of control that remains as such, while fostering institutional trust through broader participation. The United States government deployed this strategy to reduce its control over the Internet Corporation for Assigned Names and Numbers (ICANN).

A central player of the original internet architecture, the US government funded and helped operate many elements that have become critical to it, such as the Domain Name System (DNS) (Abbate, 1999). As the internet user-base expanded and technologies increasingly converged onto internet protocols, both private sector companies and foreign governments began to grow concerned about the power the US government could exercise over it (Berners-Lee, 1999). In 1998, the US Department of Commerce institutionalized control over DNS governance by creating ICANN, effectively replacing the informal, decentralized authority previously exercised by internet pioneer Jon Postel. In doing so, the Department of Commerce gained considerable influence over the root-server system which determines the visibility of top-level domains (TLDs) (Zittrain, 1999). Though ICANN was created as a nonprofit organisation with a global, multi-stakeholder governance model, much of the responsibility for operating the Domain Name System (DNS) was delegated to US-based companies like VeriSign, a publicly traded firm that managed key TLDs such as .com and .net (Mueller & Kuerbis, 2014). As a result, the US government retained a considerable degree of influence over the internet's infrastructure, which some critics argued represented a form of government control (Froomkin, 2000). Although the Department of Commerce never used its leverage through ICANN to directly cut off internet addresses for political reasons, other branches of government leveraged this influence to enforce US laws. A prominent example is the suspension or seizure of domain names belonging to foreign websites accused of violating US copyright laws, such as the Digital Millennium Copyright Act (DMCA) (Zittrain, 2019). US courts supported these actions, extending the reach of US law beyond national borders. This extraterritorial use of power began raising concerns abroad (DeNardis, 2014, p. 61). Meanwhile, requests for the US government to use its influence over ICANN to act beyond copyright enforcement were less successful (Musiani et al., 2016, p. 3).

In 2016, three years after the Snowden revelations, ICANN transitioned into an autonomous nonprofit, ending the US government's formal authority to approve changes to the DNS root zone file. Fadi Chehadé, CEO of ICANN at the time stated: "the trust in the global Internet has been punctured, and now it's time to restore this trust through leadership and institutions that can make that happen", calling for "a new model of governance in which all are equal" (L. Clark, 2013). Soon after, ICANN was transitioned into a non-profit organisation under California law and to be managed by a 16-person board of directors, which appoints the CEO. ICANN also has a governmental advisory committee with representatives from over 170 nation-states (ICANN, 2022). In this way, the US government conceded that increasing trust on the internet after the Snowden fallout required the US to devolve

power over a key point of control (Mueller & Kuerbis, 2014). Unlike India's ONDC or the EU's DMA, which sought to disrupt a point of control, the ICANN example illustrates a strategy aimed at reconfiguring governance structures over a point of control to balance the functionality offered by it with renewed trust that the point of control will not be abused.

Hijacking and controlling points of control: the US government's control over core internet infrastructure

By forging non-public alliances with actors governing key points of control, governments can redirect private infrastructural power to serve national or geopolitical interests. The US government's capture of cable landing points and platform infrastructure for surveillance shows how a point of control can be secretly exploited for strategic purposes.

Following the terrorist attacks of 9/11, the US government modified and enlarged its security apparatus to prevent future attacks. Among the key shifts was the decision to exploit the points of control that had emerged, or could be nurtured into emergence, across the internet (Farrell & Newman, 2019; Ortiz Freuler, 2022). This reorientation is noticeable in the 2003 update to the Department of Defense's Operations Roadmap, which declared that "the Department will 'fight the net' as it would a weapons system" (Department of Defense, 2003). By framing the internet as a battleground, the doctrine contributed to legitimising the reconceptualisation of civilian infrastructure as tools for surveillance and coercion.

As Edward Snowden reveals in *Permanent Record,* the combination of market consolidation around US companies and secret US policies "permit the US government to surveil virtually every man, woman, and child who has ever touched a computer or picked up a phone" (Snowden, 2019, p. 128). The US government took advantage of two key points of control: The landing points within the transport layer of the internet, managed by companies like AT&T, that were described as overly eager to cooperate with the NSA (PBS, 2015), and which enabled the effectiveness of programmes like Fairview, described in the first example. The other point of control consisted of the social media companies like Facebook and YouTube that managed the key servers over which much of the world was starting to interact. This allowed the US government to pull data from intelligence targets abroad knowing they would most likely be exchanging the sensitive information over these dominant platforms. (Greenwald & MacAskill, 2013; Washington Post, 2013). It also allowed the US government to push data into countries seeking to restrict it, such as leveraging the centrality of GitHub within the programmer community to mirror

content restricted by the Chinese government and make it available within China (Open Technology Fund, 2022; Ortiz Freuler, 2022).

The centrality of these companies places them at risk of government antitrust investigations, which, in turn, creates conditions that may make these companies more willing to cooperate with the government in controversial endeavours (Wu, 2013, pp. 237-296).[4]Meanwhile, as the Salt Typhoon hacks on US intelligence backdoors show, nourishing such points of control is risky, since it is not possible for a government's intelligence agency to guarantee that third parties will not exploit it as well (Mullin & Cohn, 2024). This is one of the reasons the Dutch government has developed a policy that prevents its agencies from adopting this strategy (Veen & Boecke, 2020). While inherently risky, this strategy shows that sometimes, instead of disrupting or weakening a point of control, governments can covertly exploit the private companies managing them to advance their own agendas.

Regulating the operations of points of control by breaking away parts into localised nodes: the example of data localisation

Governments can enact legislation and regulations to split large points of control to create a smaller, localised node, which is easier to manage and modulate by local authorities. This strategy is being deployed by many countries through what is referred to as *data localisation*.

The rise of the internet and the ad-based revenue models has made data collection central to most online businesses (Rao, 2023). Furthermore, leading companies claim that ever larger data sets are necessary to increase the performance of their artificial intelligence systems, increasing the perceived financial and strategic value of controlling data and data processing (Thornhill, 2023). Meanwhile, economies of scale in storage and computing (Williams, 2012, pp. 52-61) have led to market consolidation. In 2024, Amazon Web Services (31%), Microsoft Azure (25%) and Google Cloud (11%) dominated the global cloud infrastructure market (Statista, 2024). While the market is consolidated, the infrastructure is increasingly

4. An example of this dynamic was exposed in a Congressional hearing when a Republican representative, Matt Gaetz, questioned the degree to which Google had consolidated market power: "Do any of the rest of you take a different view? That is to say that your companies don't embrace American values. It's great to see that none of you do. Mr. Pichai, I'm worried about Google's market power, how it concentrates that power, and then ultimately how it wields it (…) My question, Mr. Pichai is, did you weigh the input from your employees when making the decision to abandon [Project Maven] with the United States military", to which the CEO responded, "As I said earlier, we are deeply committed to supporting the military and the US government" (Rev, 2020). This exchange highlights how the suggestion of antitrust scrutiny can compel companies to publicly reaffirm their alignment with governmental priorities.

geographically distributed across the world. To reassert its control over data flows, in 2018 the US Congress passed the CloudAct (Rutherford, 2019), which ensures US government access to data hosted by US companies abroad, while negotiating reciprocal access for foreign governments. Such laws show that governments see server infrastructure as points of control to be leveraged for economic and security purposes.

Servers represent a major capital expenditure for big tech companies. For example, Amazon reported changes to its accounting practices, which extended the lifespan of servers from four to six years, allowing the company to reduce annual depreciation costs and increase reported revenue by U$ 3 billion in a single quarter, with similar figures reported by other major companies (Hodgson et al., 2024). These precious physical assets thus become a financial pressure point governments are eager to leverage in the context of broader negotiations with big tech companies (Burman & Sharma, 2021). In this sense, data localisation can create a localised point of control through which governments can modulate the operations of multinational companies within their territories.

Over the past decade, most governments adopted data localisation policies aimed at controlling the flow of personal and sensitive data. Whereas in the year 2000, 80% of the 143 sampled countries had an open data model in place, by 2022 this had dropped to 22% (DLA Piper, 2024; Ferracane & van der Marel, 2024, p. 8).

The US, a historical champion of the open data model, is shifting its position under national security arguments. To add an additional example to the examples examined in the typology, the first Trump administration mandated that TikTok host its data on US servers operated by Oracle, a US provider (Chander, 2022), with provisions to audit and vet the curation algorithm (Fischer, 2022). Subsequent legislation might force TikTok's Chinese parent to fully divest or be banned from operating within the US market in 2024 (Allyn, 2024), further illustrating how data localisation can be used to increase leverage over foreign entities.

In contrast, the EU triggers an indirect process of data localisation under privacy and human rights arguments (Bradford, 2020). EU citizens have repeatedly questioned the ability of companies to resist the US government's illegal attempts at espionage when servers are physically located in the US. As cross-border flow agreements between the EU and US come under regular judicial review, the legal uncertainty and regulatory risks of not localising data within the EU indirectly drives companies like Microsoft to store data from EU customers within the EU (Smith, 2021). By framing data localisation as a means to protect citizens' rights,

the EU leverages its regulatory power to fragment global data infrastructure into localised nodes, enabling them to regulate multinational corporations while advancing national security, economic, or privacy objectives.

Discussion: the potentialities of the infrastructural turn

This article dissects a variety of government interventions impacting the internet's infrastructure. The examples presented throughout it can be synthesized into Figure 1. The figure visualizes how nation-states target or develop specific elements and components within the internet architecture to fragment, neutralize or claim authority over points of control across the network.

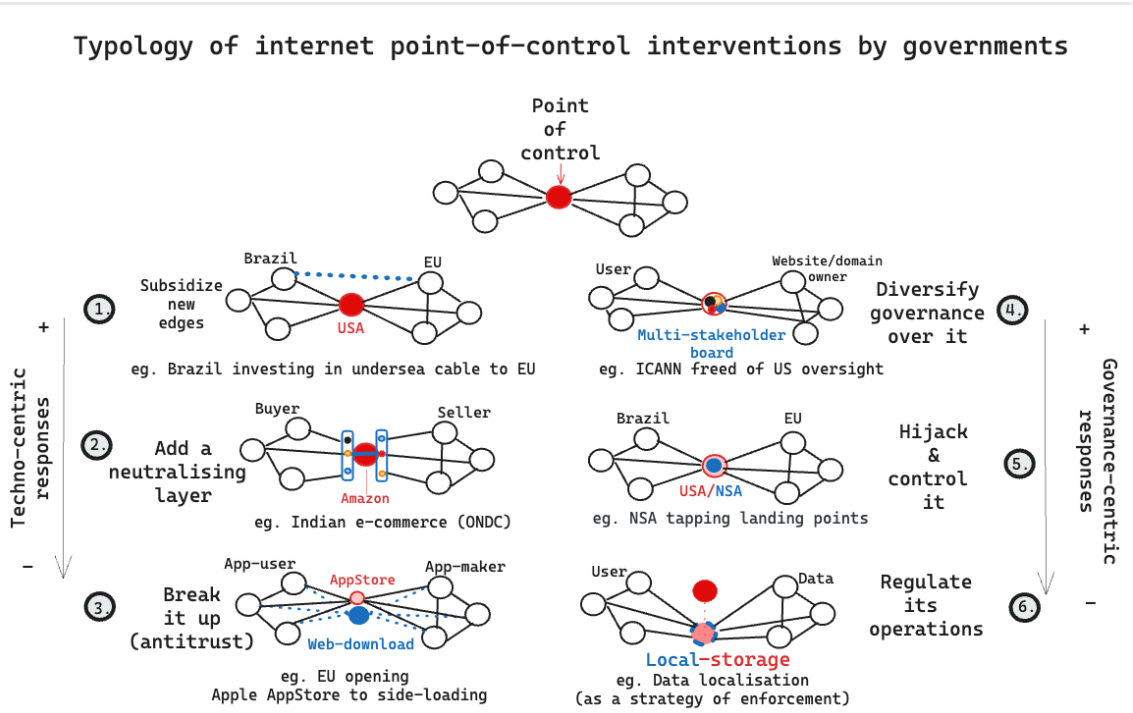

FIGURE 1: A typology of infrastructural responses to the identification of a point of control in the network as deployed by governments across the world (developed by the author).

This typology offers four key insights. First, as Francesca Musiani (2013) notes, "it is possible to design the architecture of our global communication infrastructure in order to promote specific types of interactions over others" (p. 6). The diversity of strategies and geographic examples presented illustrates a policy shift away from global consensus-building towards localised, nation-state driven interventions. The shift in US policy on this front is considerable: from actively criticising data localisation policies (Basu, 2020) to enacting them. These shifts reinforce the conceptualisation of the internet as a dynamic network of networks with an architecture that is in constant re-negotiation. The typology reaffirms that nation-states

are, in contrast with Clinton's statements of regulatory impossibility, actively shaping the internet architecture.

Second, the analysis reveals that the points of control are not static either but can move both vertically and horizontally across the internet stack. For example, while Brazil's undersea cable project (2015) reduced its reliance on US cable landing-points, and ICANN's transition (2016) diminished the US' formal control over the DNS system, the dominance of US platforms in the content and storage layers also increased during such periods, illustrating how the US government could have shifted the point of control up the internet stack. This might also explain the US government's concern over TikTok's growing market share, which could threaten this point of control. Meanwhile, emerging technologies like Starlink's satellite internet (Voelsen, 2021) could represent a horizontal shift within the internet stack, reshaping the power dynamics around data transport infrastructure, like undersea cables. The US' threat to cut Ukrainians off Starlink if they do not agree to US negotiating terms (Shalal & Roulette, 2025), underlines the possible emergence of this point of control within the Ukrainian context. Future research could track these movements over time, classify a broader range of examples, refine the typology, and the conditions necessary for successful deployments of each strategy.

Third, the shifts in US policy suggest that the typology provides a framework for contrasting political rhetoric with actual policy interventions. As Pohle and Thiel (2020) note, sovereignty, which they study as a discursive practice, remains a fluid and contested concept. Contrasting government interventions with public statements could help solidify such understandings of sovereignty and operate as an accountability mechanism in governance forums. This approach aligns with DeNardis' (2012) call to move beyond institutional analyses and towards an examination of the underlying material power (p. 721).

Lastly, the typology contributes to the decolonial turn in technology research (Aouragh & Chakravartty, 2016; Mejías & Couldry, 2021; Lehuedé, 2024) by offering a practical tool to reflect on strategies that might challenge entrenched power dynamics. Specifically, it provides a research agenda for the Non-Aligned Tech Movement (NATM): an independent and emerging network of over 100 researchers, activists, and policymakers initiated by Juan Ortiz Freuler and Ulises Mejias. A key goal of the network is to revisit and update the principles of the Non-Aligned Movement, a 20th-century initiative that sought to secure the autonomy of peripheral countries from the Cold War superpowers (NATM, nd; Ortiz Freuler, 2025). At a time in which politics, economic activity and social interaction are mediated through the internet, ensuring countries and communities can protect their digital

strategic autonomy requires identifying and managing points of control in networks that are increasingly being weaponised by central countries (Ortiz Freuler, 2022).

Conclusion

This article contributes to internet governance scholarship and policy debates by outlining a typology of strategies that can be adopted by governments seeking to shape the effects of the internet within their territories and beyond. Three conclusions emerge from this exercise.

The first conclusion is that governments are increasingly co-shaping the internet's architecture through material interventions, such as subsidising new undersea cables, or forcing the localisation of data centres. This infrastructural turn signals a movement of power from global governance forums to actors willing and able to exercise power over points of control. Meanwhile, there are few, if any, champions of unrestricted information flows left. In short, given the pillars and champions of the internet fragmentation narrative are in crisis, it is time to prepare for an age of rapid re-networking of information infrastructures.

The second conclusion is that some government interventions might increase network resilience by targeting points of control in ways that increase the number of edges or nodes in the network (e.g. responses number 1 and 3 in Fig 1), while it is likely that others (e.g. 5 and perhaps 6) will directly or indirectly reduce information flows through the network. Meanwhile, the strategy of resolving differences in values and interests by relying on a multistakeholder model of governance (e.g. number 4) seems to have lost adherents, given its perceived failures to distribute the value accrued by multinational platforms (Mueller, 2017). Making the governance strategy more attractive requires developing the types of administrative and regulatory bodies that governments have been creating within their territories over centuries, and which remain absent or weak at the global scale.

Third, the analysis shows that whereas larger and more powerful countries and common markets like the US, EU and China, can allocate resources to achieving extraterritorial effects through global standards and governance forums, less powerful governments are likely to focus their limited resources on areas they can directly influence, such as managing local infrastructure. As interdependence is increasingly weaponised for coercion (Farrell & Newman, 2019; Ortiz Freuler, 2022), some states may seek to aim their resources at reducing their reliance on (or exiting) shared networks. Encouraging participants to remain an active part of the

shared network might require limiting the ability of dominant actors to weaponise such shared networks. The typology presented in this article may offer strategies towards reducing such risks of abuse. Collaborating on these technological and regulatory designs could become a central focus of a Non-Aligned Technological Movement aimed at preserving the autonomy of peripheral countries and collectives.

Lastly, future research could contrast government representatives' stated preferences for internet governance with the actual actions their governments take to shape the infrastructure. This could involve applying the article's typology to classify government approaches to a set of key control points. Systematically contrasting policy actions with public statements would strengthen internet governance debates by grounding preferences in empirical evidence rather than rhetoric.

References

Abbate, J. (1999). *Inventing the internet*. MIT Press.

Aguerre, C., Campbell-Verduyn, M., & Scholte, J. A. (2024). *Global digital data governance: Polycentric perspectives* (1st ed.). Routledge. https://doi.org/10.4324/9781003388418

Allyn, B. (2024, March 14). *The House passed a TikTok ban bill. But is the app really a national security threat?* NPR. https://www.npr.org/2024/03/14/1238435508/tiktok-ban-bill-congress-china

Almeida, V. A. F. (2014). The evolution of internet governance: Lessons learned from NETmundial. *IEEE Internet Computing*, *18*(5), 65–69. https://doi.org/10.1109/MIC.2014.98

Aouragh, M., & Chakravartty, P. (2016). Infrastructures of empire: Towards a critical geopolitics of media and information studies. *Media, Culture & Society*, *38*(4), 559–575. https://doi.org/10.1177/0163443716643007

Avila, R. (2018). Digital sovereignty or digital colonialism? *Sur*, *15*(27), 13.

Barlow, J. P. (2016, January 20). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Basu, A. (2020, January 10). *The retreat of the data localization brigade: India, Indonesia and Vietnam*. The Diplomat. https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/

Berners-Lee, T., & Fischetti, M. (1999). *Weaving the web: The original design and ultimate destiny of the World Wide Web by its inventor* (1st ed.). HarperSanFrancisco.

Boadle, A. (2015, September 18). *Brazil to boost internet speed through Europe*. Reuters. https://www.reuters.com/article/brazil-telebras-idINL1N11N12920150918

Bradford, A. (2015). Exporting standards: The externalization of the EU's regulatory power via markets. *International Review of Law and Economics*, *42*, 158–173. https://doi.org/10.1016/j.irle.201

4.09.004

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Burman, A., & Sharma, U. (2021). *How would data localization benefit India?* [Working paper]. Carnegie Endowment for Peace. https://carnegieendowment.org/research/2021/04/how-would-data-localization-benefit-india

Castells, M. (2009). *Communication power*. Oxford University Press.

Chander, A. (2022). Trump v. TikTok. *Vanderbilt Journal of Transnational Law*, *55*(5), 1145–1176.

Clark, D. D. (2012). Control point analysis. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2032124

Clark, L. (2013, October 14). *Brazil to try shielding itself from NSA with national secure e-mail*. Ars Technica. https://arstechnica.com/tech-policy/2013/10/brazil-to-try-shielding-itself-from-nsa-with-national-secure-e-mail/

Couldry, N., & Mejias, U. A. (2023). The decolonial turn in data and technology research: What is at stake and where is it heading? *Information, Communication & Society*, *26*(4), 786–802. https://doi.org/10.1080/1369118X.2021.1986102

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

C-Span (Director). (2000). *Clinton on Firewall and Jello* [Video recording]. https://www.c-span.org/video/?c4893404/user-clip-clinton-firewall-jello

Dash, B., Sharma, P., Ansari, M. F., & Swayamsiddha, S. (2023). A review of ONDC's digital warfare in India taking on the e-commerce giants. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4323963

De Lespinois, J. (2018). La territorialisation du cyberespace: La fin de la mondialisation ? *Prospective et Stratégie*, *Numéro 8*(1), 47–56. https://doi.org/10.3917/pstrat.008.0047

DeNardis, L. (2012). Hidden levers of internet control: An infrastructure-based theory of internet governance. *Information, Communication & Society*, *15*(5), 720–738. https://doi.org/10.1080/1369118X.2012.659199

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. https://doi.org/10.12987/yale/9780300181357.001.0001

DeNardis, L., Cogburn, D., Levinson, N. S., & Musiani, F. (2020). *Researching internet governance: Methods, frameworks, futures*. MIT Press.

Diaz, M., & Wan, K. (2024, April 16). *Let the iPhone sideloading begin! iOS 17.5 lets EU users download apps from the web*. ZDNet. https://www.zdnet.com/article/let-the-iphone-sideloading-begin-ios-17-5-lets-eu-users-download-apps-from-the-web/

DLA Piper. (2024). *DLA Piper Global Data Protection Laws of the World – World Map*. https://www.dlapiperdataprotection.com/

Economic Times. (2023). Prime Minister Narendra Modi for fair competition among large, small sellers in e-commerce. *The Economic Times*. https://economictimes.indiatimes.com/news/india/prime-minister-narendra-modi-for-fair-competition-among-large-small-sellers-in-e-commerce/articleshow/103034444.cms

Emmott, R. (2014, February 24). *Brazil, Europe plan undersea cable to skirt U.S. spying*. Reuters. https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224/

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*, 38. https://doi.org/10.1162/isec_a_00351

Ferracane, M. F., & Van Der Marel, E. (2025). Governing personal data and trade in digital services. *Review of International Economics*, *33*(1), 243–264. https://doi.org/10.1111/roie.12735

Fischer, S. (2022). *Scoop: Oracle begins auditing TikTok's algorithms*. Axios. https://www.axios.com/2022/08/16/oracle-auditing-tiktok-algorithms

Froomkin, A. M. (2000). Wrong turn in cyberspace: Using ICANN to route around the APA and the constitution. *Duke Law Journal*, *50*(1), 17–186. https://doi.org/10.2307/1373113

GitHub. (2023). *Global distribution of developers. The state of the Octoverse*. https://octoverse.github.com/2022/global-tech-talent

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S.* Surveillance State. Metropolitan Books.

Greenwald, G., Kaz, R., & Casado, J. (2014, January 25). *EUA espionaram milhões de e-mails e ligações de brasileiros [The US spied on millions of emails and phone calls from Brazilians]*. O Globo. https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Grover, R., Jang, K., & Su, L. W. (2024). Beyond digital protection(ism). *Journal of Information Policy*, *14*, 161–193. https://doi.org/10.5325/jinfopoli.14.2024.0005

Hodgson, C., Criddle, C., & Kinder, T. (2024, February 5). *Big Tech boosts profits by $10bn with accounting change to server life estimate*. Financial Times. https://www.ft.com/content/ad2f407c-633a-431e-874b-44df53acc68a

Hughes, E., & Bridi, C. (2023, March 16). *Foreign policy of Brazil's Lula takes shape, irking the West*. AP News. https://apnews.com/article/brazil-lula-foreign-policy-us-venezuela-iran-2ca10d070df6177a33e909c20acbe030

ICANN. (2022, July 13). *Governance Guidelines*. ICANN. https://www.icann.org/resources/pages/governance/guidelines-en

India Stack. (n.d.). *Digital global goods – India Global Stack*. Retrieved 9 April 2024, from https://www.indiastack.global/digital-global-goods/

Jujjavarapu, G. (2017). India: New laws needed to protect citizens from invasive profiling. *Internet Policy Review*. https://policyreview.info/articles/news/india-new-laws-needed-protect-citizens-invasive-profiling/448

Khan, L. (2017). Amazon's antitrust paradox. *The Yale Law Journal*, *126*(3), 710–805.

Knight, P., Feferman, F., & Foditsch, N. (2016). *Broadband in Brazil: Past, present, and future*. Figurati. https://www.researchgate.net/publication/311206470_Broadband_in_Brazil_past_present_and_future

Lehuedé, S. (2024). An alternative planetary future? Digital sovereignty frameworks and the decolonial option. *Big Data & Society*, *11*(1). https://doi.org/10.1177/20539517231221778

Margetts, H., John, P., Hale, S., & Yasseri, T. (2015). *Political turbulence: How social media shape collective action*. Princeton University Press.

Marsden, C. T., & Brown, I. (2023). App stores, antitrust and their links to net neutrality: A review of the European policy and academic debate leading to the EU Digital Markets Act. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1676

Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, globalization and cyberspace*. John Wiley & Sons.

Mueller, M., & Kuerbis, B. (2014). Towards global internet governance: How to end U.S. control of ICANN without sacrificing stability, freedom or accountability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2408226

Mullin, J., & Cohn, C. (2024, October 9). *Salt Typhoon hack shows there's no security backdoor that's only for the "good guys"*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*, *2*(4). https://doi.org/10.14763/2013.4.208

Musiani, F. (2022). *Infrastructuring* digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, *25*(6), 785–800. https://doi.org/10.1080/1369118X.2022.2049850

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in internet governance*. Palgrave Macmillan US. https://doi.org/10.1057/9781137483591

NATM. (n.d.). *Welcome to NATM*. Non Aligned Technologies Movement. https://nonalignedtech.net/

NSA. (2012). *SSO CorpTeamBrief20Mar2012 S2D – DocumentCloud*. ProPublica. https://www.documentcloud.org/documents/2274321-sso-corpteambrief20mar2012-s2d.html

Nye, J. S. (2014). *The regime complex for managing global cyber activities* (No. 1; Paper Series). Global Commission on Internet Governance. https://www.cigionline.org/static/documents/gcig_paper_no1.pdf

Open Technology Fund. (n.d.). *oLink* [Archived webpage]. Open Technology Fund. Retrieved 18 April 2022, from https://web.archive.org/web/20220418061910/https://www.opentech.fund/results/supported-projects/olink/

Ortiz Freuler, J. (2023a). The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China*, *8*(1), 6–23. https://doi.org/10.1177/20594364221139729

Ortiz Freuler, J. (2023b). Unveiling gatekeeping practices in mobile environments: A comparative analysis of operating systems and app gardens. *International Journal of Communication*, *17*, 26.

Ortiz Freuler, J. (2025, February 4). Re-networking digital infrastructure: A Non-Aligned Tech

Movement to take us beyond the age of informational capitalism [Blog post. *Society for Social Studies of Science*. https://4sonline.org/news_manager.php?page=39356

Pandai, J., & Samdub, M. (2024). 4. Promises and pitfalls of India's AI industrial policy. In AI Now Institute (Ed.), *AI nationalism(s): Global industrial policy approaches to AI*. https://ainowinstitute.org/publication/analyzing-indias-ai-industrial-policy

PBS (Director). (2015, August 16). *Inside AT&T and the NSA's 'highly collaborative' partnership* [Video recording]. https://www.pbs.org/newshour/show/inside-att-nsas-highly-collaborative-partnership

Pierce, D., & Porter, J. (2024, January 25). *Apple is bringing sideloading and alternate app stores to the iPhone*. The Verge. https://www.theverge.com/2024/1/25/24050200/apple-third-party-app-stores-allowed-iphone-ios-europe-digital-markets-act

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, *16*(4), 672–691. https://doi.org/10.1002/poi3.426

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Rao, P. (2023, December 18). *Visualizing how big tech companies make their billions*. Visual Capitalist. https://www.visualcapitalist.com/big-tech-companies-billions/

Rev. (2020). *Tech CEOs face Congress at epic antitrust hearing*. https://www.rev.com/transcript-editor/shared/_FX24Jlb75YkV0wn0tdgEzn7hr3YnKHiYFRaJHC36cpuN8-hRZCoC_eanIZkNRqAAoCUFtC5429mmv3rvjnTX3PpTLo?loadFrom=PastedDeeplink&ts=4121.04

Robertson, A. (2021, September 12). *A comprehensive breakdown of the Epic v. Apple ruling*. The Verge. https://www.theverge.com/2021/9/12/22667694/epic-v-apple-trial-fortnite-judge-yvonne-gonzalez-rogers-final-ruling-injunction-breakdown

Rutherford, M. (2019). The CLOUD Act: Creating executive branch monopoly over cross-border data access. *Berkeley Technology Law Journal*, *34*(4), 1177–1204.

Shalal, A., & Roulette, J. (2025, February 22). *Exclusive: US could cut Ukraine's access to Starlink internet services over minerals, say sources*. Reuters. https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/

Smith, B. (2021, May 6). Answering Europe's call: Storing and processing EU data in the EU. *EU Policy Blog*. https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

Snowden, E. (2019). *Permanent Record*. Pan Macmillan.

Sriram, A., Nellis, S., & Sriram, A. (2024, March 6). *Apple escalates Epic Games feud by blocking Fortnite app in EU*. Reuters. https://www.reuters.com/technology/apple-terminates-developer-account-fortnite-maker-epic-games-says-2024-03-06/

StatCounter. (2024). *Mobile operating system market share Europe*. Statcounter Global Stats. https://gs.statcounter.com/os-market-share/mobile/europe/

StatCounter. (2025). *Search engine market share worldwide*. Statcounter Global Stats. https://gs.statc

ounter.com/search-engine-market-share

Statista. (2024, May 2). *Infographic: Amazon maintains cloud lead as Microsoft edges closer*. Statista Daily Data. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

Statista. (2025a). *India: E-commerce market size*. Statista. https://www.statista.com/statistics/792047/india-e-commerce-market-size/

Statista. (2025b, May 5). *Topic: Internet usage in India*. Statista. https://www.statista.com/topics/2157/internet-usage-in-india/

Stuenkel, O. (2020). *The BRICS and the future of global order*. Rowman & Littlefield.

Submarine Networks. (n.d.). *EllaLink*. Submarine Cable Networks. https://www.submarinenetworks.com/en/systems/trans-atlantic/ellalink

TeleGeography. (2013). *Submarine cable map 2013*. TeleGeography. https://submarine-cable-map-2013.telegeography.com/

Thornhill, J. (2023, May 11). *The likely winners of the generative AI gold rush*. Financial Times. https://www.ft.com/content/0cbe91ec-0971-4ba6-bdf1-87855aedd34c

US Department of Defense. (2003). *Information operations roadmap*. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

US Department of State. (2020, August). *The clean network*. US Department of State. https://2017-2021.state.gov/the-clean-network/

US Department of State. (2022, April 28). *Declaration for the future of the internet*. US Department of State. https://www.state.gov/declaration-for-the-future-of-the-internet/

Veen, J., & Boeke, S. (2020). No backdoors: Investigating the Dutch standpoint on encryption. *Policy & Internet*, *12*(4), 503–524. https://doi.org/10.1002/poi3.233

Voelsen, D. (2021). *Internet from space: How new satellite connections could affect global internet governance* (No. 3; SWR Research Paper). https://www.swp-berlin.org/10.18449/2021RP03/

Washington Post. (2013, June 6). NSA slides explain the PRISM data-collection program. *The Washington Post*. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

WEF. (2023, June 26). *India's Unified Payment Interface's impact on the financial landscape*. World Economic Forum. https://www.weforum.org/agenda/2023/06/india-unified-payment-interface-impact/

Williams, B. (2012). *The Economics of cloud computing*. Cisco Press.

Winseck, D. (2019). Internet infrastructure and the persistent myth of U.S. hegemony. In B. Haggart, K. Henne, & N. Tusikov (Eds.), *Information, technology and control in a changing world: Understanding power structures in the 21st century* (pp. 93–120). Springer International Publishing. https://link.springer.com/10.1007/978-3-030-14540-8

World Bank. (2024). *Overview [Text/HTML]*. World Bank Group. https://www.worldbank.org/en/country/brazil/overview

Zittrain, J. (1999). ICANN: Between the public and the private comments before Congress. *Berkeley*

Technology Law Journal, *14*(3), 1071–1094.

Zittrain, J. (2003). Internet points of control. *Boston College Law Review*, *44*(2). https://bclawreview.bc.edu/articles/1153

Zittrain, J. (2019). Three eras of digital governance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3458435

Published by

in cooperation with