UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

The Internet Infrastructure Has Never Been Open

ten Oever, Niels

DOI
10.11647/OBP.0528.03

Publication date
2026

Document Version
Final published version

Published in
The Politics of Open Infrastructures

License
CC BY

Link to publication

Citation for published version (APA):
ten Oever, N. (2026). The Internet Infrastructure Has Never Been Open. In K. Mayer, A. Mager, & R. Ridgway (Eds.), *The Politics of Open Infrastructures: Power, governance, and justice in digital knowledge practices* (pp. 65-78). (Digital Humanities Series; Vol. 5). Open Book Publishers. https://doi.org/10.11647/OBP.0528.03

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

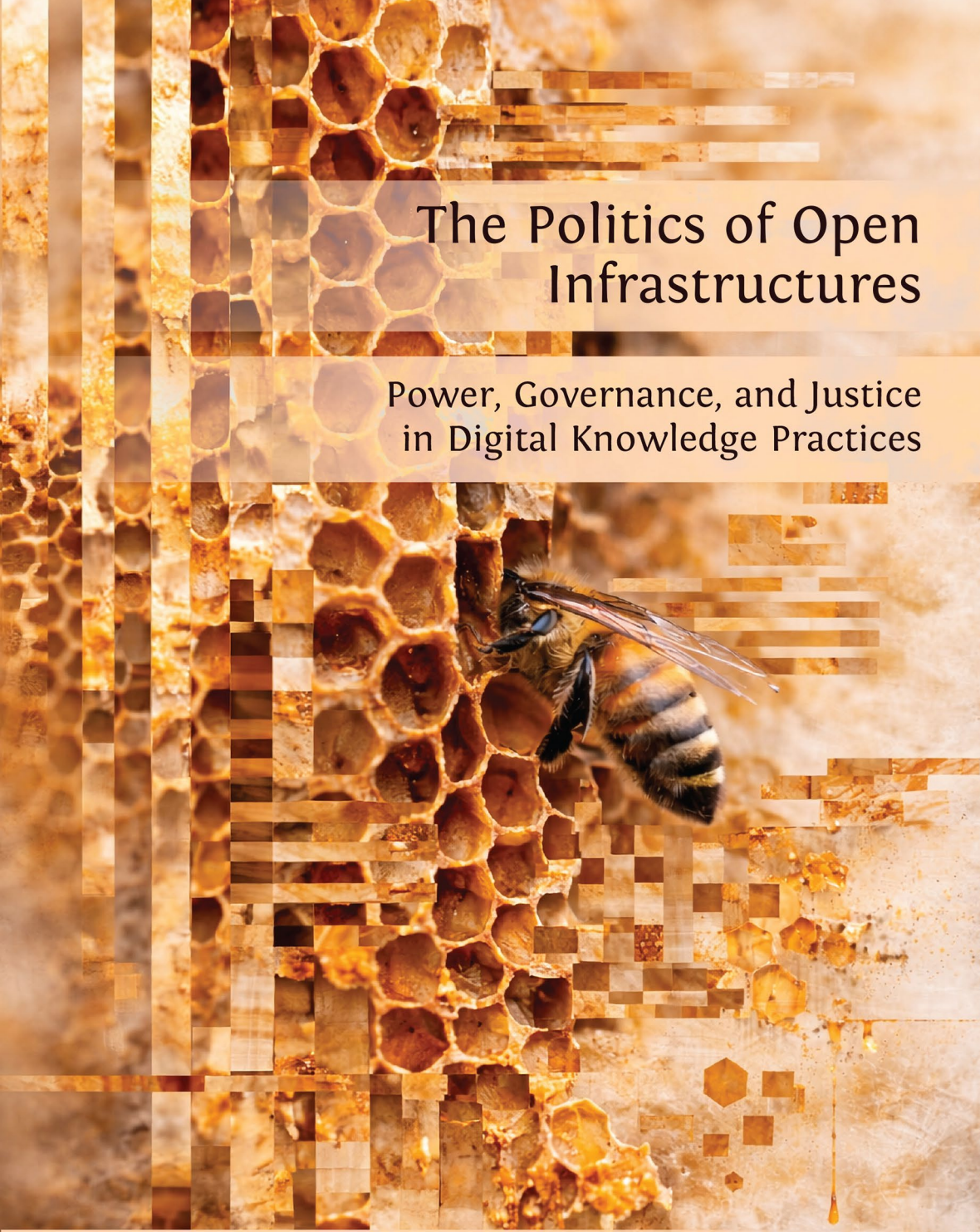
Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:08 Nov 2026

The Politics of Open Infrastructures

Power, Governance, and Justice in Digital Knowledge Practices



Edited by Katja Mayer, Astrid Mager and Renée Ridgway

https://www.openbookpublishers.com

©2026 Katja Mayer, Astrid Mager, and Renée Ridgway
Copyright of individual chapters is maintained by the chapters' authors

This work as a whole is licensed under a Creative Commons Attribution-NonCommercial license (CC BY-NC 4.0), which allows you to share, copy, distribute and transmit the text; to adapt the text for non-commercial purposes of the text providing attribution is made to the authors (but not in any way that suggests that they endorse you or your use of the work). Selected chapters are available under a CC BY 4.0 license (the type of license is indicated in the footer of the first page of each chapter). This license allows you to share, copy, distribute and transmit the text; to adapt the text and to make commercial use of the text providing attribution is made to the authors (but not in any way that suggests that they endorse you or your use of the work). Attribution should include the following information:

Katja Mayer, Astrid Mager, and Renée Ridgway (eds), *The Politics of Open Infrastructures: Power, Governance, and Justice in Digital Knowledge Practices*. Cambridge: Open Book Publishers, 2026, https://doi.org/10.11647/OBP.0528

Further details about CC BY-NC licenses are available at
https://creativecommons.org/licenses/by-nc/4.0/

All external links were active at the time of publication unless otherwise stated and have been archived via the Internet Archive Wayback Machine at https://archive.org/web

Updated digital material and resources associated with this volume are available at
https://www.openbookpublishers.com/books/10.11647/obp.0528#resources

Copyright and permissions for the reuse of many of the images included in this publication differ from the above. This information is provided in the captions and in the list of illustrations. Where no licensing information is provided in the caption, the figure is reproduced under the fair dealing principle. Every effort has been made to identify and contact copyright holders and any omission or error will be corrected if notification is made to the publisher.

Digital Humanities Series vol. 5 ISSN Print: 2054-2410 | ISSN Digital: 2054-2429

ISBN Paperback: 978-1-80511-887-9
ISBN Hardback: 978-1-80511-888-6
ISBN PDF: 978-1-80511-889-3
ISBN HTML: 978-1-80511-891-6
ISBN EPUB: 978-1-80511-890-9

DOI: 10.11647/OBP.0528

Cover images created with Stable Diffusion 3.5. Inspired by the distorted images by Lone Thomasky and Bits & Bäume via Better Images of AI. https://betterimagesofai.org, CC BY 4.0.
Cover design: Jeevanjot Kaur Nagpal

3. The Internet Infrastructure Has Never Been Open

Niels ten Oever[1]

In this chapter, I argue that openness offers a limited view, and surely not access, into closed systems. The following analysis demonstrates how openness is always a matter of openness for a particular group, namely, the group that can set and alter the configuration of the material infrastructure. Openness, then, is not a neutral design principle but an expression of infrastructural power, of who gets to define, design, and delimit participation. This group's interests may coincide with those of other groups, but when these interests are at odds, the interests of one group prevail over the other. I will analyse how the internet has been open to different groups, namely the military, business, intelligence services, the state, academia, and users. I conclude by demonstrating how the internet has been particularly open to configuration by the US military and industry, and how the essence of openness is located in its limitations.

Openness is liberalism's favourite paradigm. It emerged in response to the perceived 'closedness' of the so-called Second World during the Cold War (Edwards 1996). In the development of the precursor to the internet, which was initiated by the agency established in response to the Soviet Union's launch of Sputnik, openness took a central place. It stuck and became a guiding principle in the development of digital networks (Russell 2014). Openness meant many things simultaneously

1 This research is supported by the Ford Foundation (grant 144895), the Internet Society Foundation, the Open Technology Fund, and Omidyar's AI Collaborative.

©2026 Niels ten Oever, CC BY 4.0 https://doi.org/10.11647/OBP.0528.03

in the development of the internet: open protocols, open archives, open participation, and the ability to expand the internet network (ten Oever 2021). With the success of the internet, the concept of openness gained momentum. It first spread to directly related fields such as open-source software, and from there, it continued to expand. It began with concepts still closely tied to computing, such as OpenStreetMap and Wikipedia, and later expanded to broader initiatives, including open government and open-access publishing.

Science and technology studies (STS) over the past few decades have done excellent work in showing that every field, practice, and technology harbours power structures, hierarchies, and excludes people, beings, and practices. What I would like to contribute to the academic debate in STS and infrastructure studies is a reflection on how general-purpose infrastructures do not exist. I argue that openness can exist in infrastructure, but that it will always be openness for a particular group. Uses that go against that will be deprioritised, antagonised, and eventually written out.

While the concept of inscription is by no means new, Akrich (1992: 208) described it as 'the work of innovators [which] is that of "inscribing" this vision of (or prediction about) the world in the technical content of the new object', and the idea that such inscriptions may serve the interests of particular groups over others has already been articulated by Callon (1990: 143). This perspective is crucial for understanding openness not as universal access, but as the outcome of selective inscription by powerful actors. It underlines that infrastructures are relational. They are not solely shaped by material technologies, but also by the epistemic communities, institutions, standards, practices, and protocols that co-constitute them (Star and Ruhleder 1994). Nevertheless, because of their scale, complexity, technical opacity, and deep entrenchment in everyday life, infrastructures often remain beyond the reach of public scrutiny (Peters 2015).

Aside from the lack of scrutiny, infrastructures commonly undergo discursive examination through the analysis of myths (Mosco 2005; Bory 2020), narratives (Breuer and Johnston 2019; Hofmann 2020; Lambach and Oppermann 2022), and socio-technical imaginaries (Jasanoff and Kim 2015). There is, however, a risk of overly relying on discursive representations and analyses without coupling them with a careful

analysis of the material ordering–potentially perpetuating a discursive image that legitimises a particular ordering without describing its technical workings and material control (ten Oever 2023).

Open for the Military

When Sputnik was launched, it was not the satellite over which the world marvelled that scared the United States; it was the intercontinental ballistic missile that carried it. Sputnik was perceived as a dummy payload to distract from the material threat, much like platforms, APIs, and interfaces distract from the sedimented infrastructural power that underpins them. The infrastructural anxiety induced by the *tour de force* of the Soviet Union, which demonstrated its military and scientific supremacy, prompted the United States to respond institutionally by establishing the Advanced Research Projects Agency (ARPA).[2] This agency's first two projects and priorities still echo today: the establishment of NASA and the ARPANET, a network that could withstand a nuclear strike.

Computers had already been deeply written into the war effort: the ENIAC computer had been doing calculations for missile trajectories (much like Galileo Galilei's gunner compass had done nearly four centuries before), and the Bombe machine was used to decipher German communications. However, all these calculations would be worthless if they were not communicated. It was already clear that a vast computer network could function not merely to send calculations, but also to work like a nervous system, connecting radars, command centres, and both conventional and nuclear weapons in a system to defend the United States against Soviet threats (Edwards 1996). In these labs, machines and scenarios were devised for possible 'dead hand' scenarios where the US would retaliate against a Soviet nuclear strike, even in the case of impact, to ensure mutually assured destruction. The internet had the promise to connect all efforts, increase its resilience, and allow for better coordination.

Towards the end of the Cold War, military funding gave way to increased research funding, and after the fall of the Soviet Union, to commercialisation. Scholars like Madeline Carr argue that, at that

2 Currently known as the Defense Advanced Research Projects Agency (DARPA).

moment, US military power made way for US commercial power (Carr 2015). However, what often remains under-explored is the enormous power the US military still holds over the internet, both directly and indirectly.

In earlier communication networks, such as telecommunications, connections were always tied to a particular geography due to the underlying technology, namely circuit switching. The internet functioned as an overlay network and could therefore function over all kinds of networks. The concept of the 'borderless internet' suddenly provided the US military with access to many places around the world through a territory it had itself co-designed. When NATO officially declared cyberspace as a domain of warfare in 2016, the United States military was back in a place it had never left. A few years later, NATO would also assign space as a domain of military warfare. The two ARPA projects had been delivered.

In nearly all definitions of the internet, the internet protocol (IP) is the connecting denominator. For over twenty-five years, we have known that IPv4 addresses are running out, and the Regional Internet Registries are no longer allocating them. At the same time, the US military controls 13 /8 blocks of IPv4 addresses, in other words, 221,828,864 IPv4 addresses, which is roughly six percent of the total number of public internet addresses, most of which are never used but are kept as a strategic stockpile.

To summarise, the US military has been one of the founders of the internet, has influenced its design goals, shaped the internet, sees the internet as a military domain, and still holds a significant amount of the internet's primary resources. The military's infrastructural authorship exemplifies how openness operates: it is open to those who design and command the system, while these options are closed to those who merely use it. In this sense, the internet's earliest openness was an openness for military coordination, not public participation.

Open for Industry

The reconfiguration of communication infrastructures by the internet has led to a significant reshuffling of power from telecommunications providers to content providers. The erstwhile end-to-end philosophy

of internet engineering transformed the network from a data control network into a data transport network: '[t]he network's job is to transmit datagrams as efficiently and flexibly as possible. Everything else should be done at the fringes' (Internet Architecture Board 1996: 2–3). The new emphasis on end-to-end connectivity took power and control over data streams from the network, and promised to give it to the end-devices, thus communication infrastructure transformed from smart networks with dumb phones, to a dumb network with intelligent computers, taking away power from network operators and handing it over to endpoints.

In the tussle over control of data streams between network operators and content providers, power was never handed to end users, only to the servers of the content providers. The end-to-end connectivity turned out not to be symmetrical between all ends because not all endpoints were created equal. While people's end-devices had sufficient capacity to run their mail servers and websites, network directionality was introduced, and third-party services for email, social media, and website hosting were offered, whereas these could architecturally just as well have been hosted on end-user devices. The concept of the user was produced through the infrastructure. That the internet infrastructure was open for business meant that the end-user became a customer and a data producer, and subject to endless varieties of data extraction.

Initially, the infrastructure was monetised through simple ads, but this swiftly developed into a sprawling and intricate ecosystem of advertisement technology, including cookies, tracking, and real-time bidding on individual user profiles. The leader in this industry was and continues to be Google, through its AdSense platform (now Google Ads). It firmly galvanised this position by maintaining the world's largest browser (Chrome), and a large content offering through search, email provision (Gmail), and content provision (YouTube).

To offer content as fast as possible, whilst allowing advertisers to engage in real-time bidding and serving personalised ads with as little friction as possible, Google developed and implemented its own encrypted transport protocol called QUIC (Quick UDP Internet Connections) in 2012. Many had tried this before, but only Google was able to do so because of its ability to do experimental testing on the internet between the world's largest browser and its extensive server network (Perarnaud and Musiani 2025). This standard was brought to the Internet Engineering Task Force

(IETF) in 2015 because if this protocol were standardised and accepted as the primary new transport protocol of the internet, no one in their right mind would block it, which might not be the case if it were 'only' Google's protocol. In 2016, a working group was established in the IETF, and in 2021, the formal QUIC standard was published as RFC9000 (Iyengar and Thomson 2021).

This reconfiguration of the internet infrastructure occurred quite rapidly and with minimal discussion. It was clear that Google had successfully brought together the interests of many different content providers in the development of this new protocol. What is presented as infrastructural openness through open protocols, interoperable standards, and open processes was, in practice, an opening for industry to consolidate control. The internet thus remained open, but only to those with the capacity to inscribe their economic and infrastructural power into its standards. The combined interests were illustrated when a review was done on the potential human rights impact of QUIC,[3] which was presented at the meeting of the Human Rights Protocol Considerations Research Group (HRPC) in 2018 in Bangkok.[4]

Open for Civil Society

A couple of civil society actors from the organisations ARTICLE 19, Coding Rights, and the Association of Progressive Communications (APC) started addressing human rights considerations in internet protocols in November 2014 by giving a presentation to the Internet Engineering Task Force (IETF). This resulted in the establishment of a dedicated research group in the Internet Research Taskforce in 2015 (Cath 2021) and the publication of a dedicated methodology to engage in the review of internet protocols and their human rights impact (ten Oever and Cath 2017).

The human rights review of the QUIC protocol was based on seven 60–90 minute elite interviews with QUIC working group leadership, main document authors, and active participants in the development of QUIC, conducted using a method specifically devised for this purpose

3 See https://datatracker.ietf.org/doc/html/draft-martini-hrpc-quichr-00
4 See https://youtu.be/Bd33Be_P-FY?si=4N-NokjnNYLNa1Jc&t=5286

(ten Oever and Cath 2017). The results of the QUIC analysis were relatively mild, with some concerns regarding risks to consolidation in the internet architecture, privacy, internet transparency, and internationalisation. However, the critique of the human rights impact assessment of the protocol received was fierce; the first commenter, a member of IETF leadership, contended that the review 'did not add anything to the discussion.' Several members of the Internet Architecture Board (IAB) and even the IETF chair came out to denounce the work. The latter even added that 'just participating in working groups would be far more efficient than writing these broad-based external reviews and just coming in from the outside.'[5] The critiques offered in the session diverged (ranging from claims that the review was conducted too early to analyze the impact of the QUIC protocol, to assertions that it cametoo late in the development process to contribute to the development meaningfully; that all issues mentioned in the review had already been discussed; that the analysis was technically incorrect; and, conversely, that it was technically correct but still irrelevant). Yet despite these shifting objections, no concrete errors in the review were identified in person or posted to the mailing lists of the QUIC working group or the HRPC research group. The review, however, did have a different impact, namely, an extensive discussion in the IAB about whether the HRPC Research Group should be closed and disbanded. This was averted by the external appointment of two technical advisors to the research group in March 2019, something that had never happened in the IRTF or IETF before.

As of 2026, HRPC has organised sessions at the IRTF for ten years,[6] but participation and mailing list activity have decreased significantly. The only moment a concrete, meaningful influence on protocol development was achieved was when Verisign, the largest internet registry, most known for its management of the .com and .net domains, made a proposal.[7] This proposal would facilitate the alignment of the Extensible Provisioning Protocol (EPP) with a Chinese draft law[8] by offering the

5 See https://youtu.be/Bd33Be_P-FY?si=zy3nKBNHGviPCb2M&t=6228
6 See https://www.ietf.org/proceedings/95/hrpc.html
7 See https://datatracker.ietf.org/doc/html/draft-ietf-regext-verificationcode-06
8 See https://chinacopyrightandmedia.wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/

possibility of a Verification Service Provider (VSP) that would check the identity of someone who wanted to register a domain name. A review of the human rights impact of this proposal was made[9] and concluded that 'the proposed extension in its implementation allows the VSP to have enormous censorship and discriminatory power. The arbitrary and opaque mechanism to "verify" compliance with local regulations gives disproportionate powers to impede freedom of expression, right to privacy, freedom of association, and the right to non-discrimination.'[10] After a lengthy discussion, the working group began to agree on adding privacy and human rights considerations to the document, but suddenly, Verisign decided to abandon further development of the document.

The pattern that emerges from the example of QUIC and EPP shows that civil society engagement is tolerated when it brings up issues that do not necessarily align with US interests (in the case of EPP, which helped align the internet infrastructure with the Chinese legal system), but when it does so against the interest of the US (as happened in the case of QUIC), it is made clear that it has no place to inscribe its values.

In their respective works, from very different angles, Madeline Carr (Carr 2013), Jeanette Hofmann (Hofmann 2020), and Corinne Cath (Cath 2021) show how the voices and interests of civil society actors are welcomed in internet infrastructure governance, as long as their stances align with those of other stakeholders and legitimise the institutional ordering, otherwise, their standpoints are disregarded. Civil society actors could participate, but not configure; they could speak, but not inscribe. Their openness was conditional and revocable, illustrating that participation without infrastructural power reproduces the very exclusions that openness claims to overcome.

Open for Intelligence

In 2013, the Snowden revelations showed the world how the United States (US) and the Five Eyes collective, comprising Australia, Canada, New Zealand, the United Kingdom, and the US, collaborate to use the internet for signals intelligence. In order to do this, they leverage both

9 See https://gitlab.com/hr-rt/documents/-/blob/master/HR-RT%20Review%20of%20draft-ietf-regext-verificationcode?ref_type=heads

10 Ibid.

the infrastructure and its chokepoints (Tusikov 2016), as well as access to large infrastructure and service providers. Through the so-called Prism programme, the US National Security Agency (NSA) would have direct access to the servers of Google, Microsoft, Facebook, and Apple, and by weakening cryptographic standards, it would be able to decode data streams directly (Rogers and Eden 2017).

The collaboration between state and corporate surveillance facilitated the production of an infrastructure of extraction (Zuboff 2020; Cohen 2019; Jung 2025). The joint redesign that optimised the internet infrastructure for extraction might be compared to the redesign of Paris by the architect Haussmann (Soppelsa 2009). The broad boulevards provide the possibility, access, and overview for police and authorities, making it easier to read and control the city, and to suppress riots. But the design would also prove to work great for trucks and commerce. One thing was certain: barricades could not be easily erected, and anonymous congregations would be nearly impossible. Intelligence agencies' ability to repurpose the infrastructure for surveillance again demonstrates that openness serves those who command the chokepoints. The infrastructure's supposed neutrality concealed its deep alignment with state power. The logics of security and profit both demand selective openness: enough transparency to sustain innovation and connectivity, but sufficient closure to enable monitoring and monetisation. Extraction depends on predictable, measurable flows of data, which are only possible within infrastructures that are open enough to connect but closed enough to control. In this sense, the internet's transformation mirrors the reconfiguration of public space: what once promised a commons for exchange and assembly has become a tightly managed environment where participation is continuously monitored and monetised.

Open for the State

In the current geopolitical moment where the US is retreating from international norms, we witness something that can be compared to an infrastructural breakdown (Star 1999), but not in the sense that the internet infrastructure is not working. Rather, it is not working as many governments expected. Many governments around the world are experiencing the

infrastructural anxiety that the US experienced with the launch of Sputnik. In response, states are trying to erect barriers, but are noticing it is not easy to do so on a network that 'does not recognise borders.' Countries and regions are dusting off old strategies of industrial policy, but are having a hard time fitting them within the neoliberal ideologies of our times, where the government is generally understood as inefficient in comparison to the market as a structuring and organising mechanism. Notions of strategic autonomy and digital sovereignty collide with the inertia of infrastructures built on the concrete foundations of the Cold War.

Within the European Union, the concept of the 'EuroStack' is having its political moment.[11] However, as of writing, nowhere has it been significantly explicated what would differentiate a European Stack from a non-European Stack (because they should be interoperable through open standards), except that small and medium-sized enterprises would produce it. What adds insult to injury is that there seems to be no plan to prevent these European companies from being acquired by US capital, or for US Big Tech or its subsidiaries to participate, because otherwise the EU would violate its own rules for free market competition. This is precisely what was witnessed in the previous European digital sovereignty initiative, Gaia-X (Baur 2024).

EuroStack aims to enhance European competitiveness by developing European supercomputers and AI factories, thereby propelling its industry into a competitive race with the US and China. It is difficult to grasp this logic: how can one be expected to win a race that others began long ago, with larger budgets and far greater industrial and societal absorption capacity? Europe is struggling with the paradox of wanting to be both open and autonomous at the same time. It is therefore not surprising that European defence contractors, such as Thales and Airbus, see a role for themselves in defending European interests.

At this point, it becomes clear that alternative technological trajectories highly depend on military spending—a point also highlighted by Mazzucato (2018), who proposes developing more civil missions. Together with Eaves and Vasconcellos, Mazzucato contributes

11 An in typical European fashion, the initiative already seems to be split into two camps and three documents: https://www.euro-stack.info/docs/EuroStack_2025.pdf, https://euro-stack.eu/a-pitch-paper/, and https://euro-stack.eu/the-white-paper/

to a notion of digital public infrastructure (Eaves et al. 2024), which can be characterised at its best as uncritical. In their report, the authors equate openness with publicness, which, as we have shown before, does not at all account for power differentials in infrastructures. The critique against the digital public infrastructure project is not merely theoretical. As the critical work by Nai Lee Kalema shows, the coercive politics of digital public infrastructures have taken form (2024).

The state's renewed infrastructural anxiety exposes the contradiction at the heart of openness: to be open to all is to be vulnerable to those with greater power. The European search for 'sovereign openness' thus reveals that openness itself is a terrain of geopolitical struggle.

Freedom in Limitation: Demilitarised Infrastructures and Public Services

The international use of the word 'infrastructure' started with the communique of the NATO meeting in May 1952, which read: '[a]greement was reached on the financing of a further portion of the infrastructure program, for airfields, communications and headquarters.'[12] The history of the internet and telecommunications is deeply characterised by its use by police, military, and intelligence agencies. In physical space, it is very clearly observable where the space is public, private, or military; the internet, however, is always private and military.

Creating a communication network that functions as an open infrastructure would mean limiting its scale and use to protect users from coercion, control, extraction, and capture. It would mean undoing the excommunication of the user from the design and control over the network, and reintroducing them as citizens who would be able to observe, contest, and configure the network in meaningful ways (Galloway et al. 2013; ten Oever 2023).

If the study of power in infrastructures teaches us one thing, it is that infrastructures cannot simultaneously be open and equally accessible to all groups at the same time. If there is a future for open and sustainable civilian infrastructures, the core property should not be abundance, but limitation and distribution (ten Oever 2025).

12 See https://www.nato.int/docu/comm/49-95/c520225a.htm

Understanding openness as always situated and partial allows us to imagine infrastructures differently; not as systems open to everyone in the abstract, but as deliberately limited commons that protect against domination. Genuine openness, paradoxically, may lie in collective limitation: infrastructures that refuse universality to sustain equality.

References

Akrich, Madeleine. 1992. 'The De-Scription of Technical Objects.' In *Shaping Technology/Building Society. Studies in Sociotechnical Change*, edited by Wiebe E. Bijker and John Law, 205–224. Cambridge, MA: MIT Press.

Baur, Andreas. 2024. 'European Dreams of the Cloud: Imagining Innovation and Political Control.' *Geopolitics* 29 (3): 796–820. https://doi.org/10.1080/14650045.2022.2151902.

Bory, Paolo. 2020. *The Internet Myth: From the Internet Imaginary to Network Ideologies*. London: University of Westminster Press.

Breuer, Adam, and Alastair Iain Johnston. 2019. 'Memes, Narratives and the Emergent US–China Security Dilemma.' *Cambridge Review of International Affairs* 32 (4): 429–455. https://doi.org/10.1080/09557571.2019.1622083.

Callon, Michel. 1990. '"Techno-Economic Networks and Irreversibility."' *The Sociological Review* 38 (S1): 132–161.

Carr, Madeline. 2013. 'Internet Freedom, Human Rights and Power.' *Australian Journal of International Affairs* 67 (5): 621–637. https://doi.org/10.1080/10357718.2013.817525.

Carr, Madeline. 2015. '"Power Plays in Global Internet Governance."' *Millennium* 43 (2): 640–659. https://doi.org/10.1177/0305829814562655.

Cath, C. 2021. 'Changing Minds and Machines: A Case Study of Human Rights Advocacy in the Internet Engineering Task Force (IETF).' PhD Thesis, University of Oxford.

Cath, Corinne. 2021. '"The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force."' *Telecommunications Policy, Norm Entrepreneurship in Internet Governance* 45 (6): 102–144. https://doi.org/10.1016/j.telpol.2021.102144.

Cohen, Julie E. 2019. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press.

Eaves, David, Mariana Mazzucato, and Beatriz Vasconcellos. 2024. 'Digital Public Infrastructure and Public Value: What Is "Public" about DPI?' Working Paper Series (IIPP WP) 2024-05). https://discovery.ucl.ac.uk/id/eprint/10196645/

Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of Discourse in Cold War America.* Massachusetts, MA: MIT Press.

Galloway, Alexander R., Eugene Thacker, and McKenzie Wark. 2013. *Excommunication: Three Inquiries in Media and Mediation*. Chicago, IL: University of Chicago Press.

Hofmann, Jeanette. 2020. 'The Multistakeholder Concept as Narrative: A Discourse Analytical Approach.' In *Researching Internet Governance: Methods, Frameworks, Futures*, edited by Laura DeNardis, Derrick L. Cogburn, Nanette S. Levinson, and Francesca Musiani, 253–268 . Massachusetts, MA: MIT Press.

Internet Architecture Board. 1996. *RFC1958—Architectural Principles of the Internet. RFC-Series, edited by Brian E. Carpenter*. RFC Editor. https://tools.ietf.org/html/rfc1958

Iyengar, Jana, and Martin Thomson. 2021. *QUIC: A UDP-Based Multiplexed and Secure Transport. Request for Comments RFC 9000.* Internet Engineering Task Force. https://doi.org/10.17487/RFC9000

Jasanoff, Sheila, and Sang-Hyun Kim. 2015. *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. Chicago, IL: University of Chicago Press.

Jung, Maximilian. 2025. 'Digital Capitalism Is a Mine Not a Cloud.' *Transnational Institute* (10 July). https://www.tni.org/en/article/digital-capitalism-is-a-mine-not-a-cloud

Kalema, Naigwee. 2024. 'The "Digital Transformation for Development" (DX4D) Anti-Politics Machine.' *Policy & Internet* 16 (4): 1–20.

Lambach, Daniel, and Kai Oppermann. 2022. 'Narratives of Digital Sovereignty in German Political Discourse.' *Governance* 36 (3): 693–709. https://doi.org/10.1111/gove.12690

Mazzucato, Mariana. 2018. 'Mission-Oriented Innovation Policies: Challenges and Opportunities.' *Industrial and Corporate Change* 27 (5): 803–815. https://doi.org/10.1093/icc/dty034.

Mosco, Vincent. 2005. *The Digital Sublime: Myth, Power, and Cyberspace*. Massachusetts, MA: The MIT Press.

Perarnaud, Clement, and Francesca Musiani. 2025. 'QUIC, or the Battle That Never Was: A Case of Infrastructuring Control over Internet Traffic.' *New Media & Society*, https://doi.org/10.1177/14614448251336438

Rogers, Michael, and Grace Eden. 2017. 'The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures.' *International Journal of Communication* 11 (22): 802–823.

Russell, Andrew L. 2014. *Open Standards and the Digital Age.* Cambridge: Cambridge University Press.

Soppelsa, Peter. 2009. 'Finding Fragility in Paris: The Politics of Infrastructure after Haussmann.' *Proceedings of the Western Society for French History* 37. http://hdl.handle.net/2027/spo.0642292.0037.016

Star, Susan Leigh. 1999. 'The Ethnography of Infrastructure.' *American Behavioral Scientist*, 3: 377–391.

Star, Susan Leigh, and Karen Ruhleder. 1994. 'Steps towards an Ecology of Infrastructure: Complex Problems in Design and Access for Large-Scale Collaborative Systems.' *CSCW '94*, 253–264. New York: Association for Computing Machinery. https://doi.org/10.1145/192844.193021

ten Oever, Niels. 2021. '"This Is Not How We Imagined It'—Technological Affordances, Economic Drivers and the Internet Architecture Imaginary.' *New Media & Society* 23 (2): 271–288. https://doi.org/10.1177/20594364231193950

ten Oever, Niels. 2023. '5G and the Notion of Network Ideology, or: The Limitations of Sociotechnical Imaginaries.' *Telecommunications Policy* 47 (5): 102442. https://doi.org/10.1016/j.telpol.2022.102442

ten Oever, Niels. 2025. 'Infrastructural Futures: Transparency, Disconnectivity, and Transgressive Infrastructuring.' In *Critical Internet Governance: From Positions to a Field*, 73–78. Amsterdam: Critical Infrastructure Lab. https://www.criticalinfralab.net/wp-content/uploads/2025/06/CIL011.pdf#page=79

ten Oever, Niels, and Corinne Cath. 2017. *RFC8280—Research into Human Rights Protocol Considerations*. RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc8280.

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet.* Oakland, CA: University of California Press.

Zuboff, Shoshana. 2020. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First Trade paperback edition. New York: PublicAffairs.