SplinterCon

Sovereignty: autonomy
or isolation?

2025
PARIS

eQualitie

SplinterCon is an international and interdisciplinary conference that focuses specifically on internet fragmentation and its consequences on contemporary societies and online liberties. The inaugural event was launched by eQualitie in Montreal, December 2023. Since then, we've hosted SplinterCon to Brussels, Estoril, Berlin, Taipei and now, Paris, held in cooperation with The Center for Internet and Society (CIS-CNRS), the GEODE Center and the European Research Council. These gatherings assembled hundreds of creative minds from communities encompassing network researchers, technology entrepreneurs, network engineers and software developers, user experience designers, media and internet freedom advocates, in order to:

- Analyze the practices and impacts of network isolation and shutdowns;
- Evaluate existing and future technology solutions for communicating with and within sovereign networks;
- Invest in practical and user-oriented solutions for connectivity and content distribution across digital barriers.

SplinterCon is normally held under Chatham House rule, and we have sought explicit permission from presenters to share their materials for post-conference reporting. This collation presents highlights from three events and summarizes the 'state of the splinternet' as a point of reflection and in order to strategize from hereon.

splintercon.net equalit.ie

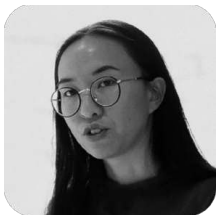
Acknowledgments

We are deeply grateful to the SplinterCon Advisory Council members and partner organizations, whose guidance and support have shaped this project from the very beginning.

Dmitri Vitaliev
Technology Director,
eQualitie

Ksenia Yermoshina
Researcher,
eQualitie, The Center for Internet and Society, CNRS

Francesca Musiani
Director,
The Center for Internet and Society, CNRS



Lai Yi Ohlsen
The Internet Index

Nicolas Diaz
Head of Digital Security,
Reporters Without Borders

Ricardo Nanni
Postdoc Researcher,
The Center for Internet and Society, CNRS

Louis Pétiniaud
Researcher, GEODE;
Associate Researcher,
Cassini Conseil

Marion Mareau
Founder, Journalist,
Hors Normes

Alena Epifanova
Research Fellow,
The German Council on Foreign Relations

Mallory Knodel
Founding Director,
Social Web Foundation

Alexey Sidorenko
Director,
Teplitsa.Technologies
for Social Good

Nick Sullivan
Cryptography and
System Security Advisor

Timothy Ball

Hammer
Founder and Director,
Project Ainita

Fereidoon Bashar
Executive Director,
ASL19

In partnership with

Contents

Introduction: a continuum of sovereignties

In 2025 the debates on the so-called digital sovereignty have not only intensified but have also taken a dramatically new shape: besides Russia, Iran or China for many years depicted as “enemies of the free Internet”, the role of the United States in maintaining digital authoritarianism has become obvious. In this new context we should speak about “digital sovereignties” as a spectrum. Besides a negative connotation with extreme control and isolation that has long been attributed to this term, the multidimensional concept of sovereignty starts to shine bright, as a promise of autonomy.

This topic became central for the latest edition of SplinterCon that took place in Paris in December 8-10, 2025.The interdisciplinary conference gathered an outstanding expert community coming from a variety of disciplines: network measurements pioneers, protocol developers, network engineers, policy researchers and on-the-ground activists. In this report we propose a synthesis of key highlights from SplinterCon in an attempt to build a classification of “sovereignties”, their causes and consequences for civil society and Internet freedom across the world. This report also covers latest technological developments presented at the conference, that are today being actively used on the frontlines as working solutions that help breach isolation and reconnect splintered territories.

During the most recent and most spectacular shutdowns in Iran in January 2026, many of the tools and approaches presented in this report were put into action. The experts from the SplinterCon community became a rapid response task force monitoring the events and helping Iranian citizens to maintain connectivity, communicate and report on the human rights violations that were hidden by the shadow of shutdowns.

In this edition we asked our keynote speakers to author specific sections of the report. So what you will read is a polylogue where different voices are heard, and different disciplines are at play.

Chapter 1

What is the Splinternet?

By Lai Yi Ohlsen,

A researcher based in New York City.
She is a Senior Product Manager of performance and network quality at Cloudflare and a part-time lecturer at the New School in the Parsons Design & Technology program. Previously she was Director and Research and Data Lead at Measurement Lab and Technical Program Manager at eQualit.ie.
She is currently a member of eQualitie's Board and Quad9's advisory PEHR council. You can read more of her work on Internet Index, an accumulation of research shaped around the Internet and its associated infrastructures.

What We Talk About When We Talk About Splintering

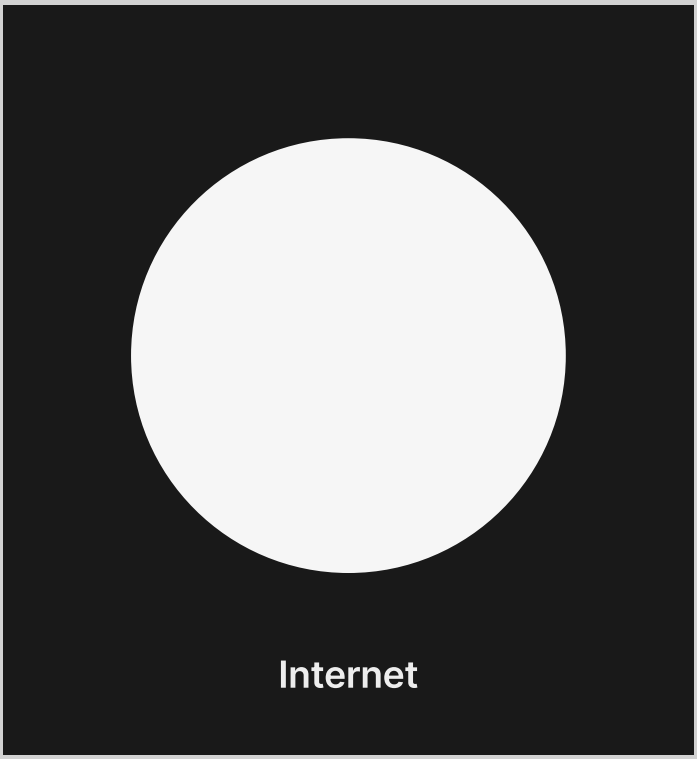
The term “Splinternet” suggests that there was a “whole” Internet to begin with - a singular entity capable of being fractured. An Internet to splinter. If we assume this to be true, that there is a state that does or has or could exist where the Internet is a single, unified entity, the next question becomes what was or is this unbroken version of the Internet? When did it exist or has it ever existed? And how would we describe it - what does it mean for the Internet to be whole?

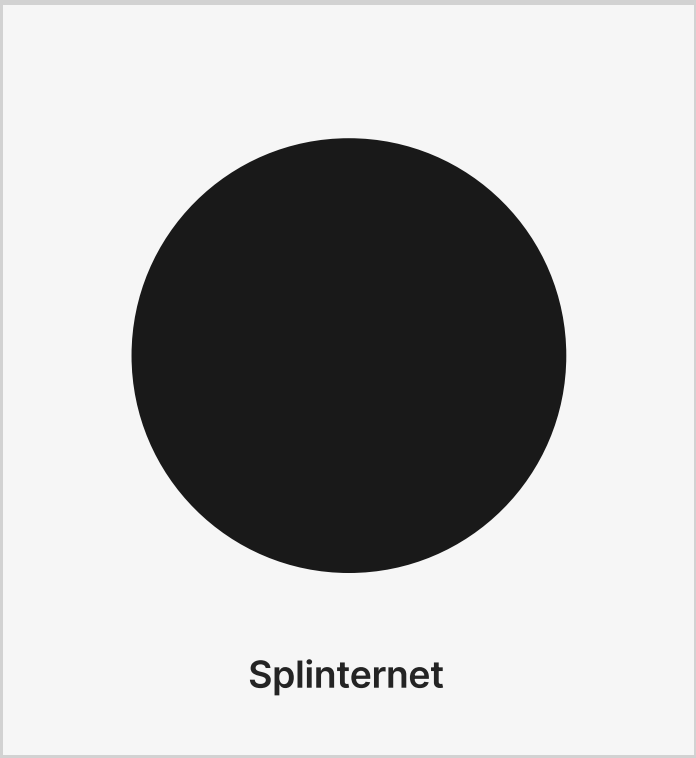
One of the earliest mentions in popular media of the term “splinternet” came from the libertarian advocate Clyde Wayne Crews who published for Forbes in 2001 about the positive potential for “parallel Internets.” In his telling, the Splinternet is the way out of what he and others call “the tragedy of the commons.” His recommendation: “Take the Internet private and split it up.” The article references the usual libertarian touch points such as private property and eliminating the monopoly, but in follow up comments to Wired, he also positions it in terms of the social. “Do people want to be connected to everyone? I don’t think so. [...] Fundamentally, people want to be connected to other people like them.” To Crews at the time the Splinternet was the anti-commons - the private park with a gate code, while the Internet is a dirty public square. Splinternet good, Internet bad. But to his likely disappointment, as the term has become popularized, it has become much more known for the inverse: Splinternet bad, Internet good.

The Internet Society defines a splinternet as “the idea that the open, globally connected Internet we all use splinters into a collection of fragmented networks controlled by governments or corporations” and routinely leads calls against Internet fragmentation. Such advocacy strongly signals that the Splinternet is something to be avoided at all costs, even going so far as to argue that a shattered Internet is not the Internet at all—that the Splinternet is its existential opposite.

But either way, the model appears to be, at least conversationally consistent - whether you’re Crews or the Internet Society - the way we talk about the Splinternet consistently positions it as the anti-Internet. To be splintered is to be antithetical to the original purpose/architecture/intent of the Internet. And this is what I find fascinating about the concept of the Splinternet, the way that it operates

as a conversational proxy for the definitional bounds of the Internet. Through the prism of fragmentation we produce inverted manifestos for what we think the Internet is, was, or ought to be. The concept of the gothic double comes to mind - perhaps we might think of the Splinternet as the Mr. Hyde to our Dr. Jekyll. But instead of just double, the Splinternet references fragmentation, or balkanization, of the many-to-many-th degree. Within the shadow twin of the Internet can be multiple internets, a nesting doll of networks of networks, each of which constitute an internet which is not the Internet.





However, the conversational dichotomy of the Splinternet as the anti-Internet has made the term quite ambiguous and sort of a catch all for fissures of multiple, indiscriminate kinds such as the ones listed here. This wide expanse and variety makes it difficult to define what it is we're actually trying to prevent.

One of the most popular uses of the Splinternet is when referencing network outages, often due to infrastructural fender-benders, government-mandated blocking of content via techniques such as packet interception, throttling or in some cases full-scale shutdowns.

[1] Clyde Wayne Crews, "The SplinterNet", Forbes, 2001. https://www.forbes.com/forbes/2001/0402/036.html

[2] Aparna Kumar, "Libertarian, or Just Bizzaro", Wired, 2001. https://www.wired.com/2001/04/libertarian-or-just-bizarro

[3] Dan York, "What Is a Splinternet? And Why You Should Be Paying Attention", Internet Society, 2022. https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/

The term is also often used to reference fractures in approaches to governance, such as data-localization mandates to contain information within geographical borders or initiatives to replace multi-stakeholder institutions with state-centric or private control.

Perhaps the most visceral association with the word is when referencing not the Internet itself but the user experience of the web. Many of us with casual acceptance discuss content shown to us by “our” algorithms, signifying that my Internet is different from your Internet. ”Internet” here refers to not the multiple layers of infrastructure and protocols and governance that facilitate the transmission of my dog videos vs. your cat videos, but the platforms which feed themselves from the data we generate when we loiter in their privatized public square. Indeed, much of what Crews’ initially imagined for parallel Internets has come to fruition through the centralization of services. Geoff Huston, chief scientist at APNIC, describes centrality and fragmentation as “diametrically opposed perils” regarding the risks they pose to the open Internet...though it’s also curious how they reinforce one another. Most people’s perception of the Internet is dominated by the same handful of tech companies which paradoxically fragments our experience further - not by consensus-driven commons, but by market-driven segmentation.

But throughout the 2000s and early 2010s, collapsing all of these different uses into the same bucket of Splinternet or anti-Internet was a seemingly straightforward technique, at least for the production of the concept. Until recently, initiatives such as Russia’s RuNet, China’s Great Firewall and Iran’s National Information Network have fallen neatly on the side of “splintered” and much of the Western world fell, at least in the Western World’s telling of it, fell neatly within “the Internet”. But as the thematic for Splintercon Paris has pointed out, shifts over the past decade in Internet governance and the rise of so-called digital sovereignty initiatives have complicated these categories.

The thematic asks: “How can governments balance protectionism without splintering the digital commons? Do ambitions for sovereignty lay the groundwork for isolation?” In reference to the EU’s pursuit of digital sovereignty as “both a regulatory and technical project, driven in Section

[4] Geoff Huston, “On Centrality and Fragmentation", The ISP Column, 2023. https://www.potaroo.net/ispcol/2023-07/fandc.pdf

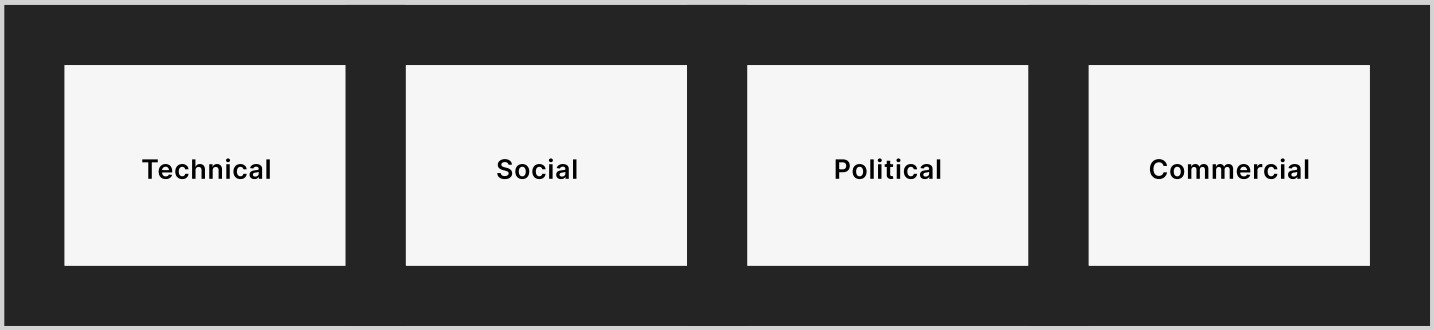
by a desire for independence from American and Chinese control over cyberspace," and the "growing number of states, including Australia, Brazil, Canada, India, and South Africa" who are also considering their own approaches to "strengthen domestic industries and secure their networks", the organizers have asked us to consider, "Are these models complementary, or do they reinforce competing visions of the internet?"

What these national initiatives, and the provocations surrounding them, signal is that the evolution of the Internet has complicated the popular dichotomy of "Splinternet bad, Internet good," or more generally the concept of the Splinternet as the anti-Internet. ***What happens when we begin to see ourselves in the mirror of our gothic double?***

Is Brazil's focus on large-scale state-supported Internet Exchange Points different from Iran's focus on nationalized Internet infrastructure? Are the EU's "digital sovereignty" and routing resilience proposals risking the vision of an open Internet that it has historically been a proponent of? While the knee jerk reaction is to say no, if nothing else because of the interests and principles of their implementers, we need more language and definition to model and reason about these approaches.

Categorizing the Splinternet

By Approach



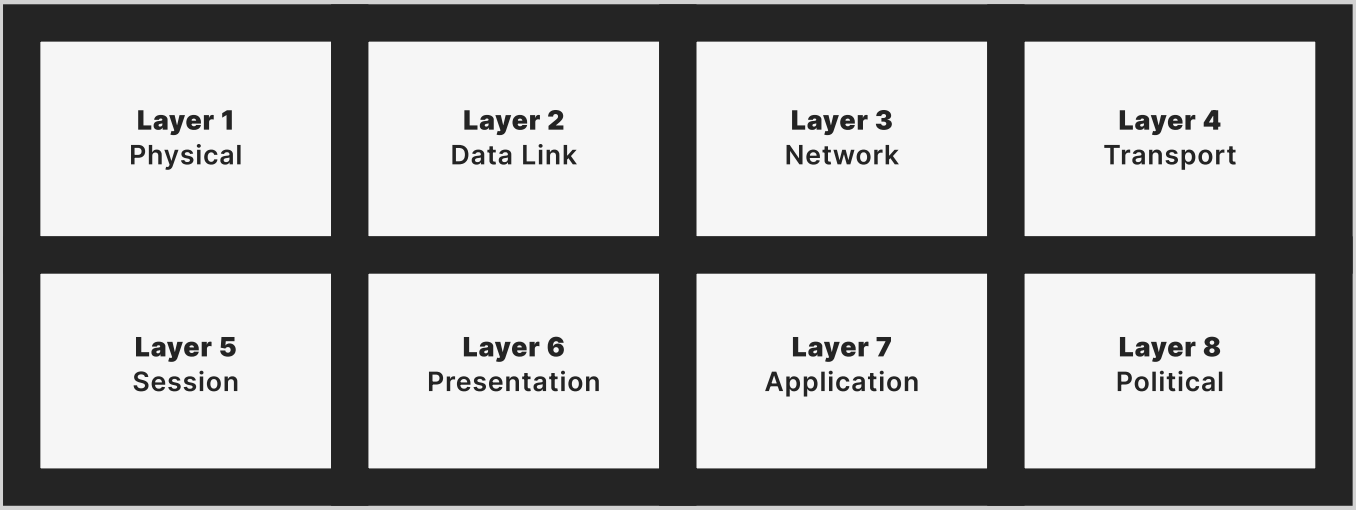
One starting proposal might be to sort them by their approach such as, technical, social, political, commercial - but most examples will quickly reveal that the barriers between these divisions are porous.

[5] SplinterCon Paris, 2025. https://splintercon.net/paris https://www.potaroo.net/ispcol/2023-07/fandc.pdf

For example, DNS court orders which mandate ISPs and DNS resolvers to effectively block content by returning incorrect DNS answers are technically technical interventions - but describing them as such doesn't properly describe the scope of their impact. Many cases such as these merge legal authority, commercial interests and technical infrastructure and make it difficult to describe them in any one mode of fragmentation.

By Layer

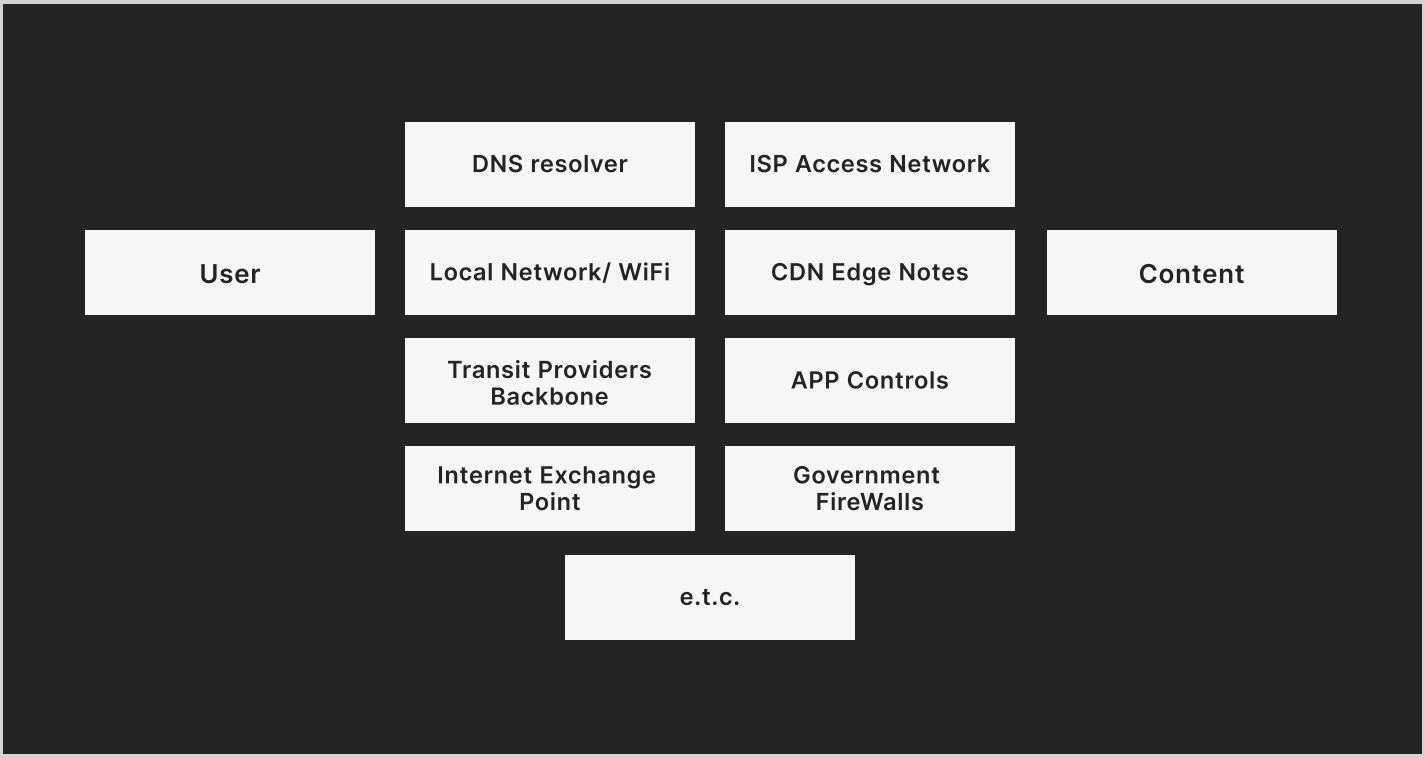
Another proposal might be to categorize splintering techniques by where they operate in the Internet stack. Making content inaccessible via TLS throttling can be described as a Layer 4 technique while could be positioned at Layer 7. Techniques which rely on governance or legal techniques could be defined to occur at the so called Layer 8 of politics, though that's potentially too broad and might require further definition.



By Place In The Path

Another slight modification here would be to instead describe interventions in terms of where they interact with a packet's path from user to content and back, from a user's device to their eyeball ISP to DNS to CDNs or transit networks and so on. This is a more fine-grained approach, but in the ever evolving Internet landscape it's tricky to say what's a "typical" experience of a user's experience accessing content is- defining standards and expectations around what a splintered vs. un-splintered path might be challenging when the patterns of those paths change on the order of milliseconds. Plus, neither of these categorization app

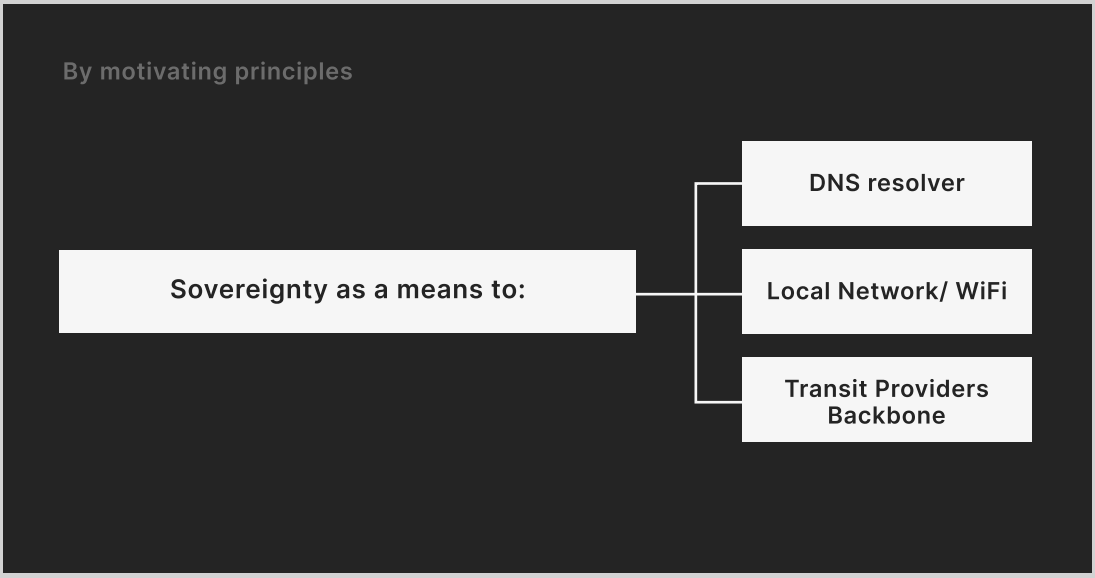
roaches do much for describing the nuance of intention — part of what we need more articulation around is how an approach to sovereignty can support democratic and open principles vs. authoritarian ones. Their impact and location on the technical stack can only do so much. Indeed, the same way engineers, hackers and researchers will often scoff at the degree of accuracy and precision that scholars of the humanities leave out of their writings on the Internet, the same can be said for the way technical-forward interpretations lump together the machinations of politics and the economy.



By Motivating Principles

We might also consider sorting the Splinternet and different approaches by their stated motivating principles, in other words, what vision of the Internet are they trying to create? Do they present sovereignty as a proactive measure to strengthen participation in the global Internet or as rationale for structural disconnection? Many recent examples of digital sovereignty movements make appeals to both the “good” Splinternet and “bad” Splinternet by emphasizing the need for autonomy and control while still pledging their commitment to the global project of interconnection. This kind of rhetoric suggests that we can and should create a third category which, in reference to the thematic, seek to provide complementary models instead of competing visions.

But is this possible in practice? It's all well and good to say this is what you want but it sounds a bit like having your cake and eating it too. How will we know that these efforts are accomplishing the balance they say they will?



By Measured Impact

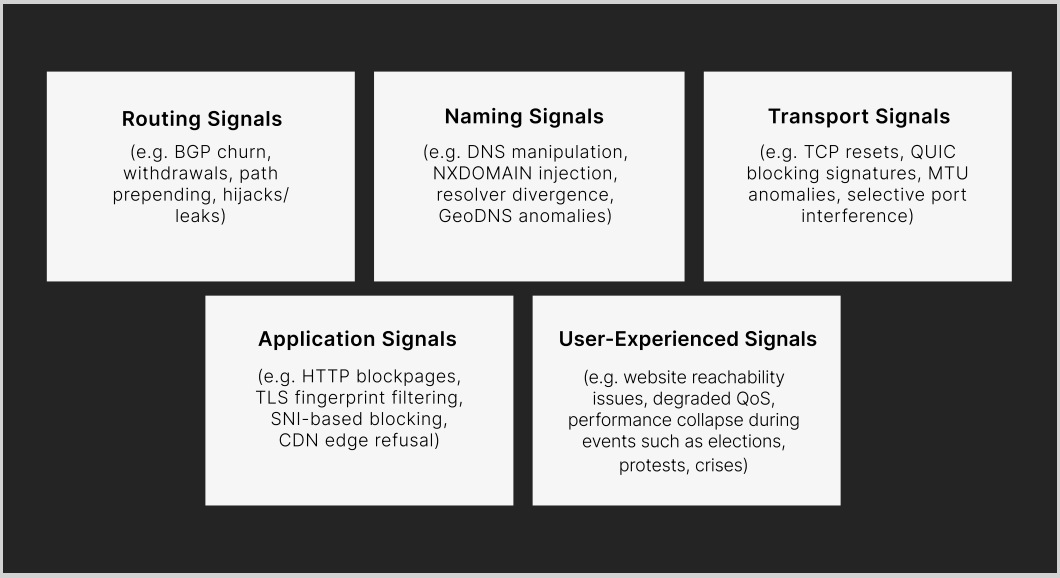
Perhaps a more practical way to approach categorization is by utilizing data-driven evidence and asking what impact can we quantify that these techniques have on the Internet? If actors say they are motivated by a global, interoperable Internet, can we find evidence of that in the data? Can we measure if the Internet is more or less fragmented as a result of a given nation's approach? Signals from routing, naming, transport, application and user-experience measurements can help distinguish fact from fiction, impact from rhetoric.

GEODE's analysis of BGP data, which examines the gap between the architecture of connectivity and publicly stated levels of political cooperation, shows how socio-political analysis combined with the study of technical artifacts can provide a framework for more effectively contextualizing and categorizing the Splinternet. However, this kind of contextualization is extremely difficult, particularly at scale. Doug Madory has written extensively about the risks and pitfalls

[6] GEODE. https://geode.science/en/cartography-of-the-datasphere/

[7] Doug Madory, "Subsea Cables Parted in Red Sea Again", Kentik, 2025. https://www.kentik.com/blog/subsea-cables-parted-in-red-sea-again/

of over-indexing on or oversimplifying data, especially when attempting to attribute activities associated with Internet fragmentation. An enormous amount of contextual knowledge is required to determine whether or not a cable cut in the Red Sea was intentional or not, or whether networks disconnecting from one another are the result of competing economic

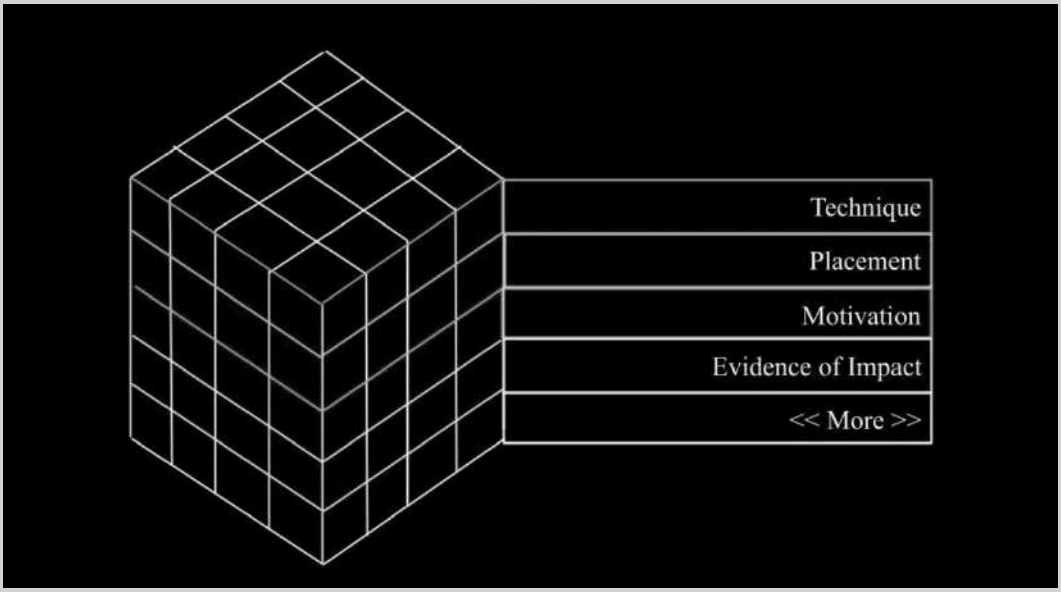


interests or the result of politically motivated government interventions. Even with that context, however, such determinations are often difficult to “prove” at least in the legal sense of the word.

Many fragmentation activities can look identical in the data and if we attempt to categorize them by their motivation and the actors enabling them, attribution becomes blurry - specially for activities that unfold over longer timescales than discrete “events” such as outages or shutdowns. For example in Cuba, the practice of network interference during protests is common; however there is also much reporting of the poor network quality, which can make the low baseline of Internet quality hard to distinguish from that of a throttling event.

While categorizing the Splinternet by its impact using data-driven techniques is compelling, it poses unique challenges which might hinder its scalability.

With all of these potential approaches to categorization and their potential pitfalls in mind, we probably need some hybrid, matrixed approach which considers technique, placement, motivation and evidence of impact and likely more vectors I haven’t covered here. No one approach will cover all of the dimensions but perhaps can provide enough shape to define these models emerging between the space of “good” and “bad”, Internet vs. Splinternet.



That said, I'd like to pose a question that came up for me while considering these examples. Do categories really matter if the end result is the same? Does it matter if the inability to connect and perform basic tasks online is due to geopolitical or economic interests? Does it matter if an outage is due to an infrastructural failure or a politically motivated action?

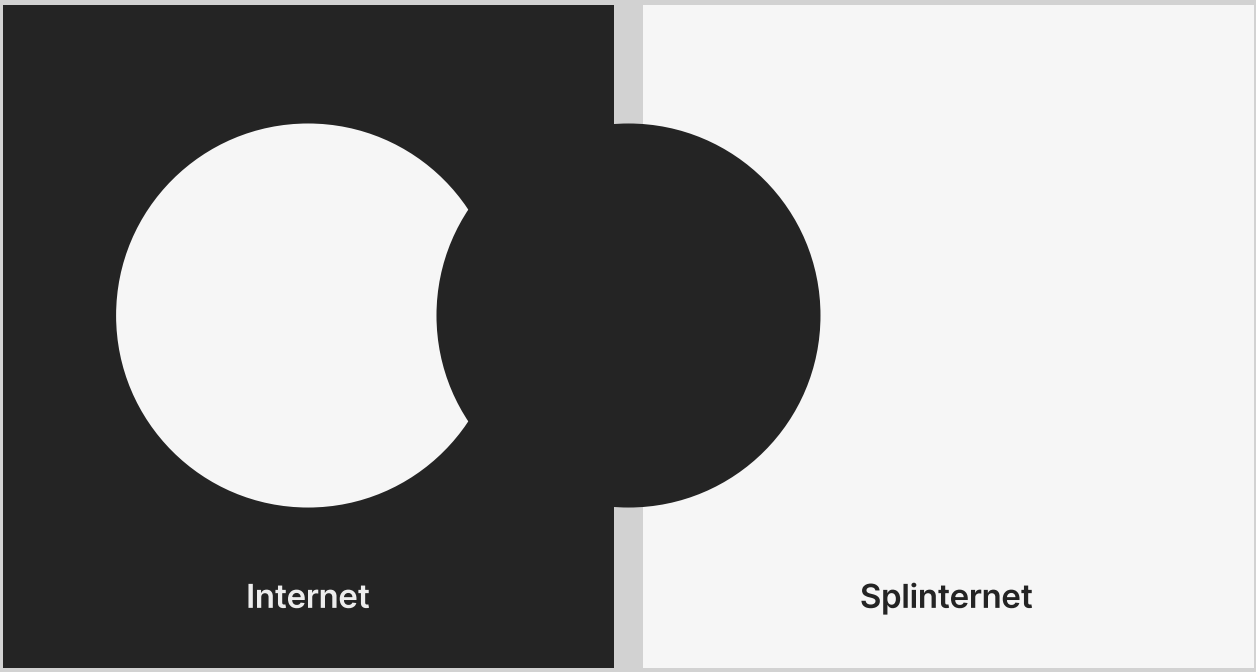
On the one hand, yes, if only because they hold different parties responsible and suggest a different menu of solutions - but in terms of defining the Splinternet, if an individual or community's access to content is restricted, then perhaps that's the only definition of the Splinternet that we need. Is the Internet facilitating global, end to end communication or is it not? And what if the answer is no?

The Internet Has Always Been Splintered

If the Internet is a "unified, open, global network that everyone in the world is able to access and benefit from" I would argue that such a state has never been. That is, the Internet has always been the Splinternet and vice versa and that the blurry boundaries of these modes is nothing new. Perhaps there is no such thing as the Internet and the Splinternet, but only one entity that is a combination of the two.

[8] Doug Madory, "A Network Crumb Back Story: A Baker's Dozen Retrospective", Kentik, 2025. https://www.kentik.com/blog/crumb-back-story-a-bakers-dozen-retrospective/

[9] Cuba, Freedom of the Net Report, 2021. https://freedomhouse.org/country/cuba/freedom-net/2021



If the Internet is a “unified, open, global network that everyone in the world is able to access and benefit from” I would argue that such a state has never been. That is, the Internet has always been the Splinternet and vice versa and that the blurry boundaries of these modes is nothing new. Perhaps there is no such thing as the Internet and the Splinternet, but only one entity that is a combination of the two.

For starters, an estimated 30% of people globally do not have access to the Internet, and so in the most basic sense the Internet is fragmented in so far as some people can access it and some people cannot. This is a predictable circumstance given the uneven “rollout” of the Internet which has always been molded by economic and political incentives - but its result is a radically bumpy texture across the surface area of the network. Digital culture and literacy vary depending on when individuals and communities come online and from a technical perspective, so does quality of experience. Even once you’re connected, your experience can vary dramatically depending on where you connect from. For example, connecting from a rural area via satellite vs. a fiber-to-the-home connection in a big city are two different experiences in terms of network quality. Similarly, a user’s path to content is often much less direct outside of North America and Europe, and yet all of these

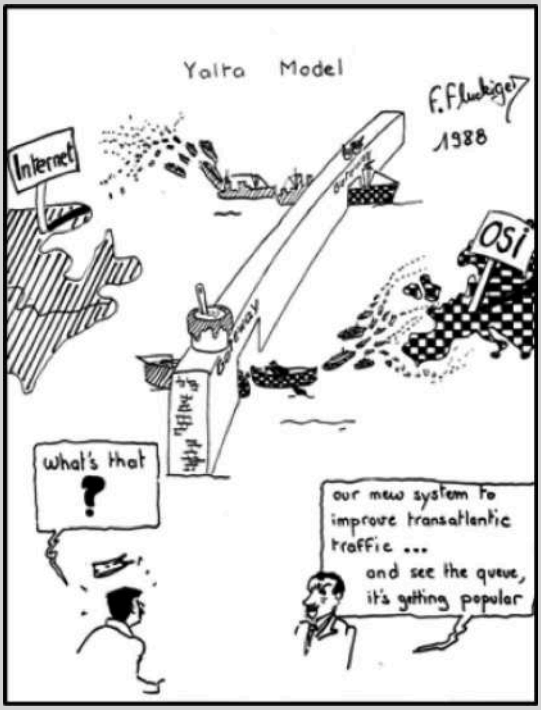
[10] International Telecommunication Union (ITU), Measuring Digital Development. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[11] Adam Rothstein, “How to See Infrastructure: A Guide for Seven Billion Primates”, Rhizome, 2015. https://rhizome.org/editorial/2015/jul/02/how-see-infrastructure-guide-seven-billion-primate/

experiences are currently summed up under the umbrella of “the Internet”. These disparities are inevitable to a degree. It would have been impossible to implement a global Internet in a uniform fashion in one go, much like it would be impossible to build a city in one day.

The Internet is not so different from a city; they are, after all, both fundamentally infrastructures and as the writer Adam Rothstein has pointed out, “Infrastructure's power, combined with its lack of visibility, is the stuff of our society's physical unconscious”. In a city, some neighborhoods have more potholes than others, some have more access to grocery stores - what it means to live in New York City can vary block to block. Why? The answers are almost always not solely technical. Similarly, the Internet is as situated within a political economy motivated by commercial and political and public interests as much as any other infrastructure and because of this the Internet is inherently splintered in terms of access and experience. **Since its creation, being connected to the Internet has never meant that you have the same quality of experience as everyone else.** But despite these discontinuities, cities and networks are bound together by common principles, shared values and use of common resources. For the Internet, this is the TCP/IP stack, the use of which has become so expected, that we often abstract it away as an assumption. To be connected to “the Internet” is to use Internet protocol. But it wasn’t always so, or at least it wasn’t always a given that TCP/IP would be how we would globally connect.

The so-called Protocol Wars showed that “some people foresaw a division between world technologies: Internet in the United States, OSI



François Flückiger (1988)

in Europe." Whether or not what we consider "the Internet" today would be fundamentally different we had chosen X.25 is a very fun question, but the premise of the question suggests that the Internet, as in the global end to end network that runs over TCP/IP was not inevitable, and could have been written to operate more than one way. Such precedent suggests that the vision of the Internet, not in terms of TCP/IP, but in terms of how to globally connect, was fragmented from the start.

When we look at the transitions between the protocols that we've progressively stacked on top and below TCP/IP, such as adoption of DNNSEC, moving from IPv4 to IPv6 or adoption of RPKI, these moves have often been bumpy and staggered as well. You get a sense of Tarzan swinging from vine to vine, loosely threading a connective tissue through a fragile ecosystem that could and might break at any time - but also, curiously hasn't, or at least in a way that has prompted splinter-y speculation. Indeed, the concept of the Splinternet is curiously reserved for only some kinds of fragmentation, despite always being part of the Internet's story.

If we accept that the Internet has always been fragmented, then the project of defining the Splinternet can become less about defining an "anti-Internet" but parsing the limits of the Internet's own fragmentation. The Internet was created in a state of splinter and has continued to be splintered but how splintered are we willing to let it become, and in what ways?

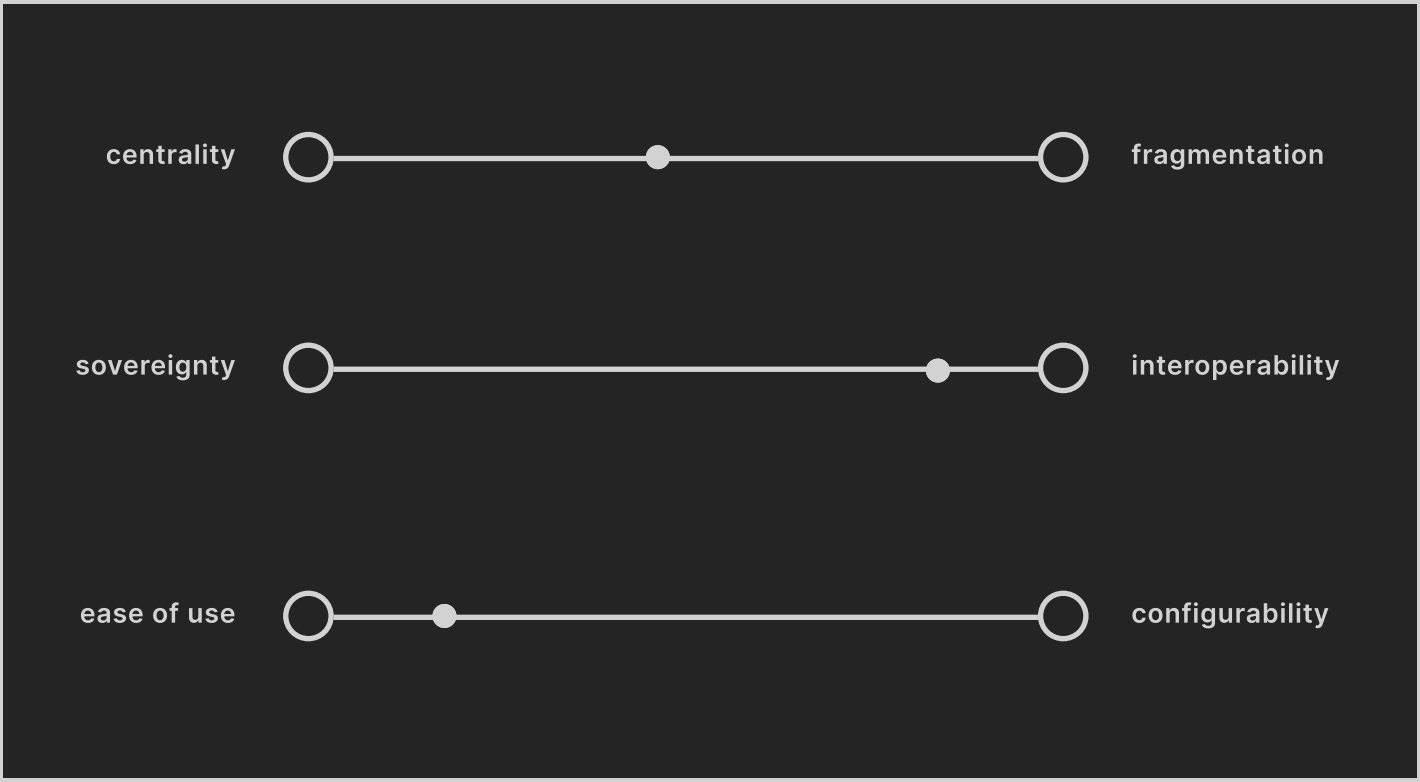
Sometimes I imagine the Internet as a glacier and all of the ways it can be fragmented as tiny taps on top of it which create cracks. If the Internet has always been fragmented and these taps are just part of its natural evolution, then the question is - what kinds of cracks will make the glacier break apart safely and perhaps most importantly, which cracks will result in shapes that can be put back together again?

Calling back to the "diametrically opposed perils" of centrality and fragmentation, perhaps the Internet, in its continuously fragmented state, is situated on a spectrum between them, sliding back and forth depending on the decisions of the many actors which enact their principles and design decisions upon it.

[12] François Flückiger, "The Protocol Wars," 1988. https://en.wikipedia.org/wiki/Protocol_Wars#/media/File:Internet-OSI_Standard_War.jpg

In fact, every design decision of the Internet is likely situated between two ends of a spectrum, such as sovereignty and interoperability, privacy and transparency, ease of use and custom configuration.

Perhaps the definition of Internet is not a “whole” entity that exists on one side, fragmentation or another, but one that is able to traverse between the extremes of these tradeoffs with relative ease.



The Splinternet might then be less about the degree to which the Internet is fragmented but the degree to which it's stuck in one particular state of fragmentation, or in other words, one particular setting of the sliders. The Splinternet might then be less about the degree to which the Internet is fragmented but the degree to which it’s stuck in one particular state of fragmentation, or in other words, one particular setting of the sliders. I propose that the Splinternet is not the anti-internet but the static Internet. The Internet which cannot evolve and repair itself from fragmentation as it inevitably occurs.

Chapter 2

Weaponization of routing in the struggle for sovereignty

By Louis Petiniaud,

a researcher in the ERC Dataroutes Project at the GEODE research center and the French Institute of Geopolitics, and an associate researcher at Cassini Conseil. His research focuses on the geopolitics of Internet infrastructures, connectivity, and governance, and on their role in shaping spatial dynamics in contexts of war and conflict. Combining Internet measurements with field research, he has worked extensively on Ukraine, Russia, and the post-Soviet region.

By Frédérick Douzet,

a is Professor of Geopolitics at the University of Paris 8, director of the French Institute of Geopolitics research team (IFG Lab) and director of the Center for Geopolitics of the Datasphere (GEODE). She has been appointed to the Bronner Commission on Disinformation and the French Defense Ethics Committee, and was part of the drafting committee for the French Strategic Review of Defense and National Security in 2017. A former director of the Castex Chair of Cyberstrategy at IHEDN and Commissioner of the Global Commission on the Stability of Cyberspace, she has received numerous awards for her research including the FIC Book Prize for Strategic Thinking and the France-Berkeley Fund Award for Outstanding Young Scholar.

The Internet's architecture is transforming

Data routing, the process by which data packets are transferred from one point of the globe to another, is one of the core processes structuring the Internet. While the Internet is primarily a complex mesh of cables and other physical infrastructure, it is also defined at the logical layer as a "network of networks." The Internet is made up of approximately 90,000 interconnected networks called autonomous systems (AS), run by entities of varying sizes and types, belonging to public or private institutions: Internet service providers (e.g. Vodafone), major content providers (Netflix, YouTube etc.), international transit operators (Lumen, Cogent), etc.

When an Internet user in Paris wants to access a website or video hosted across the Atlantic, the data traverses multiple autonomous systems, each selecting the next route. To ensure the stability of the system, operators often maintain alternative connections so that traffic can continue to flow even if some links become unreliable. In the Internet, the routes data use are therefore not only physical (they rely on transmission infrastructure) but also logical (they depend on actors that run these infrastructures, host data and interconnect).

Historically, the architecture of connectivity (i.e. the way autonomous systems interconnect to create routes for digital data) has been conceived as a decentralized process whereby each actor was free to connect, transmit data, and cooperate with others, provided they complied with shared rules (such as standards and protocols), defined and adopted through a relatively horizontal "multi-stakeholder" model of governance. The functioning of the network thus relied on trust among these actors, while security only became central in the 1990s and 2000s.

However, digital infrastructure is embedded in broader geopolitical dynamics, as the various public (states, agencies, institutions etc.), private (network operators, content providers, companies) and individual actors who structure, shape, and influence it often pursue divergent and sometimes conflicting interests. Increasingly, data routing emerges as both a site and a vector of geopolitical tensions and conflicts. Actors increasingly seek to control parts of the network, including how data circulates geographically, and leverage it to project power onto domestic and foreign territories. By doing so, these actors contribute to forms of fragmentation, understood as progressive and layered spatial differentiation of routing practices, dependencies, and governance policies, that challenge the global resilience

of the Internet but also raise significant geopolitical risks and threats to human rights.

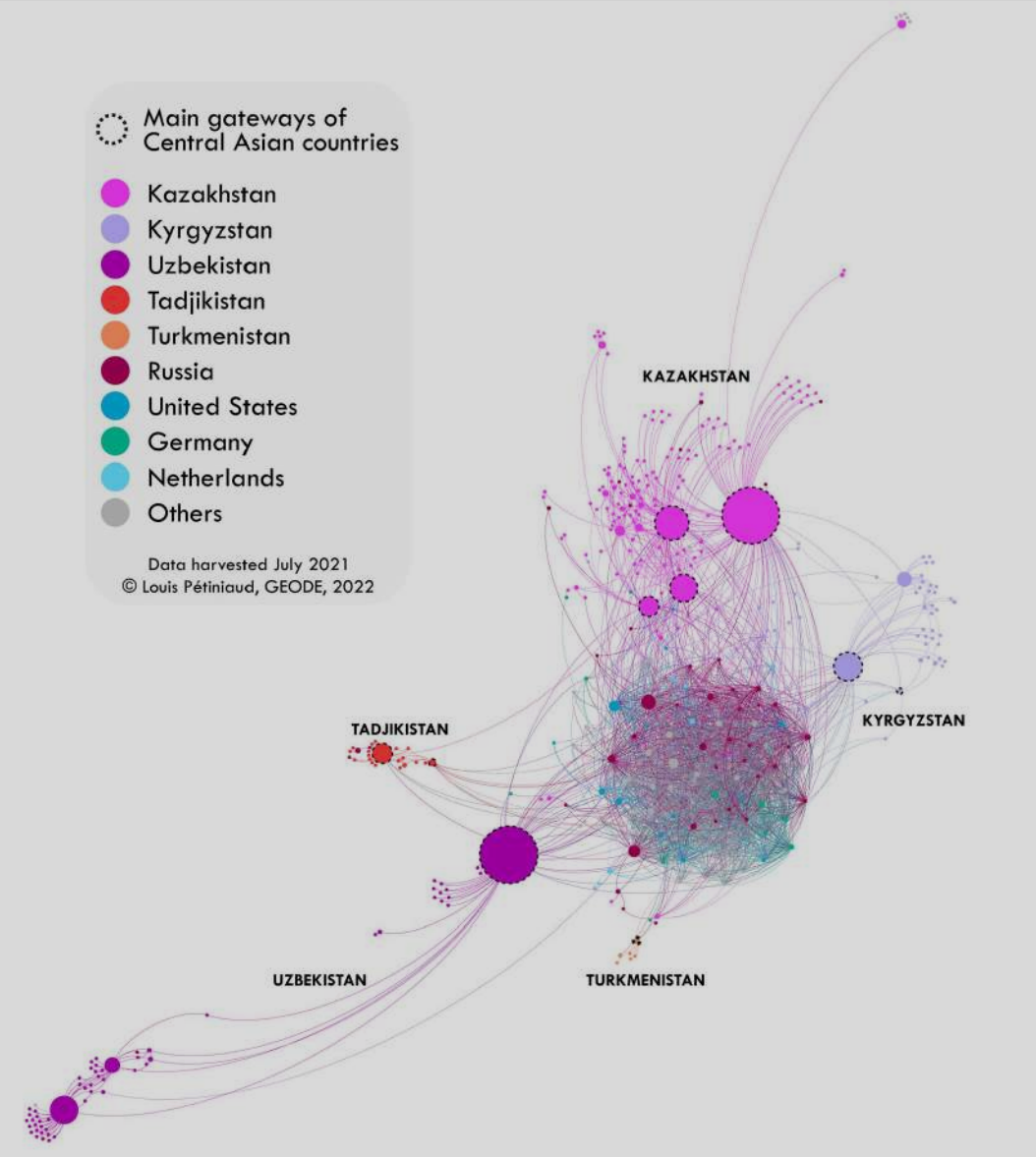
Studying Internet routing from a geographical and geopolitical perspective reveals that political power is embedded in the logical architecture of connectivity. Routing is not merely a technical process but a site where territorial strategies, strategic dependencies and vulnerabilities, and market concentration materialize, shaping the fragmentation of the global network. In the context of the ERC Advanced Grant DATAROUTES led by Pr. Frédérick Douzet, the GEODE research center has engaged in a large study of the geography of Internet routes and how they can be manipulated for strategic purposes by state and non-state actors. Using a BGP observatory that collects routing data as well as open-source tools to research the geography and geopolitics of digital infrastructures, GEODE has participated in this edition of Splintercon to provide a geopolitical understanding of current fragmentation dynamics in the Internet.

Three main dynamics are reshaping Internet routes for distinct political and strategic objectives while accelerating its splintering. First, the architecture of the network is hierarchical, which creates for some countries issues of access and route dependence on other states. But this architecture is quickly evolving in an unprecedented manner. Internet giants and hyperscalers are actively working towards operating larger parts of the network from user to content, structuring a concentration of data paths. Second, under the auspices of the concept of “digital sovereignty”, a growing number of governments enact infrastructural policies that aim at constraining data flows alongside national borders. Third, state and private actors engage in the strategic manipulation of connectivity during open conflicts for territorial control.

The Internet’s architecture is transforming

Imagined as a distributed interconnection, the architecture of network connectivity has evolved into a hierarchical structure: transcontinental transit players dominate this hierarchy. At the bottom of the ladder were users and content providers. The former rely on ISPs and transit providers to access content, the latter needed worldwide transit providers to make their content available to the most consumers. This pyramidal organization gives structural power to those players higher up than the others, and this dynamic is translated into geopolitical dependencies as well.

Central Asia provides a clear example of this type of dependence. Most countries in this enclaved region have multiple cables connecting them to their neighbors including other countries in the region, but also to China, Afghanistan and Iran. However, for commercial, technical, and economic reasons that are themselves the result of Russia's centuries-long domination of the region, these countries have little intra-regional connectivity and connect to the global internet, even to their physical neighbors, almost exclusively via Russian (and Kazakhstani) providers, making them highly dependent on Russia for Internet access.



[13] Louis Petiniaud, "The Human Factor in the Geopolitics of the Internet", 2023 "https://labs.ripe.net/author/louis_petiniaud/the-human-factor-in-the-geopolitics-of-the-internet/

While this type of country-to-country dependency remains common for multiple states, notably in enclaved territories and/or in post-imperial and post-colonial contexts, private actors are also implementing strategies that shape growing and broader strategic dependencies related to data infrastructures. The originally decentralized nature of the network has significantly changed in the past two decades. The advent of large Content Delivery Network (CDNs) in the 2000s and the quicker expansion of Internet hyperscalers in the 2010s and 2020s have fundamentally altered the decentralized way the network previously managed data transit. Hyperscalers like Meta, Google (Google Cloud), Amazon (AWS) or Microsoft (Azure) who previously concentrated their activities as content providers, have positioned themselves as central and unavoidable actors of the global data infrastructure.

Léa le Pezron explains that over the past decade, some major technology platforms have evolved from large content providers into transit infrastructure owners. Google, Meta, Amazon (AWS), and Microsoft now deploy private wide-area networks that span continents. They also invest in submarine cables, build or lease long-haul fiber, and push edge infrastructure closer to users. Increasingly, they bypass traditional transit operators altogether, and the once hierarchical structure is progressively being replaced by integrated architectures. A growing share of global traffic now circulates inside optimized proprietary networks. Often described as the “flattening” of the Internet, this development reflects a concentration of both services and routing capacity in the hands of the same firms.

This dynamic is largely traffic-driven: while video streaming first concentrated flows within a few platforms, cloud computing intensified this trend, and generative AI is accelerating it further, given its dependence on hyperscale data centers. By internalizing traffic, platforms reduce congestion on traditional backbones and improve performance for their users. However, this raises two fundamental issues for the overall resilience of the network. First, hyperscalers are not neutral transit operators. They optimize for their own services, and, by diverting traffic away from traditional carriers, and weaken them. While user performance often improves, route diversity decreases, and increasing volumes of traffic depend on a shrinking number of vertically integrated actors. Second, concentration fosters single points of failure. Major outages, such as the Facebook disruption in 2021 or large-scale AWS incidents, have shown how one network’s failure can cascade globally, at a time where hyperscalers are increasingly integrated within sovereign functions of many states. These risks are also amplified by opacity, as routing architectures remain largely inaccessible to regulators and researchers.

sovereign functions of many states. These risks are also amplified by opacity, as routing architectures remain largely inaccessible to regulators and researchers.

Most hyperscalers are U.S.-based and subject to extraterritorial legislation (e.g. Cloud Act), and the concentration of transit power, cloud infrastructure, and content distribution creates strong structural dependencies. This affects regulatory capacity, digital sovereignty, and infrastructure resilience. This growing private concentration of routing power partly explains why states increasingly seek to reassert control over data flows through sovereignty-driven infrastructural policies.

Building borders for data

Concepts related to the idea of “digital sovereignty” (including information sovereignty, cyber sovereignty, etc.) often serve as a political justification for a wide variety of state strategies. This concept gained significant traction in the 2010s across a growing number of countries. This attention to the control of data, standards, hardware and other parts of the network has been shaped by both global and localized geopolitical events such as the Arab uprisings of the early 2010s, the Snowden revelations in 2013, information operations during the 2016 US presidential campaign or, more recently, the second term of U.S. President Donald Trump. The idea of digital sovereignty generally encompasses a strongly territorialized view of the “global network” and has led to a variety of policy responses across different political systems that tend to reshape it alongside geopolitical borders.

While examples from authoritarian countries like Iran or Russia have been well documented as holistic attempts to build “sovereign Internets”, other more nuanced case studies help understand the wide policy spectrum this idea encompasses.

At Splintercon 2025, a wide range of researchers from the GEODE research center presented their ongoing research on case studies in Cuba, Pakistan, Australia, and Canada. They showed how states seek to influence, and in some cases enforce policies that shape how, where, and through which actors data packets transit.

In Cuba, Margot François’ work has shown how digital sovereignty is built not only through state-led, top-down strategies of control, but also through configurations of restricted access to connectivity shaped by scarcity (a context of shortages and economic crisis) and geopolitical exclusion (US embargo). The Cuban case highlights a peripheral form

of network fragmentation that results not only from state choices but also from external sanctions, and contributes to shifting the analysis of "splintering" to non-hegemonic contexts, highlighting the role of access inequalities and local adaptations in the production of diverse forms of digital sovereignty.

Drawing on the case of Pakistan, Nowmay Opalinski shows how territorial and security-driven conceptions of cyberspace shape Internet infrastructure and ultimately affect its resilience. Building on GEODE's digital network mapping methodology, his analysis demonstrates that infrastructure over-concentration facilitates state control, but at the expense of network reliability and connectivity efficiency.

In Canada, where the relationship with the US is marked by growing tensions, efforts to strengthen digital sovereignty and reduce dependence on US infrastructures have significantly risen. In her research, Celestine Rabouam emphasizes the major vulnerabilities of Canadian Arctic connectivity. In these regions, the lack of cooperation among local stakeholders among other reasons makes networks rely heavily on satellite systems mostly routed through the US. While Starlink development in these territories offers increased capacity and resilience, the induced dependence on US actors sharpens the tension between the need for sovereignty and the need for connectivity in remote regions.

Sophie Hamel demonstrates that, since the 2010s, the Australian government has implemented measures to control and restrict digital infrastructure suppliers, primarily against espionage and interference risks associated with Chinese actors. On the other hand, the Australian Department of Defense has set up a Top Secret Cloud with AWS.

Canberra, however, also uses digital infrastructure as an influence tool, by financing projects in Pacific Island states which it sees as a strategic extension of its own networks, in order to exclude Chinese technology and capital and to favour "trusted" economic partners. These policies participate in fragmenting the network both by preventing direct connections to China and by excluding Chinese suppliers from the Pacific islands, underlining how Australia uses technological dependencies as an instrument of its digital sovereignty.

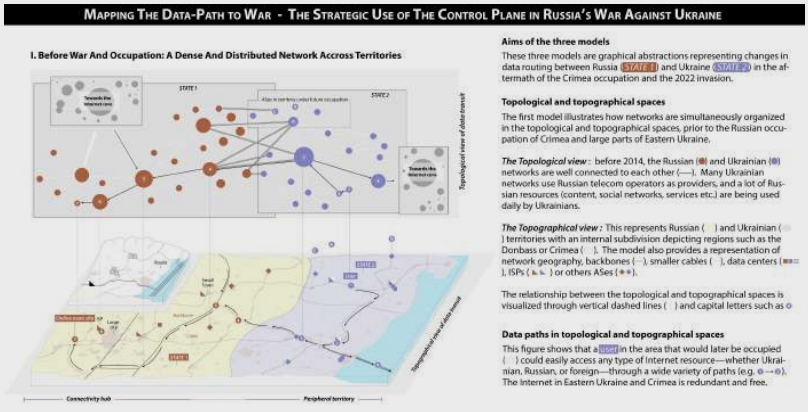
Manipulating the network to project power

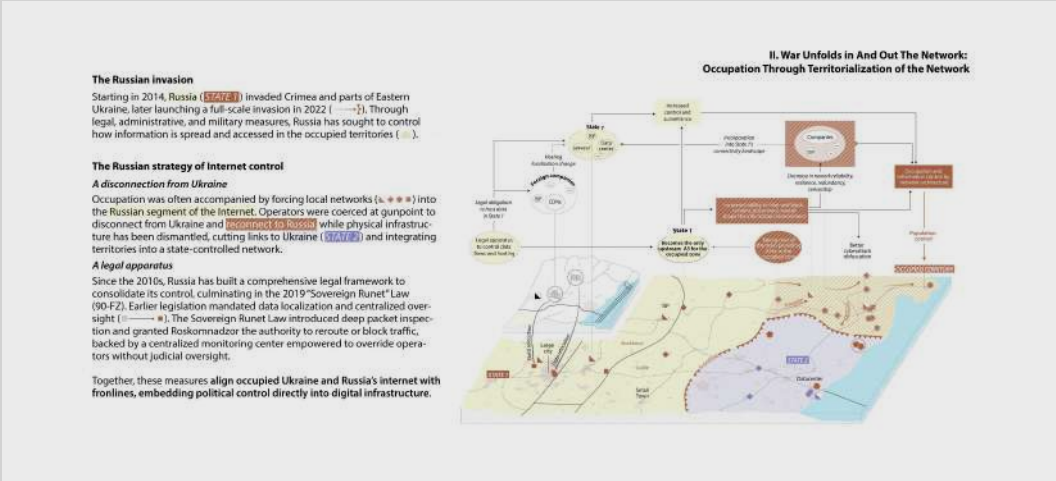
Governments, as well as private stakeholders, are also increasingly building policies in order to assert their power over territories in the context of open

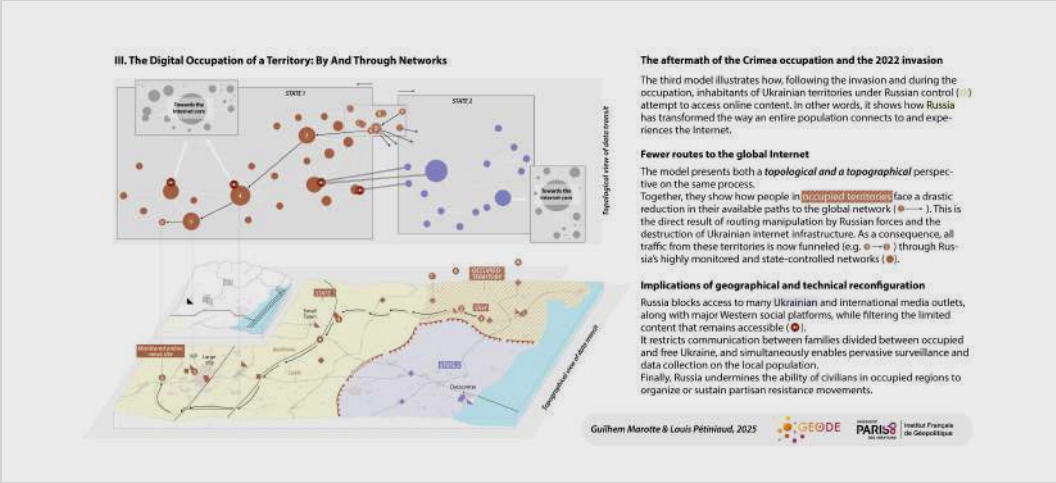
conflicts and wars. In the case of Russian invasion of Ukraine since 2014, Moscow has used network reconfiguration as a tool of territorial appropriation in occupied Ukrainian regions. Beyond military control, Russian authorities manipulated routing architectures and upstream dependencies to reinforce sovereignty through infrastructure.
By redirecting traffic flows and controlling interconnection points, they turned connectivity into an instrument of political domination.

In 2014, Ukrainian telecommunications infrastructure in Crimea was replaced and traffic was rerouted through Russian backbone networks controlled by the government. After the 2022 invasion, Kherson became an emblematic case where local providers were disconnected from Ukrainian upstream operators and forcibly re-peered with Russian transit networks at gunpoint, effectively integrating local access providers into Russian-controlled infrastructure, but also into the Russian so-called “Sovereign internet”. This rerouting de facto severed access to Ukrainian networks
and exposed traffic to centralized filtering and surveillance. As major platforms widely used in Ukraine, such as Facebook and Instagram, disappeared, access to many independent information outlets also vanished, aligning the region with Russia’s increasingly controlled information space.

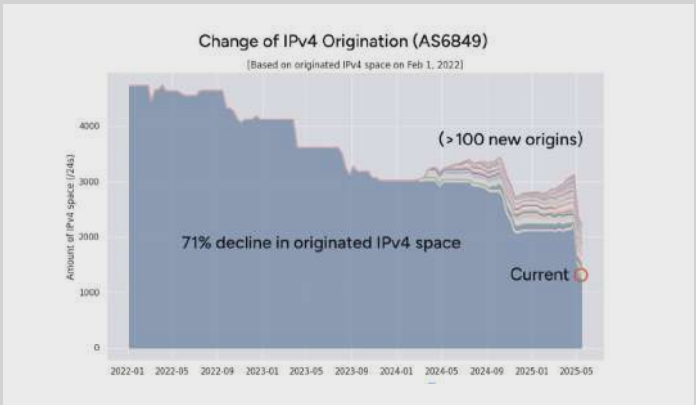
Shortly after the start of the full-scale invasion in 2022, Kyiv has also set up policies that seek to shape an “information shield” based on infrastructural policies. These included the unprecedented decision of blocking 600 Russian Autonomous Systems, effectively blocking approximately 48 million Russian IP addresses. Furthermore, private actors Lumen, Cogent and the London Internet eXchange Point (IXP) LINX also enacted sanctions against some of Russia’s main international carriers and disconnected them, signaling a rare and clear geopolitical stance by private Western network operators.







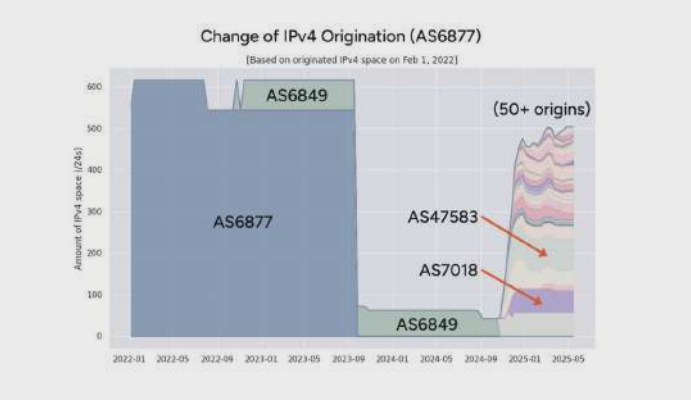
Doug Madory's presentation analyzes the large-scale migration of Ukrainian IPv4 address space following Russia's full-scale invasion in 2022, using BGP routing data, WHOIS records, and broker market signals to trace how formerly Ukrainian address blocks exited the region and entered global leasing markets. The core case study focuses on Ukrtelecom, Ukraine's incumbent telecom operator, specifically AS6849 and AS6877.



AS6849 experienced a steep reduction in originated IPv4 space:

- Declined from 4,728 /24 equivalents to 1,377 /24s.
- Represents a 71% drop in originated IPv4.
- Lost address space either:
  - Ceased being routed, or
  - Began being originated by ASNs outside Eastern Europe.

Routing analysis shows portions of this IPv4 space now originated by major international transit networks such as AS174 (Cogent), AS16509 (Amazon) and AS7029 (Windstream).



AS6877, a sister ASN of Ukrtelecom, saw an even more dramatic collapse:

- On February 1, 2022: 616 /24 equivalents originated.
- Today: effectively disappeared from the global routing table.
- Former prefixes are now originated by Tier-1 and major transit networks including:
- AS2914 (NTT)
- AS3356 (Lumen)
- AS174 (Cogent)
- AS5511 (Orange)

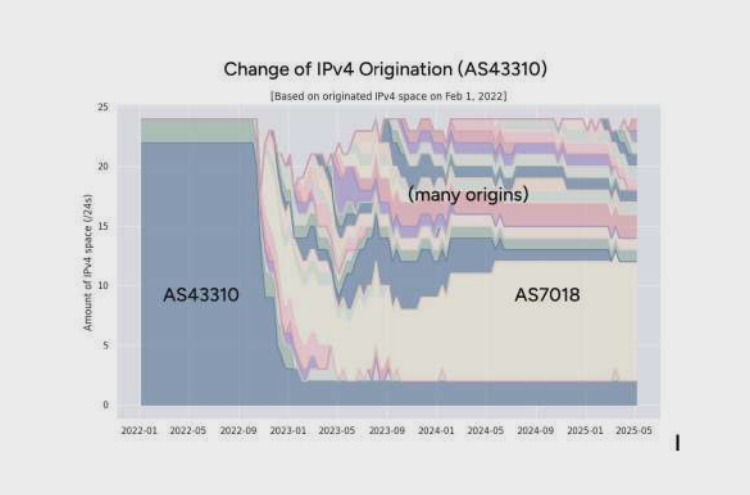
BGP and passive DNS evidence shows that some address ranges are still registered to Ukrtelecom in RIR databases but originated by foreign ASNs, indicating leasing arrangements rather than outright transfers. WHOIS lookups further reveal involvement of IPv4 broker IPXO (AS834), suggesting structured leasing of Ukrainian IPv4 space to foreign customers, sometimes with routes originated by AS7018 (AT&T).

Based on broker market rates ($100–$150/month per /24), even conservative estimates imply approximately $150,000 per month in potential leasing revenue for Ukrtelecom alone. This suggests that

leasing IPv4 space may represent a wartime financial survival strategy for Ukrainian operators. However, Ukrtelecom is not an isolated case. Other Ukrainian ASNs experienced similar patterns:

- LVS (AS43310) began 2022 originating 24 /24 equivalents; later those ranges were primarily originated by AS7018 (AT&T).

TVCOM (AS34092 and AS57033) also saw IPv4 migration out of Ukraine.



The case of Trinity (AS43554) in Mariupol is especially illustrative. It went offline in early March 2022 during the siege. Its IPv4 space began being originated by up to 54 ASes outside Ukraine. By 2024, much of the space was consolidated into Ukrainian content provider AS204384 (Sweet). During summer 2023, portions of Trinity's former IPv4 space were observed being originated by AT&T and confirmed to be used in residential proxy networks.

Residential proxies use legitimate IP address space to route traffic in ways that appear to originate from consumer endpoints. These services are frequently associated with web scraping, spam distribution, account creation fraud and account takeovers. Doug Madory documents Ukrainian IPv4 space being monetized through such proxy networks, with AT&T's AS7018 commonly used as the origin ASN. This practice provided cover under a reputable Tier-1 ASN, making filtering more difficult.

After investigative reporting by Brian Krebs expanded on Madory's findings, AT&T changed its policy. Customers were required to originate IP space under their own ASNs. This made proxy-origin traffic more identifiable and filterable. Proxy operators ceased using AT&T around October 28.

Doug Madory also examined manipulation of registration records in Russian-occupied territories.

Example:

- Prefix 151.0.0.0/20 originated by AS45025.
- Country field changed from “UA” to “RU” in July 2022.
- Later deleted from RIPE NCC records (April 4, 2024).
- AS45025 no longer in routing table.
- Address space redistributed among ISPs in Russian-held territories and leased to Western telecoms.

This sequence suggests administrative reclassification (“russification”), subsequent fragmentation and leasing; erasure of registry evidence. The deletion of RIPE records effectively purges historical evidence of Ukrainian association.

```
& Difference between version 3 and 4 of object "151.0.0.0 - 151.0.31.255"
@@ - 3,3 +3,3 @@
descr:  Online Technologies LTD
-country:  UA
+ country:  RU
geoloc:  48.045955739960114 37.96531677246094
@@ -10,3 +10,3 @@
created:  2012-01-05T13:39:09Z
-last-modified:  2018-12-10T12:06:53Z
+last-modified:  2022-07-18T12:09:23Z
source:  RIPE
```

This case study raises structural questions about the global IPv4 market: are brokers exploiting wartime distress? Or are leasing markets providing critical liquidity to struggling Ukrainian ISPs? Who bears responsibility when leased space is used in abusive proxy operations?

APNIC Chief Scientist Geoff Huston has recently questioned whether we have reached “peak IPv4,” noting declines in routed IPv4 and falling market prices. Madory suggests that increased supply from Ukrainian address space entering leasing markets may be contributing to these macro-level shifts. Doug Madory’s analysis demonstrates how geopolitical conflict manifests directly in routing tables, registry metadata, and secondary IPv4 markets. Ukrainian IPv4 space has transitioned from local origination to global monetization, often via Tier-1 transit ASNs, and in some cases into gray-market proxy ecosystems. The result is not simply an infrastructure collapse, but a reallocation of scarce IPv4 resources under wartime pressure—reshaping both regional connectivity and the global IPv4 leasing economy .

Section 1

Sovereignty as a market: private companies building digital authoritarianism

Chapter 1

Sovereignty as a market: private companies building digital authoritarianism

By Riccardo Nanni

a postdoctoral researcher in Politics of Digital Technology in Asia at CNRS Centre Internet et Sociéte. He obtained his PhD in Political and Social Sciences in 2022 at the University of Bologna and taught courses at the University of Padova, Université Paris 8 and Université Catholique de Lille.

Part 1. A market of sovereignty: circulation of standards and technologies

Sovereignty, especially in its state-centric definition, can be a driver of fragmentation. It can be about privacy, innovation, and ensuring that the powerful does not overpower the weak, but it can also be about isolation and control - thus triggering fragmentation. Evidence shows that countries such as China have increased their export of deep packet inspection (DPI) and other surveillance and traffic filtering tools in countries where centralising tendencies are emerging. A recent report by the InterSecLab, based on a leak, points in this direction. The company at the center of this is Geedge Networks, linked to a research group at the Chinese Academy of Sciences. Geedge sells a suite of tools that go well beyond simple network management: deep packet inspection, real-time tracking of mobile users, granular censorship control, blocking of VPNs and circumvention tools, and other surveillance functions. Based on leaked internal documents (over 100,000 files), Geedge has contracts to install these systems in multiple governments, including Kazakhstan, Ethiopia, Pakistan, Myanmar, and at least one other unidentified country. This example of exporting surveillance technologies is of course not isolated: one might think of the Russian company Protei exporting its surveillance and DPI technologies in Iran, and of the Canadian company Sandvine which was widely used in Belarus, Egypt, Eritreia etc.

The report highlights a critical aspect of the remote-controlled nature of these censorship and surveillance systems. The technologies developed and deployed by Geedge Networks allow for centralized management and remote operation of the Great Firewall-like infrastructure across multiple countries. This means that the governments using these systems do not necessarily need to maintain all the technical expertise in-house; instead, Geedge remotely manages and configures the censorship and surveillance tools, enabling real-time adjustments, updates, and monitoring.

This remote-control capability makes the system highly flexible and scalable, as it can be easily adapted to different political and social

[13] ILouis Petiniaud, “The Human Factor in the Geopolitics of the Internet”, 2023 ”https://labs.ripe.net/author/louis_petiniaud/the-human-factor-in-the-geopolitics-of-the-internet/

contexts without requiring significant on-the-ground technical interventions. Additionally, this approach allows the exporting company to maintain substantial control over the systems, potentially influencing how national internet policies evolve, all while keeping its involvement under the radar. The centralized, remote-control aspect of these systems further entrenches digital authoritarianism, as it enables external entities to influence or even dictate the degree of surveillance and censorship in foreign countries.

Of course, the case of Geedza is not isolated: the most recent example is the Russian company Protei exporting its surveillance and DPI technologies in Iran, as reported by the Citizen Lab in 2023 and by Miaan and Global Voices in 2026. This commodification of information control technologies and tight relations between authoritarian regimes and private companies should be analyzed on the global scale, in the light of underlying processes such as standardisation and circulation of policy models.

From markets to governments and back: circulation of sovereign standards

More in general, countries seek to globalise the technology built by their domestic industry. When such technology affects surveillance and content blocking, the effort made by governments and industry to transform domestic technology into global standards is deeply political. Nevertheless, there are situations in which countries prefer to avoid international standardization and keep national standards. For example, global cellular network standards contain specifications for lawful interception. These are basic specifications to allow interception to take place. However, each country has different rules on lawful interception. While cellular networks within each country are built according to the global standard(s), lawful interception technologies and requirements are then built on top of the globally accepted specifications. While national lawful interception technology standards are usually produced locally through a government-industry collaboration, they are often kept partially untransparent for security reasons. This may explain why the Chinese industry, while strong in cellular networks standardisation globally, does not export its lawful interception standards.

Besides technologies, the models of governance can also become

standardized and largely promoted on the international level. In her presentation, Grace X. Yang suggests to analyze relations between China and Russia precisely as a coordinated campaign to re-architect global internet governance. Both countries pursue the goal of normalization of a state-centric model of the internet in which governments exercise ultimate authority over infrastructure, standards, and cross-border data flows displacing the multi-stakeholder governance paradigm.

Within this framework, Russia destabilizes existing consensus and reframes debates around sovereignty while China fills the institutional vacuum with structured alternatives: draft texts, technical proposals, standards language. The interplay produces gradual normalization of a state-centric governance paradigm. Russia acts as the “Spoiler” - disruptive, confrontational, and politically noisy. China functions as the “Architect” - institutional, technical, and procedural. Russia’s focus is regime security, information control, and destabilization of Western-led governance norms. China’s focus is standards-setting, infrastructural leverage, and long-term institutional embedding of alternative governance models. Together, they operate across two interconnected arenas: the technical front (ITU) and the legal front (UN treaty processes). These spaces allow for both normative contestation and institutional codification.

At the International Telecommunication Union (ITU), China advanced its “New IP” proposal as an alternative internet architecture premised on centralized control, top-down governance, and built-in identity and traceability features. The model contrasts sharply with the decentralized, end-to-end architecture of the current internet. Although formally rejected by the IETF/IEEE technical community, the proposal succeeded in shifting discourse within the ITU. Core principles such
as centralization, stronger routing control, state oversight, remain embedded in ongoing discussions about next-generation standards. Here, China’s strategy was procedural and forward-looking: propose alternative foundations and institutionalize them incrementally. Russia’s role was overt political amplification. It supported the proposal diplomatically and rhetorically, challenging Western dominance and reframing debates around sovereign control. Even failed proposals served to normalize the idea that architectural redesign is legitimate terrain for geopolitical contestation.

A second ITU arena involved Russia’s 2022 bid to capture institutional leadership through a Secretary-General candidacy. The attempt failed, largely due to the geopolitical fallout from the invasion of Ukraine.

Yet China quietly supported the effort, reinforcing the pattern of backstage coordination. Even in defeat, the episode signaled that leadership of technical bodies is itself a strategic objective.

In the UN arena, the campaign shifted from technical standards to binding legal norms. Negotiations over a global cybercrime convention exposed two blocs:

- A Rights Bloc, advocating balance between sovereignty and human rights, narrow criminal definitions, and flexible cross-border cooperation.
- A Sovereignty Bloc, prioritizing absolute state control, broad criminalization (including content-based offenses), and strict state-to-state cooperation mechanisms.

Russia's tactic was procedural overload: submitting numerous aggressive amendments, attempting to criminalize vague categories such as "extremism" or "fake news," and voting to remove explicit human rights safeguards. This "flood the zone" strategy destabilized consensus and expanded the scope of what could be debated.

China's approach was structurally different. Rather than overt confrontation, it framed the architecture of the treaty: emphasizing capacity building, technical assistance for the Global South, and state-managed cooperation channels (e.g., MLAT-based processes). On key human rights provisions, China abstained rather than voting to remove protections, maintaining plausible moderation while enabling sovereignty-oriented outcomes.

The final treaty text reflects significant victories for the Sovereignty Bloc: expansive cooperation frameworks, strong state control over cross-border data access, and a model of international cooperation rooted in governmental mediation. Through this process, cyber sovereignty moved from political rhetoric into treaty language.

Yang argues that this dynamic is actively constructing the splinternet where fragmentation is not merely technical (e.g., routing or infrastructure divergence) but normative: divergent conceptions of who governs, who accesses data, and what constitutes legitimate control. Importantly, the "Spoiler + Architect" model is presented as portable. Internet governance is a proving ground and AI governance can likely become the next arena. One can expect Russia to disrupt Western ethical frameworks and China to institutionalize alternative standards emphasizing state-centric AI oversight and data governance. The Sino-Russian alignment does not operate as a symmetrical alliance but as a strategic complementarity. Through coordinated action

in technical and legal arenas, cyber sovereignty is moving from ideological aspiration to embedded institutional reality. The result is not immediate bifurcation, but incremental re-architecting, where standards, treaties, and institutional leadership collectively reshape the governance logic of the global internet.

Towards bordered markets

From a fragmentation viewpoint, these dynamics create a problem of trust. As industries such as China's are powerful in infrastructure standardisation and are known to export surveillance technology, the lack of transparency and their non-participation in standardising surveillance requirements in communication infrastructure can be construed as an attempt at preserving secrecy in surveillance infrastructure. Nonetheless, it is worth mentioning that their early attempts at creating a separate DNS have been progressively replaced by growing acceptance of the existing system and its governance mechanisms.

At the same time, as mistrust thrives in this environment, governments push towards the exclusion of selected foreign actors from their domestic infrastructure and service markets. While this does not necessarily yield breaks in the interoperability of communication infrastructures, it can yield 'bordered' markets where governments exercise stronger control on operators and service providers, including stronger control on online contents and communications.

Chapter 2

Breaking isolation, limiting autonomy? U.S. technology companies and the war in Ukraine.

By Julien Nocetti

an associate researcher at the Geopolitical Center for Technology and at the Russia/ Eurasia Center of the French Institute of International Relations (Ifri).
He is currently an advisor for digital, cyber and technology affairs at the Centre for Analysis, Forecasting and Strategy (CAPS) of the Ministry of Europe and Foreign Affairs.
He is also an associate member of the GEODE Center (Geopolitics of the Datasphere – University of Paris 8) and teaches technology diplomacy at the School of International Affairs of Sciences Po (PSIA). He was a professor-researcher in international relations and strategic studies at the Military Academy of Saint-Cyr Coëtquidan (2019-2023) and a researcher at the Russia/NIS Center of Ifri between 2009 and 2019. He holds a PhD in Political Science from the National Institute of Oriental Languages and Civilizations (INALCO).

In Ukraine, tech companies have played an outsized role, encroaching into traditional areas of statecraft. It is clear that no state could have provided Ukraine with the kind of services it needed – cloud storage, threat intelligence, satellite communications and the use of artificial intelligence for battlefield targeting – at the speed at which they were required.

Companies like Microsoft, Amazon, Starlink, Palantir, Maxar, Cisco etc., have plainly demonstrated their capabilities and infrastructural power. But rather than simply describing their actual involvement into Kyiv's war effort, the conference has sought to explain how state-private interactions have worked so far in the Ukrainian war, along three main features which carry a strong infrastructural dimension.

First of all, U.S. tech firms envisioned the provision of cloud storage services as a "sovereignty-as-a-service" matter. On the day of the invasion, Amazon and the Ukrainian government sketched out a plan to transfer critical data from Ukrainian ministries and essential companies to the cloud. The transfer was an intricate process relying on Amazon's existing logistical chains in Europe for their AWS Snowballs. By July 2022, more than 10 million gigabytes of data had been relocated from servers located in Ukrainian to Amazon's cloud, including data from 42 government authorities, 24 universities, and dozens of companies.

Amazon and Microsoft iterate that the existence of cloud infrastructure enables governments at the brink of war to ensure the continuing operation of their vital digital networks. It highlights the role of cloud infrastructure in generating co-production of sovereignty and security governance at the intersection between public and private, disrupting ideas of territorialized state control over cyberspace.

In war, these infrastructural mediations of public-private boundary drawing, sovereignty, and security governance have implications for all the states involved. The distribution of the cloud infrastructures enables data essential for military operations to be stored and processed in other states. In that sense, Amazon data centres in Germany, Switzerland, or Ireland hold data that enable Ukraine's war machine.

Secondly, the war in Ukraine demonstrated how connectivity mixed both responsabilization and contracting from U.S. tech firms. The use of Amazon cloud services relies on Amazon's continuing sense of obligation for Ukraine's war of independence. Not every Big Tech company shares the same sense of responsibility for Ukraine with Elon Musk and SpaceX being the most evident example. A few days into the war amid widespread Internet blackouts, Vice PM Fyodorov approached

Amazon conducts a disaster response training exercise using Snowball Edge data storage units. Similar units have been used to transfer Ukraine government data to the Amazon cloud. (Noah Berger / Amazon)

Amazon used small storage data units ("Snowball") to help the Ukranian government physically transport millions of GB of critical government data out of Ukraine and into it's cloud infrastructure.

Elon Musk on Twitter pleading for Starlink satellite services to ensure stable communication flows for civilians and the government. Twelve hours later, Musk replied saying that he had activated services in Ukraine, and within a few days the first of over 30.000 terminals were being shipped to Ukraine to enhance connectivity. The Ukrainian military utilized the then 4,500 satellites in orbit on the battlefield, not only for command and control but also more specifically to direct its reconnaissance and combat drones. In October 2022, Musk demanded financial compensation from the Pentagon – a request which was withdrawn after receiving public criticism. Though later, Musk refused to provide Starlink access to the Ukrainian military as they were targeting Russia's naval fleet. Musk told his biographer that he wanted to prevent a 'mini–Pearl Harbor' on Crimea that would lead to Russian nuclear escalation. In June 2023, Pentagon signed a contract with SpaceX to ensure Starlink satellite service for Ukraine, and there was no reporting about lack of coverage for the Ukrainian military until Donald Trump re-entered the White House.

The satellite infrastructure that secures stable communication flows to the battlefield mediates a particular form of public-private relation: on the one hand, it reaffirms well-known contractual dynamics between governments and private defence companies. And on the other, it recreates the non-contractual logic of responsibilization where security is considered a duty rather than a right. The infrastructurally mediated responsibilization, however, comes with a new twist in that it leaves room for erratic CEOs to make strategic decisions directly influencing a state's ongoing military operations based only on the CEOs geopolitical judgement and thus without consultation or alignment with the government it is contractually tied to.

Thirdly, providing massive cyber threat intelligence (CTI) to Ukraine, tech firms acted as knowledge brokers on the conflict itself. The extensive use of Microsoft's products and services in Ukraine positions the company to constantly monitor the ongoing activities in the country's networks, and ultimately identify specific cyber threat patterns from Russian cyber and information warfare units. The access to threat data have turned Microsoft into a gatekeeper of knowledge about the war.

Microsoft's extensive involvement in defending Ukraine from Russian cyber-attacks enables the company to position itself as the truth teller of the cyberwar. In war, knowledge about what is happening and what it means are inherently sparse and contested. Intelligence agencies often have to balance the strategic utility of knowledge sharing with the potential loss of continuing information gathering capacity. The company has published several well-designed reports on what they see of Russian cyber activity against Ukraine. The reports function as a practice of epistemic infrastructuring by analysing, presenting, and validating the large and rather eclectic landscape of bottom-up knowledge production on cybersecurity incidents in Ukraine based on open-source data.

In this way, Microsoft tells both Ukraine and the world how to understand, learn about, and adapt to protect their potentially critical digital assets. These two ways in which the boundary between Microsoft and the state is being drawn have political implications, especially in relation to the dependencies of Microsoft, also outside the borders of Ukraine. By collecting and analysing threat data against Ukraine, Microsoft is not only helping a country at war protecting itself in cyberspace. The constitution of the epistemic infrastructure enables Microsoft to also help all its global customers. Microsoft may aid Ukraine for free, but by being both a global software and a cybersecurity provider, Microsoft improves both services by collecting, analysing, and mitigating cyber threat data in Ukraine. This only strengthens Microsoft's ability to extract rent from users of its software and additional rent from the same users for protecting the insecure software these users are renting in the first place.

This multifaceted involvement has multiple consequences for Ukraine (and Europe), including for the country's digital corporate autonomy. The most obvious one is Ukraine's dependency on private sector goodwill for national security provision. Another ramification is from an international legal standpoint. Because the companies are demonstrably taking sides in the war, if their engagement

in defensive activities is interpreted as involvement in hostilities, then they could be seen by Russia as participants in the conflict and therefore legitimate military targets. This issue is intensified by the fact that the companies are understood to be helping manage not only civilian services but also military assets, for example, the protection of military networks and storage of military data in the cloud. Ukraine ceded a substantial level of control over its critical data to American companies with servers located extraterritorially, under a legal regime different to its own. Ukraine thus effectively traded a proportion of its digital sovereignty for cyber resilience. These actions also have sovereignty implications for countries hosting the servers(e.g. Poland), as they become potential Russian targets.

Chapter 3

The Red Web on export: Kremlin's internet sovereignty in Russia and abroad

By Andrei Soldatov,

an investigative journalist and Co-Founder of Agentura.ru, a watchdog of the Russian secret services' activities. He is also a Nonresident Senior Fellow at the Center for European Policy Analysis. He is a co-author, with Irina Borogan, of The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB and The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad.

We all know how aggressive the Russian offensive against internet freedoms has become in recent years. A week before SplinterCon Paris took place, FaceTime and Snapchat were blocked at once. The country is decisively moving toward a "whitelist reality" — meaning, in a very Soviet, totalitarian fashion, that citizens may use only those services explicitly approved by the government, while everything else is restricted or banned.

It's not my role to assess the effectiveness of these measures. What I will try to do is to talk about Russia's ambitions to export the Kremlin's model of internet control to other continents. Some of you remember how many years Russian diplomats spent attempting to impose the Russian-Chinese vision of "digital sovereignty" on the international community through organizations like the UN. Those efforts were only partially successful — for instance, one example is the evolution of language around "cyber" and "information" security. But in this short article I want to focus on a more recent development that began in the spring of 2024.

In late April 2024, Nikolai Patrushev, then still head of Russia's Security Council (but we all know him as a former head of the FSB and a close friend of Putin), chaired a conference in St. Petersburg of top security officials from Africa, Asia, Latin America, and the Middle East. The main topic of that conference was information sovereignty and security. Instead of just preaching the Russian vision of internet control, Patrushev did something else – he made a pitch to the participants. He presented a list of Russia's top cybersecurity companies that could help their governments gain control of their information spaces

Patrushev listed seven companies, including Positive Technologies, sanctioned by the US for helping Russian spy agencies recruit new talent; Cyberus – this company was launched by former employees of Positive Technologies and closely affiliated with Positive; Kaspersky Lab; Solar, the national telecom operator Rostelecom's security branch.

As I said, the audience consisted of top level security services officials from those countries. And those security mandarins were left under no illusion that any Russian offer would come with a backdoor for Russian intelligence: when Patrushev delivered his opening speech,

[15] U.S. Department of the Treasury, “Treasury Sanctions Russia with Sweeping New Sanctions Authority,” 2021. https://home.treasury.gov/news/press-releases/jy0127

Sergey Naryshkin, the head of the Russian Foreign Intelligence Service, the SVR, was seated at his right hand. And yet, as we see now, Patrushev's pitch was remarkably successful.

Since that meeting in St. Petersburg in April 2024, most of the companies listed by Patrushev made significant achievements overseas. Let's take, for instance, Positive Technologies, an undisputed leader on the Russian cyber security market.

Positive Technologies got a distribution agreement with Mideast Communication Systems in Cairo, gaining a strategic launch pad for its services in Africa and the Middle East—particularly in Egypt and Saudi Arabia. Positive Technologies has been attractive to Riyadh because the company provides protection against so-called advanced persistent threat attacks— and the company helped the Saudis identify the groups targeting telecommunications and military industries in Saudi Arabia.

In Qatar, Cyberus Foundation, an affiliate of Positive technologies -- signed a strategic agreement with Al-Adid Business, owned by a member of the ruling family of Qatar. The deal is to develop Qatar's cybersecurity capabilities, including by establishing Cyberdom Qatar and Hackademy, institutions for training cyber experts in the country. In Central Asia, Cyberus also secured a partnership with the Collective Security Treaty Organization.

It is in Africa, where Russia's cyber-expansion has been particularly active. Kaspersky Lab, for example, has signed an agreement with Smart Africa, a partnership among 40 African countries. Kaspersky is also involved in the African Network of Cybersecurity Authorities, an initiative established in February 2025 to "tackle cross-border cybersecurity challenges across the Continent."

Meanwhile, the Kremlin has continued to promote the companies on Patrushev's list.

For instance, this June, the St. Petersburg International Economic Forum —the annual Kremlin-backed conference — had Yury Maksimov, the co-founder of Positive Technologies and Cyberus, as one of its key speakers. And Maksimov spoke, predictably, of the need for digital sovereignty for the countries that "don't have complete technological independence."

Some might argue that the expansion of these Russian companies into Africa and the Middle East has nothing to do with the Kremlin or Russian intelligence. After all, they lost any chance of securing contracts

in Europe following 2022 — so where else are they supposed to go? I would argue, however, that what we are seeing is an effort closely coordinated with the Kremlin, and with Russian intelligence in particular.

At the St. Petersburg Forum, Cyberus's pitch was echoed and reinforced by Andrey Bezrukov. Bezrukov is one of the ten Russian "illegals" from the SVR — Russia's foreign intelligence agency — who were arrested in the United States in 2010 and later swapped. He belonged to the same group as Anna Chapman, the red-haired Russian spy and socialite. After the swap, Bezrukov reinvented himself as a foreign policy expert and was given a well-paid position at Rosneft, Russia's state oil company.

But what makes Bezrukov relevant to our discussion today is his latest role: he now chairs the Russian Association for the Export of Technological Sovereignty. And let me remind you that this entire development began with Patrushev's pitch — delivered while he was flanked by Sergei Naryshkin, the head of the SVR.

So what makes Russia's pitch to Africa and the Middle East so appealing? Unlike China, where censorship was built into the system from the very beginning, Russia introduced large-scale online censorship only in 2012. This created a challenge: the country's digital infrastructure had already been built on Western technologies, without government interference. But that is precisely why the Russian model is appealing to other countries whose communications infrastructure is built on Western technologies: Russia provides an example that a censorship and control layer can be added to an already established, Western-built internet infrastructure. And during Putin's last visit to India in late November 2025, Bezrukov led an effort to promote Russian "digital sovereignty" to Indian IT entrepreneurs.

Section 2

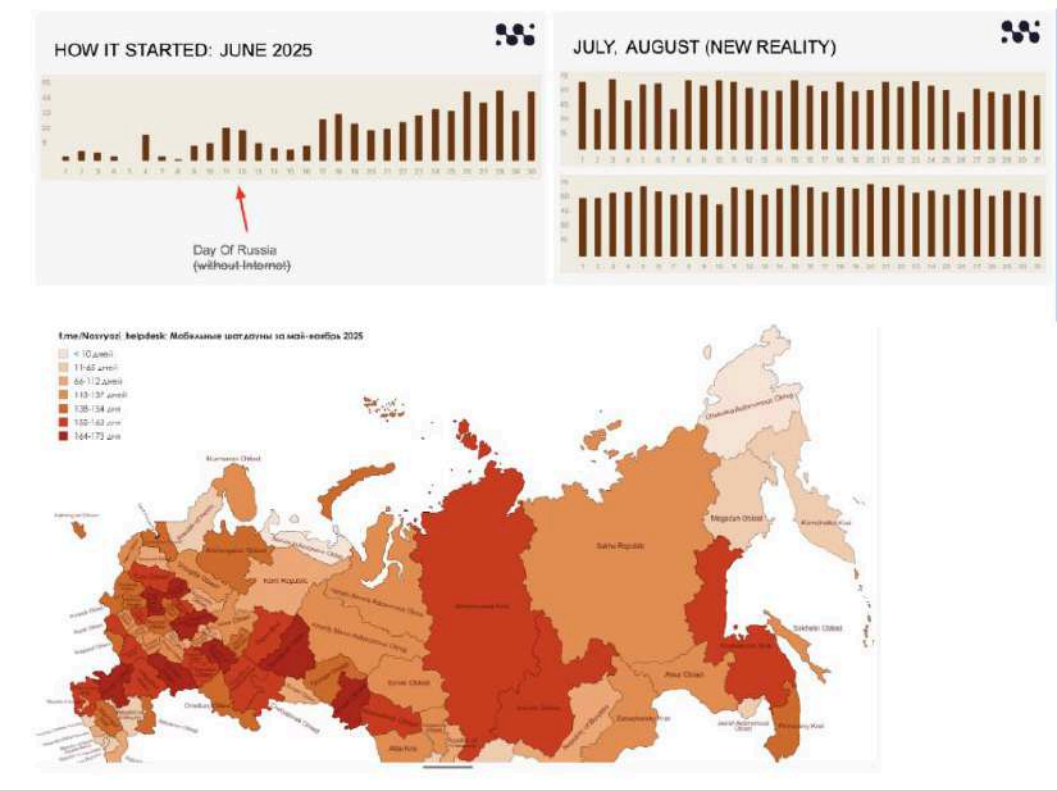
Measuring sovereignty: approaches and challenges

Chapter 1

Perceiving Russian splinternet: 2025 trends through community sourced data

Digital Helpline NaSvyazi has been collecting testimonies of shutdowns since 2024 as part of their project Ru Net Monitor. At SplinterCon Paris they presented the 2025 Runet Restrictions Review, the first report which focuses specifically on shutdowns in Russia which highlights the growing fragmentation of the RuNet. We wouldn't exaggerate if we call 2025 the Year of Shutdowns of Runet.

Indeed, the data from Runet Monitor for 2025 shows 12026 documented shutdowns just in one year, with major regions like Nizhny Novgorod and Moscow experiencing repeated disruptions.
By mid-2025, mobile internet shutdowns became a normalized part of the government's response to perceived threats. Restrictions are increasing over time, and particularly intensify around holidays like Victory Day and Russia Day.



Map of mobile connectivity shutdowns May-November 2025; source: RuNet Monitor

The data on the RuNet Monitor is mainly composed from first-hand accounts of Russian citizens who report shutdowns using either the form on the website or the Telegram bot. Of course, this data has yet to be correlated with network monitoring from sources such as IODA, OONI or Kentik. However, Na Svyazi verifies each report before counting it as a valid one. This methodology has its limitations, for instance, the regions with the least amount of shutdowns are also the most remote and with lower digital literacy levels, which could

explain lower rate of reports coming from those areas. However, the volume of aggregated reports is impressive and definitely shows trends in technologies and methods of Runet control.

Another part of this strategy, similar to Iran, is the whitelist approach. Indeed, whitelists are actively spreading to specific regions, where the "antimessenger mode" is introduced, either in response to hypothetical drone attacks or to local unrest. Under a whitelist, people can only get access to a defined set of digital services. The whitelist varies slightly by region. Currently, this list counts around 70 resources, including specific banking services, mobile internet providers, social networks (Vk.com, Ok.ru), mail services (mail.ru, yandex.ru), governmental websites and administrative services, mapping services, marketplaces.

However, vital services such as the mobile app from the Ministry of Emergency Situtations which alerts about air raids, are not included in the whitelist. On July 1, 2025 in the city of Izhevsk 35 people were injured and 3 people died in a drone attack on the electromechanical factory “Kupol”. None of them has received alerts about the air raid. Besides, other vital services such as continuous glucose monitoring (CGM) sensors, stop working under the whitelists. CGM sensors alert patients to high or low blood sugar levels, helping to prevent hypoglycemia—a critical drop in blood glucose that can lead to coma or even death. Parents of children with diabetes use the system to remotely monitor their child's blood glucose levels while they are at nursery or school. During internet shutdowns, such medical applications become unavailable,

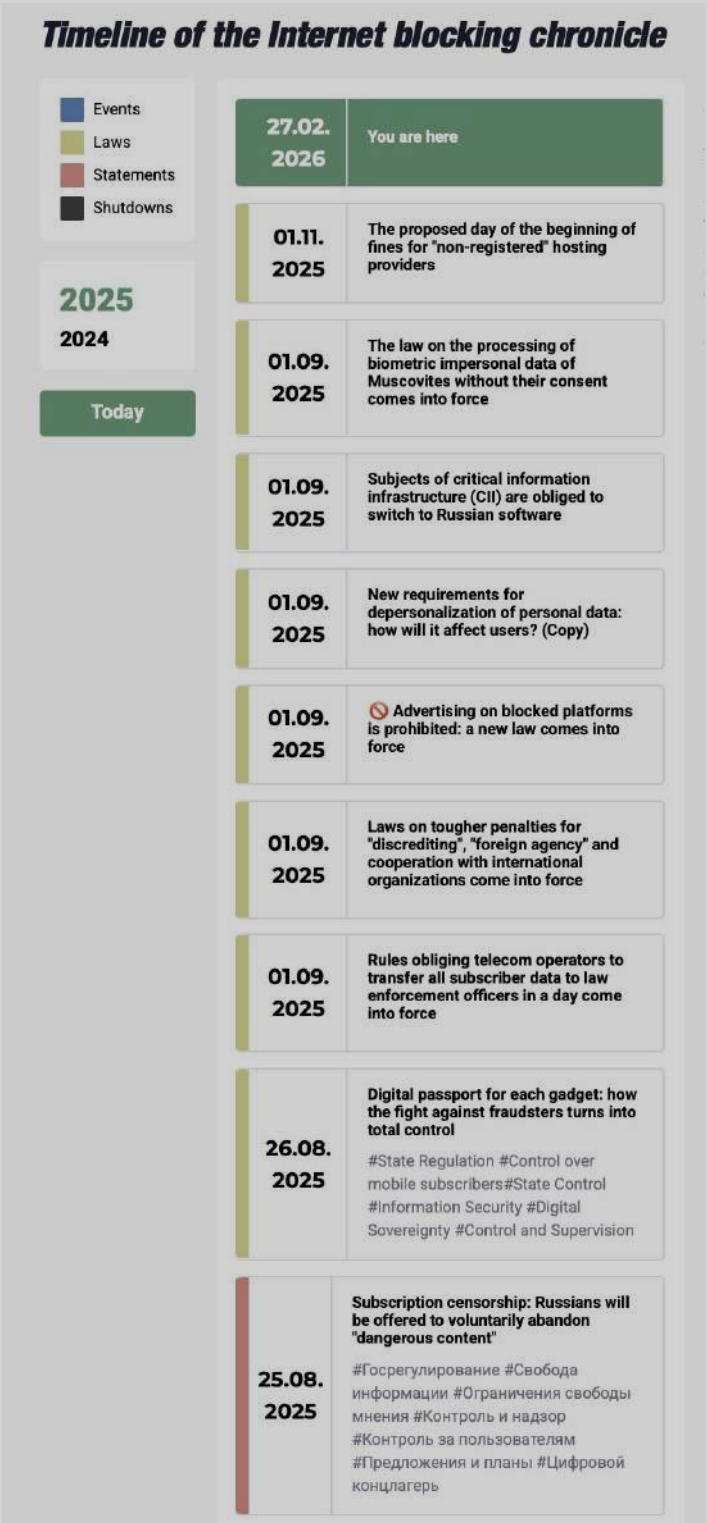
If parents do not find out about their child's drop in blood glucose levels in time, they cannot take measures to regulate their sugar levels.

The justifications for blocking services such as “protecting citizens”, “preventing drone attacks”, and “maintaining safety” — serve to normalize the loss of internet freedom. These actions lead to a societal shift where people, under continuous restrictions, grow more insecure and more inclined toward authoritarian governance as a perceived stabilizing force. Over 1.2 million websites, 258 VPN services, and 252 anonymous email services were blocked in 2025. Popular messengers like Telegram and WhatsApp have also faced consistent blocking efforts.

The review offers insights into how Russian citizens and tech-savvy users adapt by using sophisticated tools to bypass blocks. Circumvention tools like OpenVPN and WireGuard face high levels of blocking, but more resilient methods, such as V2Ray and TOR, show growing popularity for evading government monitoring.

he narrative of escalating restrictions, with increasingly pervasive censorship, exemplifies a deeper fragmentation within the internet, as Russia's digital infrastructure isolates itself further from the global network. The presentation underscores the challenges ahead for those resisting censorship and for those trying to maintain some level of unrestricted internet access.

These developments point to a larger trend of internet fragmentation, where state actors use legislative and technological methods to control digital access, undermining global connectivity and freedom.



Screenshot from Runet Timeline

Chapter 2

Measuring sovereignty from the outside: the Digital Sovereignty Index

By Jos Poortvliet

the co-founder and Communications Director at Nextcloud, the open-source file sharing and collaboration platform. An advocate for digital rights and open-source software, he has worked at the intersection of technology and policy, advising governments and telecom companies in the Netherlands on questions of digital sovereignty. He describes himself as an "all-things-open evangelist."

By Ksenia Ermoshina

a senior researcher at the Center for Internet and Society of the CNRS, eQualitie and The Citizen Lab of the University of Toronto. She is also conducting user-research, community work, and field testing for decentralized free software projects such as Delta Chat, Ceno browser, and Ouisync. Ksenia holds a PhD in socio-economy of innovation from Mines Paris Tech.

Sovereignty is a spectrum: from the European Union that is urgently building its techno-political autonomy to the authoritarian states that are steadily growing their national intranets capabilities. How can we better distinguish and define the different flavors of sovereignty? One option that seems to become popular is to measure them and develop special Indexes.

As we know, indexes are not mere rankings. They serve “as a strategic tool for producing authoritative expertise – or at least the public appearance of expertise” (Broome & Quirk, 2015). Indexes are “performative”, they have a strong impact on the funding and regulation of technological solutions, and on the fundamental policy decision. Among the most well-known Internet freedom rankings we can quote the Freedom of the Net index by Freedom house, Enemies of the Internet by Reporters Without Borders and Corporate Accountability Index by Ranking Digital Rights. Country-specific indexes also exist (see The Index of Freedom of RuNet by the Society of Internet Protection, or Project Ainita for measuring connectivity in Iran). The network measurement community is also producing its own metrics that can be used to evaluate specific parameters of digital sovereignty and Internet fragmentation, such as connectivity and routing (RIPE Atlas or Cloudflare Radar), shutdowns (IODA project by CAIDA) or censorship (OONI).

We have interviewed the author of the new Index that tries to measure digital autonomy in a positive way: Jos Poortvliet, the author of The Digital Sovereignty Index. Digital Sovereignty Index is a project driven by a team of enthusiasts inside Nextcloud who decided to offer an alternative approach to defining Internet sovereignty. The idea behind is to shift from policy level to physical level in order to measure actual infrastructure that is running locally, and not in a foreign cloud. The DSI is a metric that illustrates how much self hosted applications are actively used across nearly 60 countries. It represents the relative amount of deployments of self-hosted productivity and collaboration tools per 100,000 citizens, compared to other countries. DSI analyzes the deployment of 50 of the most relevant self-hosted tools for digital collaboration and communication. These include platforms for file sharing, video conferencing, groupware, notes, project management, and more. The results of the first Digital Sovereignty Index show significant differences in the adoption of self-hosted infrastructure across Europe and beyond. While the public debate around digital

[16] Add citation: Broome, A. and Quirk, J., [article title], [journal name], 2015. [URL]

sovereignty has gained momentum in recent years, actual usage of sovereign digital tools remains fragmented – and in many places surprisingly low.

The lead of the Digital Sovereignty Index, Jos Poortvliet, is co-founder and Communications Director at Nextcloud and an “all-things-open evangelist”, as he self-defines. Previously, Jos was working on the intersection of policies and technology as a consultant for the government and telecom companies of the Netherlands. His concerns with technological sovereignty of Europe have drastically risen in the light of the recent institutional crisis in the US. A minute after we start our conversation, he’s already sharing a link to a recent article that describes the US Federal Trade Commission’s decision that Apple, Google, Meta and other American Big Tech players do not necessarily have to comply with the EU platform regulation Digital Services Act.

Nextcloud has published an opinion piece on this subject, criticizing the Microsoft “European Digital Sovereignty” campaign and the promises of the Big Tech to preserve European tech autonomy and data privacy of the EU citizens. However, the idea of

Digital Sovereignty Index wasn’t born in the heat of political debates. The story behind the Index is unexpectedly nerdy, as Jos explains:

JP: *So, shortly after we started Nextcloud, almost 10 years ago, we discovered a security issue in our product. When we fixed it, I told our head of security at the time, you know, we should tell people to update, and he confessed that a lot of people just don't update their server deployments. I asked if he could provide concrete numbers on that, so we looked around and found a way to use a network scanning tool called Shodan. He wrote a script that checks on each of those nextcloud or owncloud servers the version they were running, and counts how many insecure versions were out there. That was in the past, many years ago, and then we decided to take that to a next level, to look not only at the nextcloud, but also at other solutions, just to get an idea of where people use these self hosted technologies more. Many interesting things came out of it. I had not expected Finland to be number one and the differences between to be so big, that really surprised me.*

[17] Niklas Lewanczik, „America First“ im Netz: Warum Big Tech jetzt EU-Gesetze missachten soll, " Publication", 2025 https://t3n.de/news/warum-big-tech-jetzt-eu-gesetze-missachten-sollen-1705040/

[18] Jos Poortvliet, “Big Tech's "Sovereign Cloud" promises just collapsed - in their own words,” Publication, 2025 https://nextcloud.com/blog/big-techs-sovereign-cloud-promises-just-collapsed-in-their-own-words/

KE: Using Shodan to measure sovereignty is of course an unexpected approach, but aren't there limitations? Many authoritarian countries like Russia for example may have less publicly visible servers, while still running free software solutions.

JP: Of course, there are many limitations. For example, about a third of the Nextcloud instances don't show up in this scan. I know roughly the real number of Nextcloud servers out there because our updater has statistics. It's not 100% precise, but it covers the vast majority. That number is more like 400k, but we could only see 130k coming out of the scan. We already know, there are firewalls, governments or people who are blocking Shodan. That's why we decided to make it a relative rating. And the other thing we did is that we decided to normalize the numbers between different products and didn't distinguish between large servers with tens of thousands of users and smaller ones with a thousand or a hundred. That's also why we don't draw a lot of conclusions on the website and in the report. We give the numbers, but we don't really say a lot about what they mean.

KE: Have you thought about cross-Index collaboration? Looking at what other Indexes do and may be working together?

JP: We did a bit of research in other indexes and a lot of them, of course, take a qualitative approach. They do surveys, which is also really interesting. We also got feedback from a couple of academics before we published our Index. We wanted to compensate a bit for the limitations of the DSI and look at other parameters. For example, if a country just doesn't have a lot of its own servers, it would score low in our Index. But maybe they use zero foreign software, and in this way they could score high in another Index. We could also take into account a digitalization index, or look for an indication of how much of the Microsoft, Amazon or Google servers are used in a country but you cannot do a count on Big Tech because they're just running a bunch of IP addresses. So there's no relation between IP addresses and how many users they have or anything.. But the Index we did is extremely simple. It's just a plain count without any kind of complications and it's very objective. If you start to add in other sub-indexes, how much would you weigh them? That's a choice. And it becomes a political choice, not objective anymore. How would you calculate? What weight would you give to it? We're a vendor and we obviously have our own ideas and opinions so it won't be credible anymore if we start to put our opinion in the Index.

KE: In the DSI France is only at fourth place, however, the French government relies on a decentralized self-hosted messaging suite which is called Tchap, it's a fork of Element based on Matrix protocol. How would you explain the fourth place here?

JP: Well, two things. One, a single government instance with 100,000 users counts as one, just like a single private user instance with two users. We just count IP addresses that run the service. We know that in Germany the government has been very slow to digitalize, so most German governments are still running on-premise software. They're not in the cloud. While in the Netherlands, the whole government is on Microsoft 365. If Microsoft shuts down 365, does the government stop functioning? The Dutch recently figured this out and are now starting to do something about it. The Germans, they're just behind, which is now an advantage because now they can actually do a smart move towards self-hosting and never get onto Big Tech. But you don't see any of that in the numbers in our Index.

KE: What about peer-to-peer technologies? Aren't they also a factor of digital sovereignty? They are designed to be run collectively, by a community of users, and often are local-first. Why haven't you included them in the Index?

JP: With peer-to-peer it's not so much about hosting your data yourself, but it's more about anonymity or circumvention, or sharing without being seen. I didn't look at something like Bit Torrent or Tor because I think for the digital sovereignty of Europe it is important where the data is, which is actually the opposite of distributed architectures or traffic anonymity. I think control is actually important for sovereignty. For instance, Nextcloud is not built around end-to-end encryption because we designed it with the idea that you trust the server. That's also why Nextcloud is big in business and in governments. As a government, you have laws around transparency

and accountability. As an administrator or a compliance officer you don't want the civil servants to use encryption. That would be simply illegal. Which, by the way, I find very interesting about the government using Matrix. Privacy is important for people, users should have privacy. Companies and governments should not have privacy. They should be transparent and accountable.

KE: Do you think the Digital Sovereignty Index also tells something about shutdown or censorship resilience? If a country scores high, would it mean that it is better connected?

JP: If there are a lot of people who are running collaborative services locally, and if a crisis happens, say, for example, the US companies stop offering service, then there are a lot of people in Germany or in the Netherlands who know how to run a server and who can provide services locally and that means resilience.

1.	Finland	64.50	20.	Australia	10.20	39.	Portugal	4.33
2.	Germany	53.85	21.	U. Kingdom	9.21	40.	New Zealand	4.23
3.	Netherlands	36.32	22.	Taiwan	8.49	41.	Israel	3.71
4.	France	25.10	23.	Romania	7.66	42.	Malta	3.38
5.	Switzerland	23.32	24.	Poland	7.55	43.	Ukraine	2.83
6.	Iceland	22.58	25.	Croatia	7.25	44.	Argentina	2.57
7.	Ireland	22.03	26.	Belgium	7.15	45.	Brazil	2.44
8.	Austria	20.23	27.	Spain	7.01	46.	Turkey	2.26
9.	Estonia	18.40	28.	Russia	6.95	47.	South Africa	1.79
10.	Luxembourg	17.72	29.	Denmark	6.50	48.	Indonesia	1.07
11.	Latvia	16.63	30.	Italy	6.49	49.	Morocco	0.94
12.	Lithuania	16.10	31.	Norway	6.35	50.	Saudi Arabia	0.87
13.	Canada	14.94	32.	Slovakia	5.88	51.	Mexico	0.57
14.	United States	14.88	33.	Qatar	5.71	52.	Tunisia	0.55
15.	Sweden	14.27	34.	Serbia	5.44	53.	Jamaica	0.51
16.	Hungary	13.38	35.	Cyprus	5.25	54.	India	0.43
17.	Slovenia	13.33	36.	Japan	5.17	55.	Greenland	0.36
18.	Czechia	13.10	37.	South Korea	5.05	56.	Egypt	0.12
19.	Bulgaria	12.93	38.	Greece	4.81	57.	Nigeria	0.03

Table: Digital Sovereignty Index scores across countries

KE: When you compare countries, you see, for example, that Russia is red, which is interesting because what Russia tries to do is exactly to build a sovereign internet.

JP: It is entirely possible that the Russian government and big Russian tech companies are all running self-hosted services that we just might not see. While in the Netherlands, a lot of people are running their own servers, which gives the Netherlands a higher number than Russia, even though the Dutch government is dependent on Microsoft 365.
And maybe we're not checking software that is very popular in Russia,

for example, we don't yet have Delta Chat or XMPP which seems t
o be popular out there.

KE: So this Russian case is pointing at a controversy with the term “sovereignty”: how would you define it?

JP: We're talking a lot about European sovereignty and we keep saying to each other that we don't want to agree with the nationalists here. Open source is a global movement, and we are pro-open borders and open standards, we have employees from all over the world. I would say it's more against big tech. Okay. It just shouldn't be that five companies own all the data on the planet Earth. That's crazy, that's a risk for humanity. You know what I mean? It's about sovereignty for humanity.

KE: So, if governments use your index for consultancy, for decision making, how would you hope it will shape their policy choices?

JP: I am Dutch, so it was interesting for me to see that the Netherlands is number three, while a ton of studies have been coming out over the last year showing that the Dutch government is completely dependent on Big Tech. And I thought, there is knowledge, skills and also interest in the Netherlands from the Dutch people in being digitally sovereign. And yet the government doesn't seem to be aligned with that. So when you're not using your people’s skills and interest, that means instead you're giving money and creating jobs in California. Countries that have less servers, for example, Spain should first look to develop locally the skills and the economic knowledge, while countries that strike high, such as Netherlands, France or Germany, should align better with the social demand for self-hosting.

Section 3

Splinternet as a “lived experience”: a user’s sovereignty inside authoritarian networks

By Ksenia Ermoshina

a senior researcher at the Center for Internet and Society of the CNRS, eQualitie and The Citizen Lab of the University of Toronto. She is also conducting user-research, community work, and field testing for decentralized free software projects such as Delta Chat, Ceno browser, and Ouisync. Ksenia holds a PhD in socio-economy of innovation from Mines Paris Tech.

We often speak of splinternet from a geopolitical perspective or internet governance point of view. But here is the thing: people already live and work inside splinternets for many hours, days or months. We do not live on the same Internet even if we live in the same country. In a splintered network, the online content appears as different for different groups and can depend on class, gender or ethnic specificities. Approaching the concept of splinternet from an angle of lived experience offers a different lens to measuring the impact of digital fragmentation. Censoring marginal groups leads to building isolated informational bubbles, introducing dramatic inequalities in the experience of Internet usage. This fragmentation of online experiences is further exacerbated by introducing tiered Internet, as it happened in Iran in January 2026, where elites could access the global web while the majority of the population was locked inside the NIN.

Shutdowns and splinternet are real world experiences that affect how we feel, physically and mentally, how we talk to our family and friends, how we do our jobs and perceive events around us. Some of the unexpected consequences of splinternet include direct harm to health. For instance in Russia the app to track insulin level in school kids stopped working when the government introduced mobile shutdowns and whitelists. Parents lost track of their children's health data which led to emergency situations endangering the lives of these children. Other effects of mobile shutdowns include people getting killed by drones because the drone alerts hadn't been delivered due to mobile shutdowns. It therefore becomes urgent to understand splinternet and individual digital sovereignty at this material, personal and bodily level.

At SplinterCon Paris we heard several first-hand accounts of living under tiered censorship and digital fragmentation: from the soviet censorship of journals and books to the contemporary cases of Ukraine or Venezuela. Besides, a dedicated panel on the topics of gender and sexuality as a factor of informational isolation covered the experiences of women and LGBTQI people and their specific experiences of “algorithmic invisibility”, as Hannes-Jeremia Jaaks has pointed out in his presentation. These accounts demonstrate that marginalised users appear to exist inside even more isolated online environments, where information is filtered even more intensely than for the majority of the population inhabiting the same territory. Our extended study of the effects of cyber occupation of Crimea including data from OONI explorer about blocking of websites in Crimea shows how Crimean tatar (the indigenous people of Crimea) were exposed to a much stricter censorship than other Crimeans. LGBTQI groups living in countries with homophobic laws are also subject to double censorship,

and many of them opt in for digital migration to more secure alternatives. The testimony from Delo LGBT presented at SplinterCon demonstrates the need for Russian queer groups to migrate to the federated social media platforms and decentralized messaging solutions, to be able to continue publishing information about their activities and other LGBT related news. In sum, the authoritarian shift for centralized control of the Internet is experienced in a different way by those who have less privilege.

Venezuela : A Laboratory of Repression and Resistance

The presentation "Venezuela: A Laboratory of Repression and Resistance" by Laura Vidal provided a detailed exploration of how digital authoritarianism is experienced in Venezuela. In Venezuela, information control is not confined to a single tool but emerges from a complex web of interconnected systems. This includes both visible and invisible controls, such as infrastructure disruption, bureaucratic barriers, and state propaganda, which collectively shape the digital and physical reality of Venezuelans. Political actors, journalists, and activists face an intense version of surveillance and harassment, which has become more pervasive over time.

The government has also used legal and administrative tools to undermine the public sphere long before digital repression took hold. Over 400 media outlets have been closed since 2009, creating information deserts across the country by 2024. Laws such as the “Anti-Hate” Law (2017) and the “Anti-NGO” Law (2024) have been selectively used to criminalize opposition and further suppress free expression. These legal frameworks laid the groundwork for the rise of digital repression, as they provided the legal cover for online censorship and surveillance.

Venezuela’s fragile infrastructure is paired with a massive surveillance regime, highlighted by the 2021 Telefónica/Movistar transparency report. This report revealed that 20% of phone lines were monitored, with over 860,000 interception requests and nearly 1 million metadata requests—all done with no judicial oversight. This massive interception regime continues to shape the state’s ability to maintain control over its citizens.

The Venezuelan government has also tied identity to political loyalty through the Carnet de la Patria, a national identity card that links data

collection to access essential services. This system, which encourages citizens to demonstrate political loyalty in exchange for services, makes it easier for the state to control behavior and punish political dissent. It represents a powerful tool of social control, where citizens are made dependent on the state for basic welfare.

The 2024 election crisis in Venezuela led to both physical and digital repression. The aftermath of contested election results saw 915 protests, 21 deaths, and over 2,400 detentions. To suppress transparency, the government blocked key websites, including tally-sheet websites, which would have helped track the election results. The use of new technologies such as Autel drones for facial recognition, VenApp for denunciations, and the circulation of forced confessions via TikTok and YouTube added a new layer of intimidation, reinforcing traditional tactics of public shaming and coercion.

Women, in particular, have faced intensified online and offline harassment. Female activists and candidates, especially those from marginalized communities, were disproportionately targeted, facing gendered attacks, including threats of sexual violence. Research found that women in Venezuela were subjected to 60% more gendered insults than their male counterparts, and community-level denunciations often affected women in poverty and Indigenous women leaders. These gendered forms of repression exacerbated the already harsh conditions under which Venezuelans live.

Despite the repression, civil society in Venezuela has found ways to resist. Organizations such as Espacio Público, Provea, and Conexión Segura y Libre have worked to document and expose the government's actions. They focus on censorship mapping, disruption tracking, and propaganda analysis to produce public evidence of the state's abuses, despite the constant risks of harassment, surveillance, imprisonment, and exile. Resistance also takes offline and hybrid forms, with initiatives like El Bus TV, which provides news to communities via public transportation, bypassing digital filters. Similarly, ARI Móvil brings reporting to communities that lack independent media. The app Noticias Sin Filtro has been developed by Conexión Segura y Libre to offer Venezuelans uncensored access to major news outlets.

In the face of digital repression, informal information networks have also emerged. Venezuelans curate and share information through private messaging apps where they engage in fact-checking, audio summaries, and social filtering. These networks play a crucial role in bypassing censorship and facilitating the free flow of information, despite the state's best efforts to control it.

Venezuela's experience is part of a broader pattern of cross-regional alliances where authoritarian tactics are shared across regions, and so are the strategies of resistance. Parallels can be drawn between Venezuela and Colombia, Palestine, and Senegal in terms of their experiences with shutdowns and digital repression. These alliances help share knowledge and bypass the traditional North-South hierarchies that often divide global resistance efforts.

Finally, digital third spaces have emerged as places of resistance that are neither strictly national nor global. These spaces are transnational, fostering safety, shared understanding, and learning. They offer community-driven support, allowing for the exchange of knowledge and ideas, and represent a critical space for strengthening resistance against digital authoritarianism globally.

The lived experience of digital authoritarianism in Venezuela shows how deeply the state's power permeates everyday life, with technology and legal frameworks working hand-in-hand to enforce control. Yet, despite the state's digital tools of repression, Venezuelans continue to resist, often with innovative and community-driven strategies, providing important lessons for others facing similar digital authoritarian threats.

Living Under Cyberoccupation: Ukrainian Experience from the Frontline

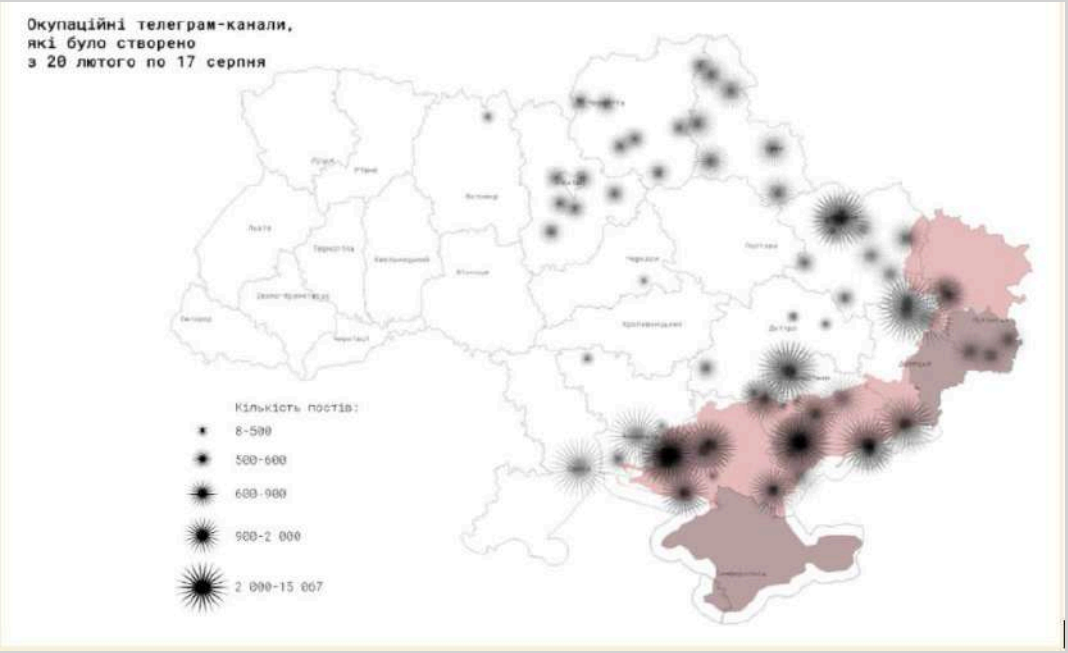
In her presentation "Living Under Cyberoccupation: Ukrainian Experience from the Frontline", the award winning Ukrainian journalist Anna Romandash explores the intense experience of Ukrainians under cyberoccupation, highlighting the impact of voluntary shutdowns, surveillance, misinformation attacks and digital censorship throughout the ongoing conflict with Russia. The presentation examines the interplay of infrastructural disruption and physical warfare, showing how information control is deployed by Russians to enforce control, monitor citizens, and disrupt communication on the occupied territories of Ukraine.

Following the annexation of Crimea and the start of armed conflict in eastern Ukraine in 2014, the Russian state has been occupying physical connectivity infrastructures, such as cell towers or Internet service providers’ offices, in order to control and manipulate online spaces, disrupt communications, and suppress independent journalism. These efforts have included targeting telecommunications networks, spreading disinformation, and employing sophisticated censorship

technologies that have been evolving over time. In Section 2 of this report we have seen how Russia hijacked the Ukrainian traffic, built its own backbone cables and progressively replaced it with Russian traffic (see Ermoshina, 2022). Anna Romandash further examines this tactic of cyberoccupation, as it has been unfolding after the beginning of the full-scale invasion of Ukraine.

A particularly striking case of cyberattacks occurred on December 12, 2023, when Russian hackers attacked the core infrastructure of Kyivstar, a leading Ukrainian telecom provider. This attack resulted in the destruction of 40% of the company's infrastructure, affecting millions of mobile subscribers and home internet users. However, critical communications for military operations were largely unaffected, highlighting the resilience of military networks. Despite these successes, the financial losses were significant, amounting to $95 million for the company.

In addition to cyberattacks, the Russian government has extended its technologies of censorship and surveillance to the occupied territories. Crimea and the newly occupied territories of Eastern Ukraine experience more extensive filtering than the Russian territories. The Russian authorities also impose the usage of MAX to the occupied territories of Ukraine. Max is a Russian government-created super app which does not support end-to-end encryption.



Besides, Anna Romandash describes a massive disinformation campaign which employed dozens of Telegram channels, created to impersonate authentic Ukrainian resistance groups or news channels.

These channels were used to spread pro-russian agenda, disinformation, manipulate the public, and disrupt the flow of accurate information. Russian-backed forces deployed these channels in the cities close to the frontline, to undermine Ukrainian efforts and further confuse the narrative by pretending to represent resistance movements. The fake Telegram channels represent a clear example of how disinformation and digital manipulation are used in hybrid warfare to control the public discourse.

The experience of occupied Ukrainian cyberspace is an experience of an informational bubble, which is subject to disinformation, bot-produced content, high level of phishing and other cyberattacks, but also physical risks of control, device seizure and searches. There is no peace in this cyberspace, it is dangerous to navigate, and Ukrainians from the occupied territories have to deal with permanent risks and informational isolation.

84%

Two in three Twitter accounts posting in Russian about the NATO presence in the Baltics and Poland are bots. They sent 84% of all Russian-language messages.

- 2022: $1.9 bill on propaganda, steady in 2023/2024
- 2023: $95 mill per commercial company to generate trolls/bots on X/ Telegram/TikTok (200,000 tweets/day)
- Operating internationally (Ukraine & beyond)
- Case: 1 mill technical accounts controlled from Kyiv by a Russian national, “opposition” political expert

The Invisible Wall: Women on Web Strategy for Algorithmic Visibility

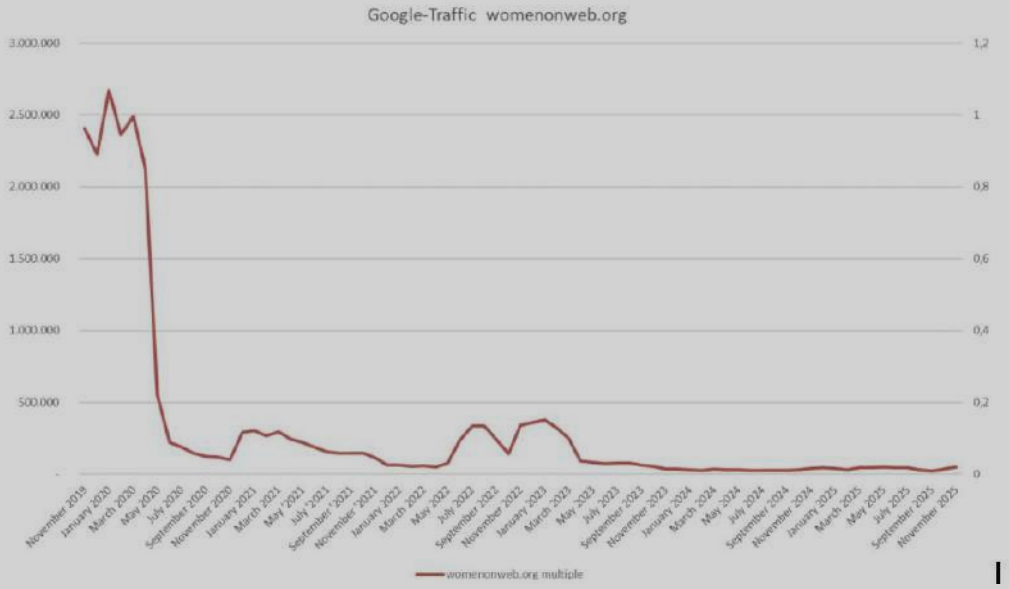
In his presentation at SplinterCon, Hannes-Jeremia Jaaks, researcher at Women on Web (WoW), which has provided online abortion support for over two decades in more than 180 countries, explained how access to abortion care has increasingly migrated into digital space—and how that shift has exposed women to a new form of structural control: algorithmic invisibility.

Search engines become the new driver of fragmentation and a building block of online walled gardens. Indeed, as Hannes-Jeremia puts it, “an uncensored website is useless if no one can find it”. As clinic closures and abortion bans proliferate internationally, especially in highly restrictive contexts, the internet has become a primary channel through which women seek information about medical abortion using mifepristone and misoprostol. Yet the very infrastructures that mediate access to this information—search engines, advertising systems, and social media platforms—have emerged as powerful gatekeepers.

The presentation documents a layered experience of suppression. In some countries, abortion information is directly blocked at the ISP level (the WoW website and its mirrors are blocked in countries including China, Iran, the Philippines, South Korea, Spain, and Turkey). In others, filtering is subtler but equally consequential: shadowbanning on social media, advertising prohibitions tied to prescription services, and sudden traffic collapses following search engine algorithm updates. WoW reports being filtered out by Bing and losing visibility after Google core updates, despite continuing demand for its services. The effect is rarely outright deletion. Instead, it is demotion, disappearance from top results, or exclusion from specific keyword searches—forms of suppression that are difficult to detect but devastating in practice.

This invisibility is particularly acute in search environments. Hannes-Jeremia highlights cases where correctly spelled queries containing the word “abortion” produced filtered or incomplete results on Bing, while misspelled versions of the same query returned more comprehensive listings. Such behavior suggests keyword-based filtering rather than neutral ranking logic. In urgent situations—when someone types “I need an abortion” into a search bar—these ranking differences are not abstract technical quirks. They shape whether medically accurate, safe information appears at all.

Search engines justify heightened scrutiny of medical content through frameworks such as “Your Money, Your Life” classifications and E-A-T principles (expertise, authoritativeness, trustworthiness). Abortion information is treated as highly sensitive content. Yet Hannes-Jeremia argues that these governance mechanisms function as de facto moral filters, redistributing visibility according to opaque criteria. Traffic graphs show sharp drops following algorithmic updates, not because user demand declined, but because ranking systems changed. In this environment, legitimacy is algorithmically conferred—and algorithmically revoked.



The gendered dimension of this invisibility is central. Women seeking abortion information often do so under conditions of fear, urgency, and secrecy. Their search behavior may be cautious, brief, and emotionally charged. If reliable providers are algorithmically buried, users are more likely to encounter misinformation, anti-abortion crisis centers, or unsafe alternatives. The harm is therefore indirect but material: it lies in the friction inserted between the search query and medically accurate information.

WoW's response is technical, adaptive, and infrastructural. It relied on the tools provided by eQualitie such as the eQpress for hosting and Delfect for DDoS protection. It has developed anti-censorship blogs optimized for search engines, embedded contact details directly into search snippets, replicated content through Wikipedia entries and mirror sites, and monitored performance through search analytics tools. The strategy reflects a clear understanding that visibility must be engineered within algorithmic systems that privilege link structures, user behavior metrics, and perceived authority signals. The goal is not merely to publish information, but to survive ranking systems.

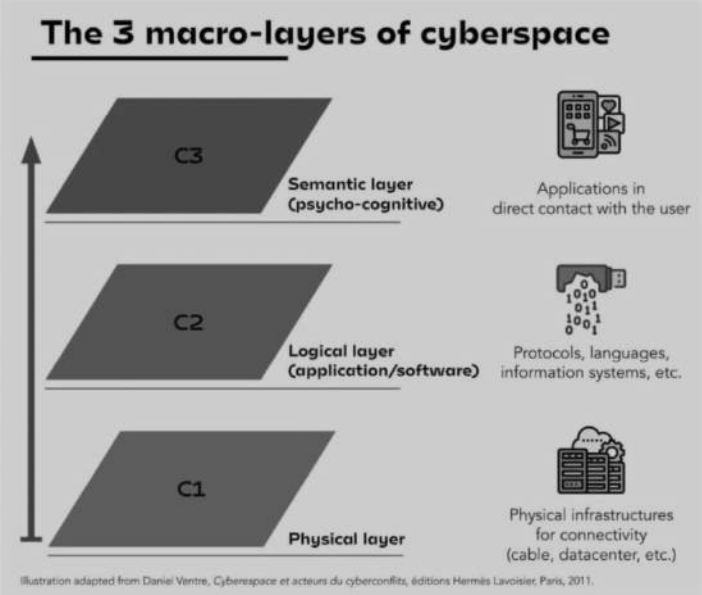
At a broader level, Hannes-Jeremia reframes censorship as multi-layered: even when content is technically accessible, it may be algorithmically marginalized. The battleground has shifted from state bans to platform governance and search engine logic. Women's reproductive autonomy and digital self-determination now intersect with ranking factors, moderation policies, advertising restrictions, and opaque filtering mechanisms. The conclusion is not only about abortion rights but about information power. As targeted attacks

on online abortion resources increase, ensuring discoverability becomes as critical as ensuring legality. The experience described is not one of dramatic takedowns, but of gradual erasure—of reliable medical knowledge slipping just out of reach at the very moment it is needed most.

The Age of Cognitive Sovereignty

In her presentation, Magdalene Karallis's (DISARM Foundation) reframes internet fragmentation not primarily as an infrastructural or regulatory problem, but as a cognitive one. In the "Splinternet era," fragmentation increasingly manifests at the level of meaning, perception, and interpretation—what the presentation calls the semantic or psycho-cognitive layer of cyberspace.

The Splinternet fractures not only technical networks, but shared realities. Conflict-driven influence operations, AI-enabled manipulation (including deepfakes and leader impersonations), cross-platform disinformation ecosystems, and opaque recommender systems have produced parallel interpretive worlds. Fragmentation therefore operates not only through routing paths or market segmentation, but through narrative divergence: different publics inhabiting incompatible semantic environments.



To conceptualize this shift, Magdalene draws on a three-layer model of cyberspace: the physical layer (infrastructure), the logical layer (protocols and software), and the semantic layer (direct user interaction

This is where cognitive sovereignty becomes central. It is defined as the ability to interpret threats independently—to resist mass misinformation mobilization, platform-driven visibility biases, echo chambers, and socially engineered divides created by domestic or foreign influence networks. In this formulation, sovereignty is no longer confined to territorial control over infrastructure; it becomes a capacity at the level of the individual mind.

This reconceptualization changes how fragmentation should be measured. If the analytical focus remains solely on cables, routing tables, regulatory regimes, or economic blocs, one may overlook the fragmentation of interpretive capacity. Cognitive fragmentation manifests when individuals' threat perceptions, political judgments, and emotional responses are systematically shaped by coordinated influence operations. The body and personality—attention, affect, trust, fear—become the sites where fragmentation materializes.

The presentation identifies a coordination problem across governments, platforms, researchers, and civil society: similar behaviors are labeled differently; investigations are conducted in incompatible formats; influence techniques are observed repeatedly without shared mapping. This semantic disunity weakens resilience precisely at the cognitive layer. Fragmentation is thus reproduced analytically: even responders lack a shared vocabulary.

DISARM offers a response to this problem. Inspired by the MITRE ATT&CK framework but adapted for influence operations, DISARM provides a structured taxonomy of tactics, techniques, and procedures applicable across regions and conflicts. It offers consistent tagging, machine readability (STIX/OpenCTI compatibility), and interoperability with EU and NATO threat-intelligence formats. The goal is not merely classification, but alignment—creating a shared semantic infrastructure for identifying and comparing influence operations globally.

Indeed, cognitive sovereignty depends on shared analytical standards. When responders across sectors use incompatible vocabularies, they inadvertently reinforce fragmentation. A standardized mapping system enables rapid aggregation of activity across platforms and conflicts, pattern recognition ("same tactic, new theater"), and interoperable workflows that do not rely on shared physical infrastructure. In this way, standardization becomes a defensive mechanism at the semantic layer.

The case studies—election interference in the Sahel and fact-checking organizations confronting Russian disinformation campaigns—

demonstrate how shared terminology and structured mapping enable coordinated response and resilience building . Through training models, study guides, and cross-sector collaboration, DISARM aims to build what the presentation calls a “Europe-driven analytical standard for the semantic layer” .

The deeper analytical shift lies in recognizing that the Splinternet is not only a geopolitical or infrastructural phenomenon. It is a psychological one. Influence operations target perception, memory, identity, and emotional triggers. AI-enabled manipulation intensifies this by creating synthetic media that directly engages sensory perception. Platform recommender systems shape attention patterns and emotional reinforcement loops. Fragmentation thus penetrates the body: stress responses, polarization dynamics, trust erosion, and identity hardening.

By foregrounding cognitive sovereignty, the presentation suggests that measuring fragmentation requires examining how individuals experience reality—whether they can independently interpret information without being captured by engineered narratives. The unit of analysis shifts from networks and markets to interpretive autonomy. The “response layer” must therefore be standardized before fragmentation hardens irreversibly.

In this framework, cognitive sovereignty is both a diagnostic and a normative goal. It reorients internet governance debates from infrastructure control toward the preservation of interpretive agency. Fragmentation becomes measurable not only in routing paths or regulatory regimes, but in the degree to which populations retain the psychological capacity to evaluate information critically, resist manipulation, and maintain coherent shared realities.

Section 3

Infrastructuring autonomy: protocol level solutions for countering isolation

MahsaNet: building grassrooted resilience

MahsaNet is a grassroots, globally distributed engineering effort born out of Iran's escalating censorship regime and sharpened by wartime shutdown conditions. What began as an Android-only circumvention app evolved, under intense political and technical pressure, into a full-stack resilience ecosystem designed to survive deep packet inspection, IP blocking, infrastructure takedowns, and even coordinated disinformation campaigns targeting the tool itself.

At its core, MahsaNet is structured around a dynamic relationship between MahsaServer and client applications such as MahsaNG VPN. MahsaServer aggregates a massive collection of donated VPN configurations and distributes them intelligently based on real-time conditions . One of its key innovations is a "protocol availability radar," which continuously assesses which protocols are currently viable under Iran's filtering regime.
This is critical in an environment where censorship tactics shift rapidly—through SNI filtering, TLS fingerprinting, active probing, or wholesale IP blocking. Instead of relying on static endpoints, the system pushes working configurations dynamically to clients, enabling over 3.5 million successful connections per day .

On the client side, MahsaNG is a heavily customized fork of v2rayNG and xray-core. By building on these flexible proxy frameworks and integrating custom components such as "knocker-core," MahsaNet can rapidly adapt transport layers and obfuscation strategies. The architecture is designed for agility: configurations rotate, protocols shift, and endpoints evolve as soon as filtering patterns are detected. With more than 1.5 million active users, the system functions less like a traditional VPN service and more like a distributed, adaptive tunneling network.

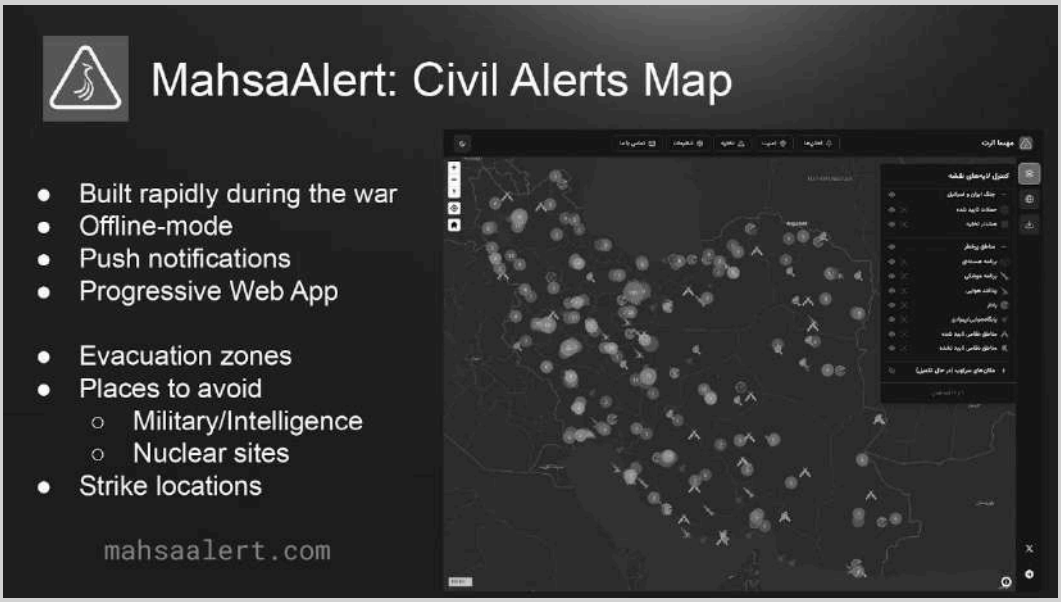
The year 2025 marked a decisive escalation. Funding cuts destabilized the broader circumvention ecosystem, other tools became ineffective, Iran's filtering apparatus grew stricter, and Cloudflare actions disrupted proxy infrastructures. During the Iran–Israel conflict, the regime imposed a full internet shutdown while simultaneously launching disinformation and malware campaigns against MahsaNet itself. In response, the team overhauled backend infrastructure, released multiple new versions of its clients, and expanded into cross-platform support, including iOS. This period transformed MahsaNet from a single application into an integrated resilience platform.

A central component of this expansion is the SegmentVPN SDK, an open-source, cross-platform VPN framework built with Flutter and designed around a multi-core architecture supporting engines such as knocker-core and Outline. Its modular structure allows other developers to integrate circumvention capabilities directly into their own applications. This reduces monoculture risk: rather than one easily fingerprinted app, circumvention becomes diffusely embedded across multiple tools. For users on the ground, this diversification makes blanket blocking more difficult. If one signature is detected and filtered, alternative implementations remain viable.

Complementing this client layer is CompassVPN, a scalable, self-hosted VPN server agent with built-in monitoring, automated management, and horizontal scaling features. By enabling activists, diaspora communities, or civil society actors to deploy and manage their own infrastructure, CompassVPN reduces reliance on large commercial cloud providers that may withdraw support under political pressure. Automated firewall configuration, ingress management, and monitoring dashboards allow rapid redeployment when IP ranges are blocked. In shutdown conditions, the capacity to spin up new nodes quickly can determine whether connectivity resumes in hours or remains suppressed for days.

MahsaNet also extends beyond tunneling. During wartime, the team built MahsaAlert, a Progressive Web App designed to provide civil alerts with offline capability. It includes evacuation zones, strike locations, and markers for military or intelligence sites. Offline caching and PWA architecture allow partial functionality even during degraded connectivity. This represents an important shift: circumvention is not only about reaching social media but about preserving situational awareness when infrastructure collapses. In shutdown environments, the ability to disseminate or cache critical information can have direct life-saving implications.

Finally, CensorDB introduces a structured intelligence layer. This crowdsourced censorship database aggregates data, enables user submissions, and exports configurations compatible with tools like V2ray and sing-box. By transforming censorship events into analyzable datasets, MahsaNet shortens the feedback loop between detection and response. Rather than reacting blindly to blocking waves, developers can adapt configurations based on empirical filtering evidence. Over time, this creates a learning system that improves resilience against recurring techniques.



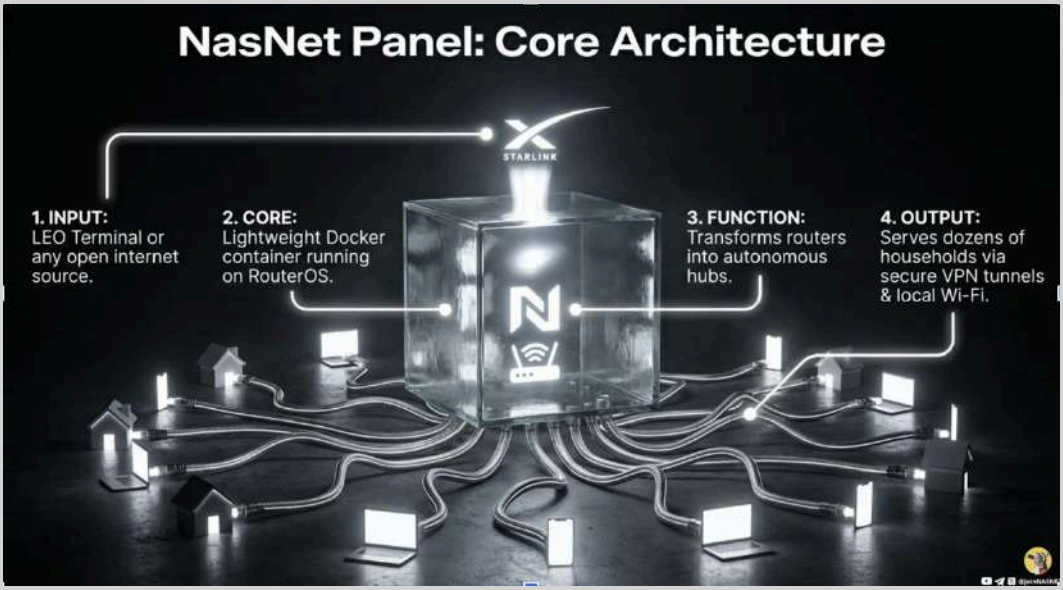
Taken together, MahsaNet's architecture operates across multiple layers: dynamic configuration distribution, multi-protocol client agility, decentralized server deployment, embedded circumvention frameworks, wartime civil information tools, and a data-driven censorship intelligence database. This layered approach is essential in high-intensity filtering environments, where regimes combine DPI, infrastructure pressure, legal threats, and psychological operations.

For people on the ground during shutdowns, the practical implications are significant. Adaptive config distribution increases the probability of reconnecting during filtering spikes. Self-hosted infrastructure reduces dependence on politically exposed intermediaries. Offline-capable civil alert tools preserve critical information flows when connectivity is intermittent. And structured censorship data accelerates recovery after blocking events. MahsaNet thus represents more than a VPN. It is an attempt to engineer operational resilience under digital siege building an ecosystem that evolves as quickly as the censorship apparatus it confronts.

NasNet: Building Shutdown-Proof Connectivity for a Free Internet

NasNet is the largest Farsi-speaking Starlink community in the world building parallel networks that offer more independence from governmental control and shutdown resilience. Currently, over 50000 terminals are active in Iran. The project started as a technically complex

inititative facing network engineers, with a hard to digest 52 pages guide. It has progressively evolved into a user-facing easy to install solution with a configuration generator based on only 8 questions. Due to the censors capacities to quickly learn about and suppress circumvention technologies, NasNet has introduced the Nas Net Panel, a dynamic connectivity stack.



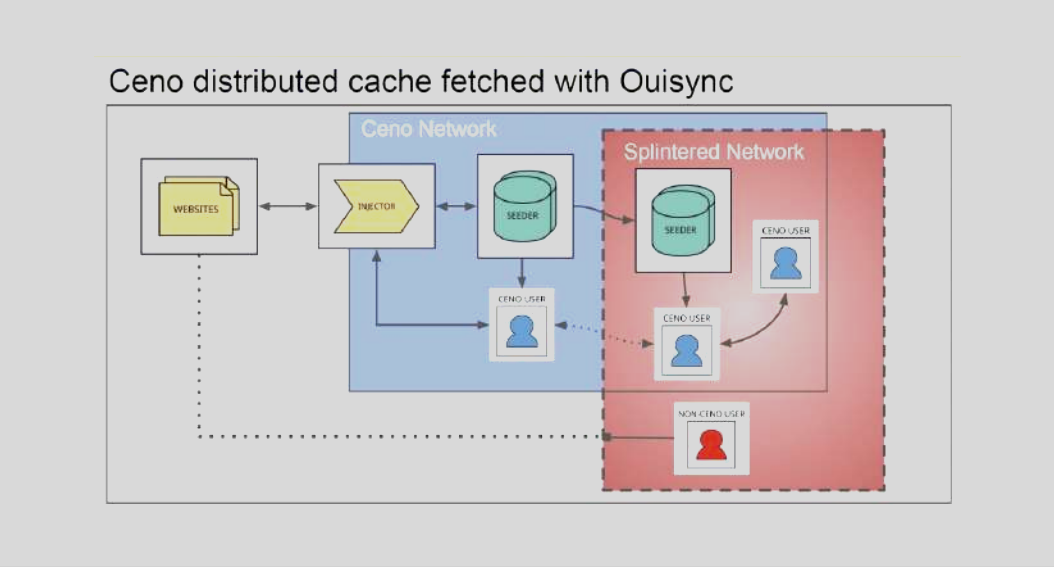
NasNet stack is source agnostic. In the future it will be used not just with Starlink but with other LEO providers such as Amazon Project Kuiper, but also with mobile connectivity technologies (SIMs, e-SIMs, Direct-to-Cell). In the future it will support any open internet source. Currently the Proof of concept has been released and the project is actively field-tested. Next steps include One-click installation, Multi-link Failover and finally releasing the Edge Platform that supports other applications.

Ouisync for websites

In splintered environments, applications and services that depend on centralized cloud infrastructure face several challenges such as synchronizing application state across devices, distributing files or content to users and providing access to up-to-date web content when origin servers are unreachable. Traditional client-server architectures fail when connectivity to central servers disappears. Ouisync can the be used as a decentralized mechanism to maintain data availability and synchronization in these constrained conditions.

Ouisync is a user facing application for secure p2p file sharing developed by eQualitie. But it is also a distributed storage and transport library with an API. It allows encrypted storage, mutable content-addressable data structures, peer-to-peer synchronization and does not depend on centralized servers. The system supports synchronization among trusted and untrusted peers, enabling distributed collaboration and content distribution. Ouisync relies on DHT (Distributed Hash Table) for peer discovery, PEX (Peer Exchange) for network topology expansion and Local discovery on LAN.

Ouisync implements three access models: Read-Write (Multiple participants can modify data) Read-Only (Users can only read content shared by the repository owner) and Blind (Repository is stored but can not be read). These modes enable different collaboration models and allow fine-grained control over distribution and collaboration scenarios.



Ouisync can synchronize application state across user devices: data stays end-to-end encrypted, no user accounts or centralized services are required, optional caching server can be added.

One of the intergration use-cases is the Ceno browser where Ouisync helps to synchronize browser settings and cached content between devices using the Ceno browser app.

Ouisync can be used to transfer data in the case of splinternet. Files can be packaged into an Ouisync repository bundle and injected into restricted networks. Distribution methods include: satellite transmission, sneakernet (physical transport) and offline injection points. Content bundles are transmitted via satellite and propagated locally through peer-to-peer synchronization.

The integration of Ouisync with 451 tools enables automatic synchronization and propagation of website mirrors. If the 451 tools plugin is added to a website, the user can accesse a website normally and in the case of blocking, the system will redirect the user to a mirror. Ouisync keeps mirrors synchronized with the latest content.

Traditional ways of updating mirrors with fresh data (e.g. rsync, scp, sftp) have the disadvantage that if the mirror is positioned inside a censored country, access to the data source can be easily blocked. This is due to the static acyclic graph network topology implied by these tools. Ouisync instances can update themselves with new data in both directions and will automatically attempt to establish connections to other instances even if those are deployed later. This implies a dynamic network topology permitting cycles which is harder to block and simpler to maintain.

Besides mentioned use-case examples, Ouisync can be integrated in other applications through library integration, Linux CLI and Storage Access Framework. Ouisync provides a secure, decentralized data layer for applications and content distribution that works even when the

global Internet is fragmented, central servers are unavailable or connectivity is intermittent. By combining encrypted repositories, peer discovery mechanisms, and flexible distribution models, Ouisync enables resilient information flows across fragmented networks.

Conclusion

Sovereignty will be federated

By Najib Safieddine,

a researcher of digital governance, socio-technical imaginaries and the politics of AI regulation. Najib is also an independent consultant with the German cooperation and development agency, GiZ, and the Friedrich Ebert Foundation.

Sovereignty will be federated

Najib Safieddine, researcher of digital governance, socio-technical imaginaries and the politics of AI regulation. Najib is also an independent consultant with the German cooperation and development agency, GiZ, and the Friedrich Ebert Foundation.

Digital sovereignty is becoming an evermore present issue, and a potent idea in the global techno-political discourse. There are different understandings and current applications of digital sovereignty, from sectoral data sovereignty, to infrastructural digital sovereignty to total network sovereignty, as we see in RuNet or NIN. The digital and the political realms are converging, and an early impact point is taking the shape of digital sovereignty.

Digital sovereignty, I argue, is a nation-state reaction to the intensification of the materiality of data in today's world. Data is increasingly holding material qualities that fundamentally alter the political and economic role of digital technologies. It has become less a proxy and more a mirror; an increasingly more accurate referent to the data subject - whether an individual, a structure, or a system; from people to power grids. In this sense, data has moved from description to simulation, and it is this shift that grounds the growing materiality of the digital itself. However, underrepresented groups risk to be exluded not only by the nation-state plan but also from the possible alternatives to it: not all the faces are reflected in that mirror.

As this intensifies, data will thus be legally bound by national politics within a nation-state international system. At the level of everyday life, this transformation is already visible. Individuals are rendered legible through tens of thousands of data points generated through routine digital interaction. We are no longer a society of humans, but a society of data points. As stacked data points approach functional equivalence with natural persons, the infrastructures that collect, process, and circulate them become legally and politically consequential. Data materiality here is not metaphorical: it is infrastructural, economic, and jurisdictional. But, how did the digital realm come to be characterized by such pervasive and asymmetric control?

Early digital imaginaries resisted this outcome. The early internet was envisioned as a horizontal space of free movement, immune to hierarchy and centralized authority. Yet even at that moment, it was already clear that infrastructure -not content or culture — is the decisive

encoder of power. Control over networks, cables, standards, and financialized data systems was already consolidating in the hands of existing corporations. The failure to challenge these infrastructural foundations allowed a techno-utopian vision of the internet to coexist with, and ultimately give way to, the technofeudalism that followed.

The result has been a reconfiguration of capitalism rather than its transcendence. The open and under-regulated internet enabled the corporation to become the dominant unit of social organization, accelerating a regression toward feudal dynamics. At the moment, 5 corporations essentially own and operate the digital commons, extracting rents from individuals, companies, and states alike.

Here, is the inflection point which digital sovereignty emerged from: techno-nationalization as the reaction of the nation-state project to the corporate globalism project. Digital sovereignty is emerging as the state's response to this globalized concentration of power. After all, the nation-state project was conceived as an antithesis to feudalism. We can see history rhyming again now, as Mark Twain would say.

Why sovereignty in the digital? Because sovereignty is the spatial demarcation of struggles for legitimacy and control. In a battle of control with global actors, national actors enforce the national as a jurisdiction. This reaction is not merely ideological or protectionist; it reflects a structural contradiction between territorially bounded authority and globally scaled digital infrastructures. Digital sovereignty reflects the tensions between the national and the planetary scales.

This shift is observable worldwide. Models of digital sovereignty increasingly move from sectoral data protection toward comprehensive network control, ranging from state-managed internets to tightly regulated information flows. While authoritarian systems drive fragmentation through overt network control, the European Union also contributes to fragmentation through its emphasis on personal data protection and competition law. The difference lies less in the fact of fragmentation than in the political rationale and institutional form through which it is pursued.

The United States digital project illustrates a contrasting model: build infrastructure first, lobby aggressively, and consolidate power through scale. A handful of firms now operate cables, clouds, platforms, and applications while simultaneously deploying the largest digital lobbying apparatus in Brussels. Europe, by contrast, has specialized in regulation rather than construction. Its primary digital export has not been a product or service but law. Yet the regulatory "Brussels Effect"

weakens when confronted with the lobbying-driven “DC Effect,” as regulatory ambition collides with infrastructural dependence.

This asymmetry exposes a structural limit. Regulation codifies power relations, but infrastructure produces them. A conception of digital sovereignty grounded solely in legal authority cannot rebalance a landscape in which the material foundations of the digital remain externally owned and opaque. What is required instead is an understanding of sovereignty as the capacity to build, govern, and safeguard interoperable and publicly accountable digital infrastructure.

Such a project requires federation not as a technical preference, but as a political strategy: a way of reconciling sovereignty with openness, and democratic control with cross-border interoperability. Such a model implies a layered approach. At its base, law must be translated into technical baselines, compliance mechanisms, and enforceable standards embedded directly into infrastructure. This requires coordinated action by European institutions, cybersecurity agencies, and data protection authorities, using regulatory instruments to anchor rights within technical systems. Above this legal foundation, governance must become participatory. A European Digital Infrastructure Board could coordinate public authorities, private operators, and civil society to manage standards, oversee certification, resolve disputes transparently, and publish audit data in publicly accessible registries.

Operationally, this framework depends on federated and interoperable technical systems. Data spaces must rely on shared connectors, common security baselines, and open architectures that allow secure cross-border data movement without central control. Open software plays a critical role here—not as an ideological preference but as a practical governance tool. Open reference implementations, digital identity wallets, and automated compliance systems ensure that public institutions, SMEs, and civic actors can inspect, modify, and collectively improve the infrastructure on which sovereignty depends.

Recent EU initiatives suggest that this infrastructural turn is beginning, albeit unevenly. Semiconductor policy, sovereign cloud procurement, and digital public infrastructure resolutions signal a shift from pure regulation toward limited construction. Yet democratic institutions remain weakly positioned within this process. The risk is that Europe attempts to certify or regulate sovereignty into existence rather than materially building it, reproducing dependence under the guise of compliance.

At its core, this is not a technical failure but an imaginative one. Techno-solutionism cannot resolve techno-feudalism or techno-nationalization. What is lacking is a socio-technical imaginary in which public interest, collective governance, and democratic accountability shape infrastructure itself. Such imaginaries are not spontaneous; they are institutionally stabilized and publicly performed. As long as Europe's digital project remains primarily regulatory, corporate imaginaries will continue to be infrastructurally reinforced.

The historical analogy is instructive. The digital economy developed alongside neoliberal governance models that hollowed out public innovation capacity and outsourced platform functions to private firms. Reversing this trajectory requires infrastructural ambition comparable to past public works projects—treating digital systems as networks of networks governed by shared rules and democratic oversight.

Ultimately, digital governance cannot be democratized without being politicized. As data becomes increasingly material, it necessarily enters the political realm. Without public ownership or stewardship of core digital infrastructure, democratic governance of the digital remains structurally impossible. For Europe's digital layer to be governed democratically, it must be problematized, materialized, and openly contested. Only then can digital sovereignty function not as isolation, but as a shared, federated project rooted in public institutions and accountable infrastructure.

SPLINTERCON.NET

eQualitie