Network paradigms and infrastructural ideologies: Standards and protocols in a geopolitical context

Maxigas,
2023

critical Infrastructure lab

Network paradigms and infrastructural ideologies: Standards and protocols in a geopolitical context

Published by the critical infrastructure lab, Amsterdam, November 2023.

Set in Source Sans, Source Serif and Source Code.

Made with free software from plain text:
https://doi.org/10.5281/zenodo.8412230
DOI 10.5281/zenodo.8412230

critical infrastructure lab document series
CIL#005
https://doi.org/10.5281/zenodo.8412252
DOI 10.5281/zenodo.8412252

This work was generously supported by funding from the Ford Foundation [grant number 144895, 2022] and Omidyar Network.

Table of Contents

Draft released for the debate on"Standards, Protocols and Governance" on the 20th June in Amsterdam, organised by Open Future and the critical infrastructure lab.

For the standards & protocols workstream collaboration.

Executive summary

Communication protocols such as HTTP[1] define common rules for the transmission of information in media and control infrastructures. What they also do is shape geopolitical power struggles, urban conflicts and everyday lives. Protocols don't fall from the sky, however. They bear the marks of the places and serve as signs of the times where and when they were forged. Thus, it is possible to interpret protocol specifications media archeologically as the material residue of the human cultures that produced them and the social conflicts that shaped them.

The central question of this report is how the public interest is articulated through protocol design, and consequently what strategic interventions can policy advocates and policy makers embark on to further such public interest in future (identity) protocols. The question is answered on the basis of the longitudial study of three network paradigms relating to the Internet, mobile phones and 5G smart networks — and more detailed case studies that yield a cross-sectional analysis of identity protocols (at the time of writing, we analysed OpenID and Aadhaar). It is observed that contemporary identity protocols draw on historically situated network paradigms. The argument drawn from the analysis is that geopolitical hegemony shapes network paradigms and sovereignty grounds the identities offered by protocol designs.

The conclusion is that policy advocates and policy makers should look beyond the immediate technological problems of protocol design, further towards strategic interventions in constituent power that can shape the emergent sovereignities in which the (identity) protocols of the future can be anchored. The public interest is shaped by sovereign power as much as protocol design, in standards bodies and elsewhere. In fact, sovereign power increasingly shapes publics through the standardisation and governance of communication protocols. Thus, impact for change should be motivated by political decisions and ideological convictions about what kind of powers we are willing to subject ourselves to. The ensuing recommendation is to engage with telecommunications companies who are in the best position to propose — and even impose — interoperable identity protocols in the near future.

---

01 The Hypertext Transfer Protocol, an application layer protocol in the Internet protocol suite, first standardised in RFC 1945 in 1996 and "has been in use by the World-Wide Web … since 1990" (Berners-Lee, Fielding, and Frystik Nielsen 1996, 1).↩

1 Standards-setting in the public interest infrastructures

1.1 *Problem statement and approach*

The contemporary Internet consists of open protocols overlaid with the parasitic growths of proprietary platforms, with adverse impact on trust and democratic values. This condition has been framed by the Ford Foundation, New America's Digital Impact and Governance Initiative and Microsoft - leading organizations in the Missing Layers collaborative, as the case of missing layers of a digital ecosystem that is people-centric, functions as a digital commons, and is enabled by open protocols. One of the goals of this collaborative is to seek designs that build on the principle of openness to balance innovation with the protection of fundamental values.

The Critical Infrastructure Lab contributes to this line of thinking with the present report. In the report, we identify the cultural aspects of protocol design that may inform the standardisation and governance of future protocols. We also advise that viable pathways to adoption and effective advocacy will have to consider not only prior work in protocol design but also the current state of play in geopolitics and global political economy. In order to build that argument, the report constitutes a departure from the Missing Layers framework in that it puts the question of sovereignty centre stage, highligting its influence on interoperability in the real world. The thematic focus of the report is one of the "missing layers" – identity — but the context is drawn widely and the results are generalisable to other layers.

The report is written from a critical humanities perspective, taking a socio-technical apprach to the subject matter of protocols, standards and interoperability. This is to complement parallel investigations into trade-offs between alternative protocol designs and governance mechanisms. The promise of the critical humanities is to produce a rounded understanding of phenomena by interpreting it in a wider context, identifying the limits of alternative approaches, and pointing beyond the current material conditions towards a better world. In turn, taking a socio-technical approach to technological matters comes with the assumption that the material configuration of technologies is the outcome of contingent power struggles between actors who bring their own interests, social positions, and cultural background into play. The critical humanities perspective and the socio-technical approach makes it possible to research where protocols come from, in order to make normative recommendations about where they should be going. Identity protocols serve as a key example because they integrate humans into protocological regimes of power.

For the purposes of this report, a preliminary definition of identity describes how users become users of socio-technical systems by virtue of infrastructural effects. Identity is granted in three discrete moves, where

only the middle one is traditionally considered the domain of identity protocols. In line with the critical humanities approach, however, we consider what can happen before and after "logging in" as crucial context for understanding the power of digital identities.

First, *access* **is sought:** Systems may seek to identify users or, conversely, users may seek to identify with systems. In any case, there is a desire (machinic or not) for becoming a subject to a certain regime of power. The regime grants freedoms and impose restrictions in the same gesture. Users are empowered by the system, acquire agency to act — but in particular ways. For the same reason, identity systems are ideological constructs that need justification and through which power is exercised (see section 2.3). The infrastructural ideology behind the protocol has to account for the legitimacy of the system and its benefits for users. There are many possible and necessary moments in which justification may take place. Identification may be justified at the standardisation stage where identity is mandated to take place in the link layer (see section 3.2), or much later at the moment individual users sign in to a service (see section 4.1).

Then, the user is *authenticated***:** In other words, the self-similarity of the user is established by the protocol. The user is this user and not another one, a particular user from the totality of accounts on the system. The user becomes a particular user through individuation, starting as a generic user whose only need is to concretise its identity, to an actual user who has a history in the system and thus who is recognised by the system. This recognition legitimises the participation of the user in the protocological regime. The recognition allows the user to be part of the media and control infrastructure with which they now identify.

Finally, *authorization* **to access resources takes place:** Identity protocols serve a purpose. The authorisation of access to resources cannot be separated from the problem of identifying users, because it is always already a consideration when choosing to rely on a particular identity protocol design. Infrastructures may work better or worse for different people, and lines of inclusion and exclusion within digital infrastructures are often drawn through granting access or denying resources. This is not to suggest that any one person is defined by how they are identified by media and control infrastructures. In fact, critiques of cybernetics (Tiqqun 2012) suggest that there is more to life and freedom than what can be captured in a digital identity. The critique of control society instigated by the French philosopher Gilles Deleuze (1992) hinges on the idea that we become *dividuals* whose identity is shattered and captured as shards

in separate databases that we can access or being denied through passwords.[2]

To summarise, identity is how users become users, comprised of a three stage act in which access is sought, self-similarity is established, and authorisation is performed.

Shaping identity protocols is a strategic undertaking that

> *What are the standards bodies that impact different layers of communication infrastructures? What are the actors and forces within standards bodies that shape infrastructures? What is the relationship between contemporary geopolitical development and standards bodies? What are the relations between the geopolitical developments and the operationalization of standards? How can standard-setting processes more explicitly support communication infrastructure as a human rights enabling environment? What are the limitations and opportunities within standard bodies to produce public interest technological infrastructures? What are the opportunities for 1) governments, 2) civil society activists and advocates, and 3) public interest technologists to engage?*

While in the current chapter we set out the approach to these problems, in the next one we clarify some of the key concepts that inform the analyses. Chapter three and four provides answers to these questions in selected cases. In chapter three, broad network paradigms are identified in a "long view" of communication protocols. In chapter four, some strategically chosen contemporary identity protocols are analysed in line with the above questions. The longitudial and cross-sectional study chapters are followed by a final chapter with conclusions and recommendations.

---

02 We hope to show that many other ways of identification with media and control infrastructures exists than passwords, but thinking of identity protocols as infrastructural elements whose effects drive alienation under capitalism and the anxieties that perain to late modernity is a helpful perspective that we develop further in section 2.1 later.↩

1.2 *Standards-setting*

Standards-setting can be viewed as a process during which techical design decisions are hashed out in obscure discussions between engineers. Readers who pick up this report may already know and believe that the reality of standards-setting involves much more "politics" than its boring processes and glacial speed may suggest. A previous Critical Infrastructure Lab report (Cath 2023) gave a damning view on how power relations shape even purpotedly "open" standards processes through cultural factors. These cultural factors have a decisive influence on who can participate in standardisation, and consequently shape what standards are made. In turn, these standards shape the action possibilities of actors when widely deployed in society. As we have argued in the previous section, infrastructures work (or break down) differently for different people. Who they work for is determined through standards-setting, and other factors mentioned in the next section.

Traditionally standard-setting is dominated by private sector participation (Perry and Nöelke 2005; Carmin, Darnall, and Mil-Homens 2003) and global standard-setting is dominated by industry from specific geographic areas such as the US (Carr 2015; Scholte 2017) followed nowadays by Asian countries (Yates and Murphy 2019; Tang 2020). This can be explained by market dominance and the fact that this stakeholder group is extra incentivized to engage in standard setting because it is most likely to directly benefit from standards (Olson 1971), as well as the availability of both case matter and standard-setting expertise and experience (Balzarova and Castka 2012; Hallstrom and Bostrom 2010). Even when the private sector has the largest interest and significant engagement with standard-setting, other stakeholders at times can play important roles, whether it be directly or indirectly. In the areas of ICT standardization there has nearly four decade trend of deregulation and limited government engagement, after the IETF won over the government-backed ISO in the standardization of the architecture of the Internet (Russell 2014). However, there are indications that this trend might be reverted with the resurgence of government interest (Haggart, Tusikov, and Scholte 2021), even though the government-led International Telecommunication Union (ITU) still plays a marginal role in the standardization of digital technologies (Balbi and Fickers 2020). As noted above, citizens, in the literature and standards processes described as 'users' (Nottingham 2020) or 'consumers' (Farrell and Saloner 1985), often know very little about standardization (Healy and Pope 1996). Some authors even describe the distance between users and standardization processes as 'worlds apart' (Jakobs, Procter, and Williams 1996, 138). This can be in part attributed to the expertise, time, and resources that are needed to

participate in the standards process, as well as the steep learning curve and the time it takes to knit relationships and legitimacy in standards bodies.

There have been initiatives in standards bodies to develop standards for the positive societal impact of the standard setting process, as well as developing standards to certify levels of 'corporate social responsibility' (Bryson and Winfield 2017). However, these norms never reached full standard or certification level: they exist only as guidance standard and their implementation cannot be mandated. This can be attributed to the fact that the stakeholders that are already active in standards bodies, most notably corporate actors, have no direct interest in limiting their activities (Balzarova and Castka 2012). Further, new standards developed within the framework of existing standards need to be in line with existing frameworks, which makes it harder to disrupt the status quo to improve the situation of those who are not directly represented in standard setting (Castka and Balzarova 2008). RFC formally stands for Request for Comments, but the series describe internet protocols, architectures, and procedures for several internet infrastructure bodies, most notably the Internet Engineering Task Force (IETF). Organizations that produce RFCs, such as the IETF, have developed review processes to take the societal impact of protocols into account. Examples are an RFC published by theInternet Architecture Board for privacy considerations for protocols, which also describes guidelines for privacy reviews (Cooper et al. 2013), an informational document published by the Internet Research Taskforce (IRTF), a sister research organization to the IETF, that described the relationship between human rights and protocols and produces guidelines for human rights reviews of protocols (ten Oever and Cath 2017), and an RFC from the Internet Architecture Board that described how users should always be the prioritized stakeholder group in trade-offs in protocol development (Nottingham 2020). As in the ISO, these RFCs are not normative and are only informational, meaning that they do not make normative changes to the RFC development process, in contrastto other considerations, such as security considerations, which are mandatory for every published RFC (Doty 2015).

Consequently, identifying a clear pathway to adoption for a certain standard backed by civil society should account for the dynamics of standards bodies, the dynamics of the respective markets, and the larger power plays behind those developments. In chapter 3 we show that any one time, there are only a limited number of actors who are in a realistic position to propose and impose standards, whether those come from the established standards bodies, or produced by a whole new set of standards-setting organisations set up by the hegemon to advance their interest. Standards-setting allows for substantial collaboration, debate and agreement even between actors who would otherwise be in open competition, but the terms of the engagement are shaped by power struggles inside and outside the organisational perimeters of standards bodies.

1.3 *The public interest*

While standards-setting serves market efficiencies as much as the public interest, we have argued that in both cases the real question is who sets the terms for efficiency and values that others are measured against. It is relevant that the public interest as a concept emerged historically from US infrastructure policy in conjunction with the Transportation Act and the Radio Act in the 1920s (Napoli 2001). Government policy and regulation is often enacted in the name of the public interest, in line with the democratic mandate of the state. The role of the state is to shape markets towards outcomes that serve the public interest rather than the narrow objectives of capital accumulation.[3] Simply put, in a neoliberal democracy the state is there as a safeguard against market failures. In turn, the role of civil society and grassroots movements is to represent and embody the public interest in cases where the state falls short of its responsibilities of upholding it.

The public interest is useful to debate in the singular, because only then actors can engage with each other productively to work towards universal values. At a historical moment when humanity have to act intentionally on a planetary scale, in the face of the climate crisis and global inequalities, this is not only an abstract ideal, but a demand of our times staked on the survival of our species. What is the public interest remains elusive and open to definition. The critical infrastructure lab centres people and planet over profit and capital, which is consistent with the idea of the public interest as a collectively held, democratic, and aspirationally universal-normative

Whether a protocol serves the public interest is hard to discern from the protocol design itself. Controversies about the public interest can arise at any stage of the innovation process. For the purpose of this report, we treat the innovation pipeline as three disinct moments: *standardisation*, *implementation* and *deployment*. For instance, the HTTP protocol mentioned in the introduction has been standardised within the Internet Engineering Task force, which publishes a series of standards documents called Request for Comments that define the protocol. HTTP is for fetching information resources, but the RFC cannot do that — the RFC is a recipe document that systematically explains how to do it.

The protocol is implemented based on the RFC in tools and libraries such as `curl` or `requests`, and embedded in user-facing applications such as web browsers like Mozilla Firefox or the software running in Tesla cars. Successful standards have various different implementations, including competing and complementary ones, exactly because the implementation detail matter. The implementation details can constrain the action possibilities of actors as much as the protocol design itself.

Governments who have long supported standardisation processes are just waking up to these realisations about the important role of implementations. A case in point is the establishment of the Sovereign Tech Fund by by the German Federal Ministry for Economic Affairs and Climate Action last year. The goal of the Fund is "strenghtening digital infrastructure and open source ecosystems in the public interest" and it disperses with a 11.5 million EUR available budget in 2023 (SPRIND GmbH 2023). Protocol implementations are prominent in the highlighted entries, including sometimes several different implementations of the same protocol.[4]

The exact configurations in which standards and implementations are deployed in a particular context can make as much difference as the design details of the protocol and the implementation details of the chosen components. Protocols meet the ground as parts of infrastructures and shape lives through deployments. Infrastructure building is about configuring and integrating components. Protocols and implementations aim to be flexible to support infrastructure building, leaving their material effects somewhat undetermined. Most end users meet technologies in the context of their life worlds, when those technologies are fully integrated into functional and performant infrastructures. A long line of scholarship in Science and Technology Studies has focused on how users "domesticate" technology, including making sense of technologies symbolically, and reconfiguring them materially (Oudshoorn and Pinch 2003).

There is a consensus amongst infrastructure scholars investigating the street level impact of technologies (Burrington 2016; Gabrys 2016; Mattern 2021) that innovative methodologies inspired by artistic research methods are needed to probe the nexus of users and infrastructures and articulate the public interest. The critical infrastructure lab used a prompt of our own design — an interactive sculpture evoking the behaviour of 5G antennas — to engage participants in conversations about communication infrastructures and the public interest (critical infrastructure lab 2023). The experiment resulted in 75 semi-structured interviews with visitors at the Central Public Library in Amsterdam. The findings show that rather than innovation in new features and capabilities, what users actually want from media infrastructures is usability and reliability, even to the detriment of efficiency. Conversely, what users do *not* want from media infrastructures is obscurity and breakdown, because they rely on infrastructures to get things done and to get by in an uncertain world.

In the context of the uncertain world, we found significant mistrust of media technologies amongst respondents. This is theorised by the Good Infrastructure Lab in Norway as *infrastructural doubt*, and identified as an emerging trend in users' sentiments towards media infrastructures (Berker 2023). Infrastructural doubt means that users are not convinced that the infrastructures they rely on in the context of their everyday lives (a) really do what they are advertised to do and (b) serve their interests. Mobile phones, wireless antennas, and become uncanny objects that haunt everyday lives.

The critical infrastructure lab has conducted infrastructure walks to investigate citizen perspectives on media and control infrastructures in the

context of the built environment. What we have learned from those walks with citizens, activists, policy makers and academics is that as a first step towards inscribing the public interest in media and control infrastructures, infrastructures should be *noticable*, *observable* and *contestable*. Noticable, so that users should be able to discern that they are used in a respective context. Observable, so that it should be possible to find out what they do and how they do it. Contestable, so that their deployment should be open to debate through democratic avenues. These three principles can inform protocol development and give flesh to the abstract notion of the public interest as it is advocated by the critical infrastructure lab.

What we called the three principles for public interest infrastructures *noticable*, *observable* and *contestable*, but they are infrastructural effects that can be the subject of advocacy, standardisation, implementation and deployment. In the next section, we spell out what we mean by infrastructural effects.

---

03 The last few years saw infrastructure policy shifting towards interventions in infrastructures to further wider policy goals, which can be called "policy *as* infrastructure", away from the baseline case of "policy *for* infrastructure" (Jansen, Oever, and al 2023). This has increased the importance of both infrastructures and infrastructure policies in politics. The critical infrastructure lab answers to this shift through research into the politics of infrastructure.↩

04 The Sovereign Tech Fund supports implementations of the OpenBGP, OpenPGP, and Wireguard protocols for routing, encryption/authentication, and building virtual private networks (VPNs), respecively.↩

2 Infrastructural ideologies and subject production

2.1 *Infrastructural effects*

…are how power is exercised through standards and protocols.

Infrastructures shape the action possibilities of their users by offering specific choices and constraining many others. These can be material constraints when "the computer says no" or the antenna is too high up to reach. But it is naive to stage infrastructural power as a meeting between an individual user and a technological artefact. Media and control infrastructures are environments that mostly work under, above, and behind the backs of users. For instance, Internet connectivity in work places is often successfully provided in ways that allow users to forget about the standards, implementations, and deployed infrastructure. The strongest and most often cited infrastructural effect is thus the invisibility of the infrastructure (Star and Bowker 2006).

The invisibility of infrastructure also entails that the infrastructural effects through which power is exercised through standards and protocols function on the scale and scope of populations rather than individuals. The corollary is that citizens' invividual experience with and within these media environments is a necessary but not sufficient guide to understand the power and politics at play. This is a problem for articulating the public interest, where civil society can do its part. Civil society can identify issues, frame them as a controversy and going public with them, engage with technology makers (through industrial fora and standardisation processes) and policy makers (through democratic processes and policy advocacy).

Sometimes, though, infrastructure can expose itself without help from civil society. Infrastructure becomes visible when it breaks down. To return to the experience of using the internet in a work place, access to internet connectivity in public spaces such as libraries or train stations still requires users to consider and engage with the underlying infrastructure. The ubiquituos solution of the captive portal sits uneasily in the context of the contemporary digital media environment, bolted on the top of standard access infrastructure. Captive portals are largely incompatible with current access provision infrastructures, standard operating systems, network manager software, and ultimately with the protocols that provide the underlying connectivity. The reason is simple and it is in fact one of the main claims of this report. Identity provision is an unresolved question within the network paradigm of open internetworking (the missing layer, if you will). Thus, users need to reach for their mobile phones to interface a laptop with the library network that provides Internet access. In doing so, they hark back to a different network paradigm: to cellular mobile networks, which have standard and interoperable ways to handle identity provision.

This is why it is useful to make an analytical distinction between the various network paradigms in play within contemporary media and control infrastructures, and thus they are the suject of the next section.

2.2 *Network paradigms*

...are a totality of infrastructural effects.

Network paradigms are few and far between in the history of technology. It takes a quasi-hegemonic position in the world system to propose, produce and impose a network paradigm on a planetary scale, as it has been happening with the telegraph, the Internet, mobile telecommunications and smart networks like 5G. Even central economies in the global division of labour need political will, concentrated effort and ripe historical conditions to successfully introduce a network paradigm.

We identify three network paradigms in the longitudial study of chapter 3. As artefacts, network paradigms reflect the times, spaces and peoples that produce them. The engineers, policy makers and advocates that work on communication protocols and other standard elements of media infrastructures that are destined to become part and parcel of a network paradigm in the future are not necessarily aware of all the factors they work into the standards and protocols that they produce. Nor such awareness is necessary for successful the standardisation of communication protocols. That is because they are always already immersed in their own culture and routinely keep their own interests in mind. Identifying and analysing network paradigms therefore involves shedding light on the unquestioned assumptons, cultural logics, political principles and political-economic realities that served as a backdrop for the production process.

Infrastructural effects exert power in the here and now and can be potentially configured at the deployment stage of an infrastructure. Network paradigms constitute a totality of infrastructural effects, including the means through which infrastructural effects can be configured. As such, network paradigms inhabit longer time scales and change incrementally. A particularly pertinent consequence is that once one has been established, there is no guarantee that it will continue to serve its masters infinitely. For instance, openness as as it has been inscribed into the Internet protocols may have served US interests at the time, when it has been US capital that was in the best position to compete on the global market the protocols supported. Today, such openness might serve the interest of ascendant capitalist eclasses in East Asia that are now competitive with the US IT industry. Yet, even the US cannot change the network paradigm of open internetworking in order to correct course. The geopolitical power struggle has to play out on the grounds of the current emergent network paradigm (smart networks). What the US can do is to regulate deployment to reconfigure network effects, such as by issueing calls to “rip and replace” Huawei mobile communication hardware.

We show in chapter 4 in a cross-sectional study of identity protocols that specific communication protocols — used on the Internet, in mobile telecommunications, or in smart networks — hark back to specific network paradigms that serve to frame them. Network paradigms provide frameworks for protocol development and come with their own ideological committments. The next section concentrates on unpacking the ideological character of infrastructures, and why it is useful to consider infrastructural ideologies in policy work.

2.3. *Infrastructural ideologies*

…justify and legitimise the adoption and imposition of network paradigms.

Geopolitical hegemony in the world system is held through control over territory, capital and technology: three variables that intersect in global telecommunications networks (Zajácz 2019). Studies examined the role of telecommunications in geopolitical power struggles, how power shapes technology and how technology is used to exert power. Here, we look at how culture shapes technology shapes power.

Ideology is a useful term to theorise the power and politics of programmable infrastructures because it implies that infrastructures serve particular interests, and accounts for how they serve those interests. While our focus is on the exercise of power through technology, and how technology shapes power itself, in the subsequent chapters we account for the role of the territory and capital in that process. In particular, we develop the claims over the subsequent chapters that the identity provisioned through standard communication protocols is either meagre, or anchored in sovereignty — usually the sovereignty over a territory. What this means is that strong digital identity provision is ultimately based on government-issued identification.

We use the term infrastructural ideologies to refer to the justification and legitimation of imposing, or adopting network paradigms and their respective infrastructural effects within territories, populations and by users. Infrastructural ideology is a means of (a) enrolling people as users of infrastructures (with or without their informed consent), (b) empowering them to benefit from the infrastructural effects and media affordances granted by said infrastructures, and (c) exercising power over them by shaping and denying their action possibilities through design. More broadly, we argue that infrastructures produce their users, and they do so because of their ideological character. Infrastructures, as all media, organise space and time in particular ways that yield affordances to users, but also shape their action possibilities in non-obvious ways.

All ideologies make misleading promises to users in response to users' demand, promises that ideologies undermine while implementing them (Boltanski and Chiapello 2005; Hess 2005). However, since standards and protocols define rules for interoperability, they integrate deeply with media and control infrastructures, so that their infrastructural effects rely less on persuasion and more or material performance. In this sense, infrastructural ideologies can be positioned somewhere between the ideological state apparati identified by Althusser such as the school, the church and the family, on the one hand, and direct physical dominance legitimised by states' monopoly on violence such as the police, the prison and ultimately

the army, on the other hand. This will be an important point in the following two chapters. In the following Chapter 3 we show the kind of subjects that network paradigms produce. In the subsequent Chapter 5, we take a closer look at standards and protocols that have been specifically developed for identity provision, and connect identity provision to the production of subjects.

3 Longitudial study: Network paradigms

3.1 *Internet: open internetworking*

...where users identify with specific computers.

The US could design a new network paradigm at the historical moment after the collapse of the USSR through taking advantage of its hegemonic position in the world system. The ideology of openness has its roots in the 19th century, when Open Doors was a trade doctrine devised for China that the US pursued as an alternative to colonialism (Russell 2014, 8), aiming for a "world open to American ideas and influence" (Williams Appleman 1978) – a form of economic imperialism. During the Cold War, US propaganda framed the Soviet Block as a closed world, while the Western side of the iron curtain has been pronounced the free and open world. Since Neoliberalism was enacted into policy in the 1980s, it justified opening markets to US capital. The Internet cemented the US' superpower status for the next decades, showcased its cultural and technological leadership, and provided a funnel for US capital to pump revenues from open markets.

Internet standards are called "open standards", and they are produced by a whole new set of dedicated international standards and governance bodies. These include the Internet Engineering Task Force that issues the RFCs mentioned in section 1.2, including the specifications for the Internet Protocol and the Transmission Control Protocol (TCP/IP). Another key player is the World Wide Web Consortium, whose flagship standards are widely recognised as the Hypertext Transfer Protocol (HTTP) and the Hypertext Markup Language (HTML). The major governance body whose work is essential for Internet standards and protocols to operate is the Internet Corporation for Assigned Names and Numbers (ICANN), which manages rules for allocating IP addresses and domain names for the Domain Name System (DNS) that connects names such as `criticalinfralab.net` to IP addresses such as `195.190.28.231`.

What should be emphasised is that in the late 1980s and early 1990s the Internet — as a project initiated by the US Defence Advanced Research Projects Agency (DARPA) — had enough traction to sideline parallel efforts within the International Standardisation Organisation (ISO) and establish its dedicated standards bodies instead of participating in existing industrial standards organisations such as the ISO or the ITU. We ascribe this to the unparalleled central position of the US at the time in the global division of labour and the world system. The take-away is that a new network paradigm emerges in specific historical moments, under specific historical conditions, and bears the mark of the hegemonic cultural, technological, and political movements of those times.

The Internet Protocol and the Transmission Control Protocol (TCP/IP) are often singled out as representative of the design philosophy of the whole

protocol suite. As their names suggest, the Internet Protocol is responsible for addressing and routing, while the Transmission Control Protocol is responsible for data transfer. The focus of the analysis in this section is the Internet Protocol and the way it establishes a context for the whole stack of protocols in operation on the Internet. Choosing the IP protocol as an entry points is in line with the mandate of this report to investigate questions of identity provision.

The Internet Protocol identifies nodes in the network and works in conjunctions with other protocols such as the Border Gateway Protocol (BGP) to define topologies that are planetary in scale. IP addresses are 32-bit numbers that identify nodes on the network and interfaces on computers. Much has been made of the fact that IP addresses do not systematically map onto geographical boundaries, and the protocol does not account for national borders in any shape or form, fuelling imaginaries of immateriality (Peters 2015) and cyber-autonomism (Gerbaudo 2017). Chenou (2014) even argues that the creation of a separate set of standards bodies was legitimised by "Internet exceptionalism", the belief that the Internet constitutes its a separate realm, a virtual world.

Internet users get an IP address when they connect to the Internet, but on IP version 4 networks this is usually a local address, and often a temporary one. A router serves as a gateway, mediating between the global internet and the computers on the local network using a technique called Network Address Translation (NAT). The gateway can be part of a another local network, or it can be directly on the global Internet. It is the address of the global gateway that is visible to other computers and networks on the global Internet. Thus, the NAT mediates between the local and global contexts, hiding users in the process. A crucial side effect is that the IP of the end user is not trivial to discern, only their origin network. The IP address is, therefore, a poor indication of user identity.

IP addresses are mapped to geography through governance mechanisms that have little basis in the materiality of the protocol, and still disregard the borders between nation states. The distribution and assignment of global IP addresses is governed on a continental basis by Regional Internet registries, organisations such as RIPE NCC for Europe, Middle East and Central Asia. IP addresses are tied to legal entities and remain assigned to them for long periods of time. This system allows coordination between Internet operators and the possible assignment of responsibility for network traffic to said operators. Yet, for the reasons mentioned above, IP addresses map topology to topography rather poorly. They do not readily translate either to national borders or to user identities, even though they span nations and allow users to participate in global data interconnection.

Thus, users end up identifying themselves on the Application layer, which sits on the top of the protocol stack. The subject position is a neoliberal subjectivity operating in a borderless world of the free market. It is the expression of the US world view where the medium of globalisation is the market of goods and services, where anybody can participate. The political economical reality behind the neoliberal ideology of open

internetworking is that US capital is in the best position (topologically and financially) to take advantage of the opportunities offered by such a freedom. There is a (market) competition between identity providers and services where, according to the ideology, the user is empowered to make choices about their dependencies. In practice, users are thrown in the context of a fractured spaces where they become what French philosopher Gilles Deleuze calls *dividuals* — schizophrenic subjects identified by passwords that grant them access or deny them certain services, spaces and time affordances. The life world of Internet identities is a specific expression of the "open and free world" that is the foreign policy goal pursued by the United States towards the end of the Cold War, and certainly after the fall of the Berlin wall. In conclusion, this is a subject position under the sovereignty of a global superpower propelled by a liberal ideology.

3.2 *GSM: mobile cellular networks*

...where Users identify with the network.

European telecommunications firms — the so-called "national champions"[5] led the contribution of a new network paradigm in the 1990s and early 2000s. Supported by the US through the Marshall plan, Europe has been rebuilt following the Second World War and after the fall of the Berlin wall European economies re-integrated into the global division of labour. Internally, European integration was achieved first through the European Economic Community (1957), and then through the European Union (1993). The tension between a relatively advanced economic union and a more limited political union continued to plague the emergence of a new superpower.

The ideology of mobile cellular networks also a contradiction in terms. The promise of mobility through radio communications is limited by "roaming", which involves switching between carrier networks internationally.[6] Compared to the Internet, mobile phone protocols and their network topologies are very much aware of the national boundaries within which carriers operate. As if the foundational contradictions of the European Union were cast into protocols. The single market works through well-defined interfaces of interoperability, which are bolted on the top of national infrastructures to ensure compatibility. Yet, each carrier network should retain its sovereignty in terms of control over its users, even if telecommunications service providers thrive to present a single unified infrastructure towards those users. Globally, the ownership structures of national telecommunications providers in the Majority World reflects the colonial heritage, so that French telecommunications companies would own subsidiaries in French-speaking ex-colonies.

Taking a page out of the political history of the standardisation of Internet protocols, mobile phone protocols have also been standardised by a complete set of new standards bodies and governed by dedicated international organisations. These include the European Telecommunication Standards Institute (ETSI, headquartered in France), the Global Standard for Mobile Communications Association (GSMA, headquartered in the UK)[7], and later Third Generation Partnership 3GPP (also headquartered in France). The odd-one out is the role of the International Telecommunications Union, one of the oldest international organisations,[8], which sets broad requirements for each generation of mobile phone protocol stack, in terms of both functional features and performance metrics. We come back to the role of the ITU in the next section. Here, it is enough to note that as we know from Russell's (2014) account, computer engineers working on Internet protocols avoided

working with the ITU already because of the dominance of telecommunications engineers in the organisation.

The naming of the first standardised mobile phone protocol stack already showed European ambitions: Global System for Mobile Communications (GSM). Mobile phone protocols are developed in subsequent generations in order to coordinate carrier companies rebuilding their radio access networks periodically. Switching between generations often involves replacing antennas and licencing new frequency bands. Post-GSM protocol suites have been called by different names such as Universal Mobile Telecommunications System (UMTS) and then Long-Term Evolution (LTE), also called 4G. In order to develop an argument about sovereignty and identity, the further analysis is limited to the general scheme of establishing a network connection, which works similarly across the various generations of mobile phone protocol stacks, starting with GSM.

As all mobile phone users know, telecom users are distinguished from each other through a mobile phone number. The composition of the mobile phone numbers shows the influence of methodological nationalism and the limitations of the promise of mobility. Mobile phone numbers start with a country code identifying where the mobile phone subscription have been set up, followed by a second number that identifies the mobile phone provider within that country. As mentioned above, roaming between countries and carriers remain an issue in many cases even within the European single market, which shows that roaming solutions are a problematic part of the protocol stack. Mobility as an ideological promise is implemented first and foremost as the mobility within a carriers' network and a country's borders.

In the course of establishing a network connection between a mobile phone and a cell tower, three unique identifiers are determined. First, an International Mobile Equipment Identity (IMEI) number is sent by the phone, which is globally unique for each piece of mobile phone equipment. Second, an International Mobile Suscriber Identity (IMSI) number is also communicated, stored on the SIM card of the mobile phone and sent to the radio access network as part of setting up the connection. Third, the phone number of the user is established. This initial part of configuring the connectivity is traditionally called the "billing" phase of the operation, implying that the user is identified for billing purposes. The end user can make a call or receive an SMS only after the billing information is validated.

The digital identity of the end-user is thus established against pretty strong factors compared to the Internet protocol. The hardware device itself is identified to see whether it is allowed to interface with the carrier's network. A physical token, the SIM card is used to identify the user. The subscriber number is tied to a contract established within the legal jurisdiction of a particular nation state. In some countries getting a SIM card and setting up a contract requires the presentation of a state-issued identification document. Mobile networks offer a strong identity rooted in physical material properties provisioned by the industry, and ultimately a legal infrastructure provided by the state. While Internet users identify with

particular applications on the Application Layer, cellular users identify with the network itself on the Data Layer.

The convergence of mobile telecommunications with Internet-based services is partly motivated by the fact that mobile phone operators capitalise on connectivity, but they cannot turn on a profit on the services running on top of the network. The End-to-End principle of the Internet protocol suite discourages interference with packets transmitted over the more recent generations of cellular protocols infrastructures, and anti-trust legislations in various countries make it difficult for mobile phone providers to move into digital services on the Application Layer.

Silicon Valley capital is therefore able to make the most of the infrastructure operated by telecommunications companies. A case in point is digital identity provision, where Application Layer log-ins to Internet-based platforms are secured through automated phone calls and SMS services. As noted in section 1.2, this shows the limitations of both the Internet protocol suite and the cellular networks: one cannot give strong guarantees for the identification of its users, while the other cannot pass on identification information without user interaction to the Application Layer services.

In summary, the subject position harks back to the Westphalian sovereignty of European nation states and the articulated through their *national champions*. These *national champions* are telecommunication companies that are quasi-state-sanctioned monopolies at the time GSM is design and continue to be big players in their respective telecommunication markets after the liberalisation of those markets. Even if the flagship promise of the GSM communication protocol is mobility, such mobility is conceived across national borders. Users get an identity from the network, and such identity is a number prefixed by the number assigned to the nation state where the users' contract is anchored. Cross-border mobility is called *roaming*, and this word points to the specific problem of mediating connectivity from one sovereign territory to the other. Correspondingly, the phone number is linked to the materiality of the mobile phone through the IMEI, the identity given to that piece of hardware by the IMSI number, and the contractual relation between a legal person (citizen or company) and the communication provider. It is good to remember that these aspects are handled more loosely by TCP/IP and Internet providers.

---

05 While Nokia and Ericsson stand out as vendors of network equipment and solutions, national service providers in major European economies contributed significantly to mobile phone standards.↩

06 A similar problem exists in the local context where it is called "handover": switching between eponymous cells of the network, which are the areas assigned for coverage by particular antennas on cell towers.↩

07 Originally called Groupe Spécial Mobile.↩

08 Originally called International Telecom Union.↩

3.3 *5G: smart networks*

...where users identify with a combination of the network and the computers.

Smart networks refer to a whole new set of technologies, standards and protocols that open up market segments such as software-defined networking, Internet of Things, and edge computing. While these industry buzzwords are loosely defined, 5G infrastructures are actually existing applications of those ideas, based on a standardised protocol suite. Our assumption is that the convergence of networking and computing that we see in 5G networks and theorise as *programmable infrastructures* constitutes a new network paradigm of its own.

The market leader in developing, manufacturing, deploying and operating cost-effective and performant 5G infrastructures is Huawei, a national champion for Chinese telecommunications. For this reason, 5G is widely seen by politicians, industrialists and analysts as an important component in a Chinese big for the status of global superpower. Other firms across Asia are also important 5G vendors, replicating the structure of US dominance in the operation of Internet infrastructures and the strong role of European national champions in mobile telecommunications and cellular networks.[9] China switched from a "Make in China" to a "Created in China" policy, which included generous government subsidies for technology development. Just like in the case of the Internet and GSM, developing a new network paradigm comes at a high cost that requires coordination between industry and state funding.

Chinese actors did attempt to create new standards bodies (3GPP2, 1998-2023) and protocol suits (new IP, 2018-2020) previously, but these attempts were hampered in a standards policy space where China had little experience. Subsequently, Chinese efforts switched to established standards bodies and targeted the new generation mobile phone protocols. The China Communications Standards Association (CSSA), founded in 2002, joined the 3GPP in 2004. By 2018, Chinese members signed for 40% of research items related to 5G standardisation, with from the telecommunications vendor Huawei and the national champion phone company China Mobile presenting the first 5G access point on the market in the same year (Shijia and Jun 2018; Jones 2018). According to industry analysis, "Huawei submitted the most contributions to 3GPP for 5G by a considerable margin (19,473), followed by Ericsson (15,072)" in 2019, and by 2021 the firm lead in terms of *approved* contributions too (Bruer and Brake 2021, 17; IPlytics 2019, 9; 2021, 7).

The cultural impact of a potential Chinese network paradigm remains a question to investigate. What can be discerned from current developments is that the advance on 5G fits into a "new grant strategy" (Wang 2016)

epitomised by the Belt and Road initiative of infrastructural projects including along a logistical corridor connecting the country to Europe across Asia by land and sea (Huang 2016). While cultural imperialism has been a cornerstone of US strategies, and European expansion went hand in hand with exporting European values, the Chinese strategy is about building infrastructural power through creating supply chain dependencies and efficiencies.

Each network paradigm presents an order of magnitude more complexity for engineers and analysts than the previous one, and smart networks are no exception to this rule. 5G standards target three application areas that have separate feature and performance requirements. Enhanced Mobile Broadband (eMBB) is the application area that is replacing the functionality of 4G networks, enabling Internet connection, voice calls and messaging for end users. Ultra-Reliable Low-Latency Communications (URLLC) is for mission-critical applications, including latency and availability guarantees. Massive Machine-Type Communications (mMTC) provides the infrastructural base for the Internet of Things, enabling drones, autonomous vehicles, and factory automation. Differently than in the case of the previous network paradigms, 5G standards and protocols are developed for specific applications and problem domains in communications and control. However, the programmability of the infrastructure and the direct access of the network to substantial computing power also provides flexibility for reconfiguring the infrastructure in real time for specific use cases serving specific users.

An example of the flexibility of 5G networks is in making full use of IPv6 features, which allows multiple addresses assigned to end user devices, defining several overlapping contexts of different scale and scope. In section 1.1 we introduced the claim before that the version 4 Internet Protocol addresses are either local or global in scope, presenting a smooth open space for market interactions. In section 1.2 the claim was that GSM protocols allow mobility within a particular cell around an antenna, and between national networks, dividing the territory to largely adjacent zones. In 5G networks the end user device can operate on the neighbourhood level within a cell, for instance for the purpose of delivering cached content like popular TV shows from an edge computing server coupled to the cell tower. Concurrently, it can operate in a national context for transmitting personal data that should stay inside a particular jurisdiction, or on a global scale for online retail transactions.

For the sake of the argument, we focus on the idea of *"verticals"* in the subsequent discussion. Verticals provide services to external parties, and especially services that draw on functionality and information residing on several different layers of the 5G protocol stack. It is the operators of the telecommunications infrastructure who would be in a position to deliver such services, perhaps in cooperation with other actors. Verticals may become interesting for providing services for digital identity provision. Telecommunication companies have the opportunity to *expose* the GSM-based user identities as a specific service to partner companies and end

users, thus becoming players in the identity provider market. As analysts of the consulting firm Deloitte put it,

> *"[c]arriers could also negotiate solutions that help share data from the billions of devices from various companies and sectors that reside on their network to strengthen the investment case for 5G." (Deloitte 2018, 9)*

This is a possible revenue stream offered by their strategic switch from providing connectivity — in line with the concept of net neutrality — to participating in the platform market of digital services. Identity provision would be but one of these "vertical" data-based services that could be provided on smart networks. What makes identity provision interesting is that — as seen in the previous section (3.2) — carriers have privileges access to strongly anchored user identities that no other player can muster. As noted in the same Deloitte report (8), Internet Service Providers and telecommunications companies missed out on the profit derived from the platform market of digital services in the context of previous network paradigms, all the while they provided the underlying connectivity for that market to function. This is their moment of revenge.

---

09 Positions that are also eroding since these power blocks established a network paradigm of their own conception.↩

4. Cross-sectional study: Identity protocols

4.1. *OpenID: open interoperability*

xri://example.org/username/(=!CanonicalID)/(@!ProviderID)

The first case study is about OpenID, a decentalised authentication protocol defined as an open standard for single sign-on. Users are offered to create an account with an OpenID provider, and the account can be re-used for logging in to other web services that support the OpenID standard. A minimal example of an OpenID identifier string is is displayed above this paragraph.

ProviderID and CanonicalID in the above Universal Resource Identifier are a name and number that point to the organisation providing the identity. Relying parties accept this identity through the protocol as a valid login method. OpenID users have to trust their OpenID providers: the protocol itself gives no assurances about the trustworthyness of a provider. Web services that accept OpenID may have ways to validate the behaviour of an OpenID provider, and block malicious providers.

OpenID is backed by the OpenID Foundation, a standards and governance body open to individual, corporate and government agency membership. Eight corporate members and six community members make up its board. In practice, OpenID participants and board members are drawn from the ranks of the industry: the major players in digital service provision or firms whose core business is in identity management.[10]

In the typology proposed in Chapter 3, the OpenID protocol is situated in the context of open internetworking. OpenID provision is an open market where any organisation can offer their services. The catch is that in practice it is US Silicon Valley capital — the platform monopolies — that is best placed to leverage the opportunities offered by the interoperability offered by this decentralised protocol. Alexander Galloway has identified this way of operation as a neoliberal model of social control in a book aptly titled *Protocol: How Control Exists After Decentralization* (2004).

The declining popularity of the protocol with end users led to many relying parties who accepted OpenID logins in the past this login option. The most popular single sign-on methods today are provided by Google's and Facebook's APIs. Users tend to be always already authenticated with one of the platform monopolies. The general trend is identified by Helmond (2015) as the platformisation of the web, whereas open standards and protocols are replaced by proprietary APIs under monopoly control.

The limitations of OpenID can scarcely be written down to its technical inadequacy. On the one hand, OpenID yields a lightweight identity by design, which cannot be used to access financial, legal or government services. On the other hand, proprietary alternatives run by platform monopolies excel in adoption by relying on the network effects in multi-sided markets. The moral of the story is that OpenID is a limited solution for

digital identity provision because it is unclear how it is backed up by a sovereign power, be that a nation state or a platform monopoly (Bratton 2015).

---

10 Board members are listed on the website: https://openid.net/foundation/board/.↩

4.2. *Aadhaar: sovereign interoperability*

6622-2350-9284

The second case study is about Aadhaar, a proof of residence managed by the Unique Identification Authority of India (UIDAI). As seen above, the identification is a simple twelve digit number. The number also comes printed on a card that includes additional information like a photograph and the basic personal details of the subject. Users' biometric data such as iris scans and fingerprints are attached to their digital file. Aadhaar is used for both authentication and authorisation to access government subsidies, apply for loans, acquire a SIM card, make online payments (O'Hara and Hall 2021, 190–93). It functions in a larger API framework dubbed the India Stack, taking clues from the open-source movement and open standards such as the OpenID discussed in the previous section.

A significant limitation of the system is that it is only useful in the Indian context. While India is exporting the technology itself, cross-national interoperability understandably remains a low priority. This identification protocol is closely coupled to the territory of national sovereignty. This is in stark contrast with OpenID, where it has been an unquestioned assumption that the technology will work in a borderless world and serve a global market dominated by US firms.

Therefore, we argue that Aadhaar shares its assumptions with the network paradigm of cellular mobility, even if in this case it is perhaps social mobility that is the key promise of the technology. Be it as it may, the price to pay is social control, since the identification offered by Aadhaar is strongly anchored in materiality, biology and legal provisions. The limitation to the territory, and through the territory, the anchor in state sovereignty, makes Aadhaar a very powerful identification solution, for better or worse. Aadhaar's interoperability is conceived within the limited perimeter of a national network just like with the GSM protocol. For the same reason, Aadhaar has been criticised for allowing promiscuous access for the public and private section to the personal information of users, a criticism upheld by the Supreme Court (Bhatia 2019).

Even though the Supreme Court also ruled that nobody can be denied their rights because of the lack of a unique ID, it seems increasingly difficult to get by without one, and a matching mobile phone. Indeed, it has been developed with a population in mind where mobile phone adoption is far ahead of the adoption of personal computers. In this capacity, the system both overcame and entrenched the digital divide. It increased access for those who manage to benefit from the system, while also increased the exclusion of those for whom the infrastructure does not work, for whatever reason. As a successful infrastructural ideology, Aadhaar might have empowered citizens, but also increased the hold of the state over their lives.

5 Strategic outlook in protocols and identities

5.1 *Summary of findings*

Identity protocols are as powerful as the sovereignty backing them. Protocol design can tie a digital identity to lower protocol layers in the stack, and through the lower layers to materiality outside the digital realm, and through such materiality, to the territory, and through the territory, to the sovereignty of the state. Design choices are political in so far as they negotiate the tradeoff between a strong identity giving more power over the user to the operators, or a weak identity that is practically less useful to its end users.

In the case of the Internet, the identity provisioned by the network ideology of open internetworking conceived the world as an open market of permissionless participationa and innovation. This has led to a fragmented identity landscape where users identify with the many particular computers connected to the network. Service providers such as Google, Apple, Facebook, Amazon and Microsoft (GAFAM) in the US arguably opted for advancing their own platform sovereignty in order to produce relatively strong user identities. Identification happens on the Application Layer where each service provider is left to their own device to provision identities.

OpenID fits into the network paradigm of open internetworking becasuse it provides a lightweight identity that any actor on the open market can offer. In this capacity, it is not designed or intended to address the need for a powerful identity provision that would make it really useful for the most important things people need to get done in their lives. Failing that, its decentralised model is outcompeted by the platform monopolies that can provision an equivalent lightweight identity and take advantage of their monopolies for adoption.

In the case of mobile telecommunications, the communication protocol stack has been developed and it is managed by national champions that offer mobility within national borders in exchange for strong identity provision. Devices, SIM cards, and subscriber contracts are identified at the moment when connection is established with the network, so that users identify directly with the network itself. The identity provision is a powerful one that we can observe actors working within the open internetworking paradigm to reach out to in order to identify their users, through SMS and phone calls. These replace the Internet-native email mailbox as the anchor of user identity. However, telecommunications corporations cannot expose the low-level identification behind making phone calls and sending text messages as a service that can be reused by third parties.

Aadhar follows the pattern of cellular mobility, aiming for a powerful identity provision backed up by state sovereignty, and consequently it is

limited to the perimeter of the national context by design. The powerful identity Aadhaar provides is tied to the materiality of the human body through biometrics, in addition to SIM cards and legal frameworks provided by the state. While many citizens benefit from a strong digital identity, the public interest is at jeopardy when different kinds of anchors for identity and personal information from various sources is pooled to the same database without appropriate access control guarantees. Furthermore, for those for whom Aaadhar does not work, it itself becomes a barrier for access to essential public and private services.

In the case of smart networks, we observe a convergence between the computers with which Internet users identify with, and the networks that mobile phone users identify with. The convergence makes it possible for carriers to expose strong user identities that are established at a very low level of the protocol stack, in the Data Layer, as a business-to-business service that can become available to third parties providing user-facing services on the Application Layer. The combination yields relatively powerful identities that are potentially operative on a planetary scale, transcending the territorial limitations of sovereign power.

5.2 *Strategic outlook*

We argued that the proposition and imposition of interoperable protocols and standards – for communication interconnection or digital identity provision — hinges on the question of sovereignty. Users who are immersed in these media and control environments subject themselves to power structures larger than themselves. Consequently, it is a crucial question *what kind of powers should provision communication protocols and identity standards so that those infrastructures would best serve the public interest?*

We demonstrated that in the case of the Internet, it was the US who was in a position to propose and impose a new network paradigm at the time and the infrastructural ideology of open internetworking has been based on US foreign policy doctrines. The industrial consortium behind OpenID could not reach its goal for the wide adoption of its identity provision standard, and even though the design goals of the protocol has been limited. The next network paradigm has been advanced by European national champions who opted for a stronger identification regime in the new communication protocol stack, inspired by the political experience and economic reality of the European single market and community. This has achieved limited success because interoperability was constrained by the identity being readily available only to the carriers themselves, and seamless mobility has been achieved by the design only within a single carrier network.

The Indian state efficiently backed and rolled out Aaadhaar, a national digital identity system that provides strong identification by design, and can be used by third parties, which presented its own set of challenges. The network paradigm of smart networks, epitomised by 5G, promises a flexible vertical integration between different functions of the protocol stack, which would allow strong low-level identities to be exposed to third parties in the form of a business-to-business service. Such programmable infrastructures are currently backed by Chinese political ambitions, manufacturing capacity and engineering prowess. 5G networks are thus an element in an overarching geopolitical strategy through which the country pursues to project its power infrastructurally, as in the wider Belt and Road initiative.

The UN Sustainable Development Goals include the recommendation for nation states to provide citizens unique digital identities by 2030. Who and how will propose and impose the communication protocols and identity standards that make that possible remains to be seen. Policy advocates may consider whether a strong digital identity backed by low-level identification on the protocol level and powerful sovereignty on the political level is a desirable outcome. Is it good for citizens and non-citizens to be unambiguously identified? To what extent stable, rich, and powerful identities may serve the public interest? Can bodies be separated from the

sovereign territory, and can platform monopolies develop their own sovereignty vis-a-vis nation states? Alternatively, can self-sovereign identities and lightweight communication protocol designs be useful tools to advance the public interest? These questions point to the underlying problem of how best to distribute power in societies and on a planetary scale.

Therefore, instead of debating merely technical solutions and governance mechanisms, policy advocates may consider shaping the strategic terrain by building consituent powers that can shape those sovereign powers that impose and propose infrastructural ideologies. The much debated question of European technological sovereignty might boil down to the more pertinent question of European sovereignty proper. In order to navigate these conundrums, the key is to clarify the position of each sovereign power in the global division of labour, which yields a clearer picture of action possibilities.

5.3 *Policy recommendations*

The European Digital Decade Programme mandates the provision of a unique digital identity (eID) to everyone living in the EU by 2030. The technical specifications are being developed in the expert group called "electronic IDentification, Authentication and trust Services" (eIDAS). There is an ongoing formal consultation process through the EU's Futurium public participation platform, while civil society actors are monitoring the process. **11**

The eIDAS reform is a strategic point of engagement for European civil society in order to ensure that communication protocols and identity standards serve the public interest. Moreover, in light of the present report, the role of programmable infrastructures, specifically the next generation telecommunications networks, in the provision of interoperable digital identities, should be critically investigated. The possibilities for public scrutiny and public participation in standards processes should be expanded, from the standardisation of the 5G protocol stack to the eIDAS expert group for digital identity, but efforts best concentrate on the venues that provide the possibly best point of leverage for impact.

The nexus of 5G roll-out and digital identity provision is a crucial conjecture to monitor and engage. The potential concrete points for intervention are numerous. On the specific point of 5G roll-out, three promising levels of engagement can be identified:

1. A substantial amount of EU funding from the COVID-19 recovery fund was earmarked for projects advancing the development and deployment of 5G technologies in Europe. These funds subsidise industrial project with little or minimum impact assessment, civil society participation, or other public interest measures. They could potentially include all these in the light of high-level language enacted by the Commission about its approach to 5G and related technologies. National
2. National spectrum allocations and frequency auctions to support 5G roll-out provide another venue for advancing the public interest. These have been organised in most European countries as industry-facing processes without public participation or civil society engagement. As in the case of community radios, it can be argued that the electromagnetic spectrum is a critical natural resource (Herter Jr. 1985), so that civil society should be able to make use of them and the public interest should be safeguarded in their exploitation.
3. Municipal regulations also play a crucial role in the 5G roll-out. The street-level deployment of programmable infrastructures depends on the real estate licences handed out by the municipal authorities who preside over the public spaces where radio access networks are deployed.

Therefore, municipalities have a strategic role in setting the conditions for the introduction of the new network paradigm.

The general principles set out by the critical infrastructure lab for infrastructures to serve the public interest can serve as a guidance in engaging on these three levels. Infrastructures should be *noticable*, so that citizens should be aware that they are immersed in specific media and control environments. Moreover, infrastructures should be *observable*, so that citizens should be able to find out what programmable infrastructures do and how they work. Finally, infrastructures should be *contestable*, so that citizens should have a say in their introduction to the built environment and in their continued operation.

Beyond working upwards towards shaping power dynamics and policy making, broader civil society should work with social movements and rally around citizens' concerns in so far as these are crucial sites where the public interest is articulated.

Open Future and the critical infrastructure lab organised a roundtable debate in Amsterdam on June 20th, 2023, to debate the topics of the report.

11 For example, a number has issued an open letter in January 2023 to the European Parliament: https://epicenter.works/sites/default/files/open_letter_eidas_2023-01_0.pdf↩

References

Balbi, Gabriele, and Andreas Fickers. 2020. *History of the International Telecommunication Union (ITU): Transnational Techno-Diplomacy from the Telegraph to the Internet*. Oldenburg: de Gruyter.

Balzarova, Michaela A., and Pavel Castka. 2012. "Stakeholders' Influence and Contribution to Social Standards Development: The Case of Multiple Stakeholder Approach to ISO 26000 Development." *Journal of Business Ethics* 111 (2): 265–79. https://doi.org/10.1007/s10551-012-1206-9.

Berker, Thomas. 2023. "The Good Infrastructures Lab: User Agency Within, Through and Against Infrastructures." Presentation at the Launch Event of the Critical Infrastructure Lab, 14 April. https://www.criticalinfralab.net/2023/03/13/launch-event-programme/.

Berners-Lee, Tim, Roy T. Fielding, and Henrik Frystik Nielsen. 1996. "RFC 1945: Hypertext Transfer Protocol." Request for Comments. https://datatracker.ietf.org/doc/html/rfc1945.

Bhatia, Gautam. 2019. "Judicial Evasion and the Status Quo: On SC Judgments." The Hindu, 10 January. https://thehindu.com/opinion/lead/judicial-evasion-and-the-status-quo/article25953052.

Boltanski, Luc, and Eve Chiapello. 2005. *The New Spirit of Capitalism*. New York, NY: Verso.

Bratton, Benjamin H. 2015. *The Stack: On Software and Sovereignty*. Boston, MA: MIT Press.

Bruer, Alexandra, and Doug Brake. 2021. "Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy and Policy." Information Technology and Innovation Foundation. https://itif.org/publications/2021/11/08/mapping-international-5g-standards-landscape-and-how-it-impacts-us-strategy/.

Bryson, Joanna, and Alan Winfield. 2017. "Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems." *Computer* 50 (5): 116–19. https://doi.org/10.1109/MC.2017.154.

Burrington, Ingrid. 2016. *Networks of New York: An Illustrated Field Guide to Urban Internet Infrastructure*. Brooklyn, NY: Melville House. http://lifewinning.com/projects/networks-of-new-york/.

Carmin, JoAnn, Nicole Darnall, and Joao Mil-Homens. 2003. "Stakeholder Involvement in the Design of U.S. Voluntary Environmental Programs: Does Sponsorship Matter?" *Policy Studies Journal* 31 (4): 527–43. https://doi.org/10.1111/1541-0072.00041.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium* 43 (2): 640–59. https://doi.org/10.1177/0305829814562655.

Castka, Pavel, and Michaela A. Balzarova. 2008. "The Impact of ISO 9000 and ISO 14000 on Standardisation of Social Responsibility—an Inside Perspective." *International Journal of Production Economics*, Research and Applications in E-Commerce and Third-Party Logistics Management, 113 (1): 74–87. https://doi.org/10.1016/j.ijpe.2007.02.048.

Cath, Corinne. 2023. "Loud Men Talking Loudly: Exclusionary Culture of Internet Governance." critical infrastructure lab report. https://www.criticalinfralab.net/wp-content/uploads/2023/04/LoudMen-CorinneCath-CriticalInfraLab.pdf.

Chenou, Jean-Marie. 2014. "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s." *Globalizations* 11 (2): 205–23. https://doi.org/10.1080/14747731.2014.887387.

Cooper, Alissa, Hannes Tschofenig, Bernard Aboba, Jon Peterson, John Morris, Marit Hansen, and Rhys Smith. 2013. “RFC6973 - Privacy Considerations for Internet Protocols.” RFC Editor. https://tools.ietf.org/html/rfc6973.

critical infrastructure lab. 2023. “Exhibit.” Web page. https://www.criticalinfralab.net/exhibit/.

Deleuze, Gilles. 1992. “Postscript on the Societies of Control.” *October* 59: 3–7. http://www.jstor.org/stable/778828.

Deloitte. 2018. “5G: The Chance to Lead for a Decade.” Report. https://archive.org/details/5GAndConnectedCities.

Doty, Nick. 2015. “Reviewing for Privacy in Internet and Web Standard-Setting.” In *Security and Privacy Workshops (SPW), 2015 IEEE*, 185–92. IEEE.

Farrell, Joseph, and Garth Saloner. 1985. “Standardization, Compatibility, and Innovation.” *The RAND Journal of Economics* 16 (1): 70–83. https://doi.org/10.2307/2555589.

Gabrys, Jennifer. 2016. *Program Earth: Environmental Sensing Technology and the Making of a Computational Planet*. Minneapolis, MN: University of Minnesota Press.

Galloway, Alexander. 2004. *Protocol: How Control Exists After Decentralization*. Leonardo. Cambridge; London: MIT Press.

Gerbaudo, Paolo. 2017. “From Cyber-Autonomism to Cyber-Populism: An Ideological History of Digital Activism.” *tripleC: Communication, Capitalism & Critique* 15 (2). https://www.triple-c.at/index.php/tripleC/article/view/773.

Haggart, Blayne, Natasha Tusikov, and Jan Aart Scholte, eds. 2021. *Power and Authority in Internet Governance: Return of the State?* 1st edition. Abingdon: Routledge.

Hallstrom, Kristina Tamm, and Magnus Bostrom. 2010. *Transnational Multi-Stakeholder Standardization: Organizing Fragile Non-State Authority*. Cheltenham: Edward Elgar.

Healy, Maurice, and Nicholas Pope. 1996. “Consumer Representation in Standards Making.” In *Compendium from 3rd Annual EURAS Conference*, 1:95.

Helmond, Anne. 2015. “The Platformization of the Web: Making Web Data Platform Ready.” *Social Media + Society* 1 (2).

Herter Jr., Christian A. 1985. “The Electromagnetic Spectrum: A Critical Natural Resource.” *Natural Resources Journal* 25 (3): 651–63.

Hess, David J. 2005. “Technology- and Product-Oriented Movements: Approximating Social Movement Studies and STS.” *Science, Technology and Human Values* 30 (4): 515–35. https://doi.org/10.1177/0162243905276499.

Huang, Yiping. 2016. “Understanding China’s Belt & Road Initiative: Motivation, Framework and Assessment.” *China Economic Review* 40: 314--321. https://doi.org/OPTnote.

IPlytics. 2019. “Who Is Leading the 5G Patent Race? A Patent Landscape Analysis on Declared SEPs and Standards Contributions.” IPlytics report, November.

———. 2021. “Who Is Leading the 5G Patent Race? A Patent Landscape Analysis on Declared SEPs and Standards Contributions.” IPlytics report, February.

Jakobs, Kai, Rob Procter, and Robin Williams. 1996. “Users and Standardization—Worlds Apart? The Example of Electronic Mail.” *StandardView* 4 (4): 183–91.

Jansen, Fieke, Niels ten Oever, and Maxigas et al. 2023. “Building a Relational Infrastructure: The Launch of the Critical Infrastructure Lab.” critical infrastructure lab report. https://www.criticalinfralab.net/wp-content/uploads/2023/06/infralab-launch-report-2023-06-08.pdf.

Jones, Dan. 2018. “China Mobile Claims First 3GPP Standards 5G CPE.” LightReading. https://www.lightreading.com/mobile/5g/china-mobile-claims-first-3gpp-standard-5g-cpe/d/d-id/740908.

Mattern, Shannon. 2021. *A City Is Not a Computer: Other Urban Intelligences*. Princeton, NJ: Princeton University Press.

Napoli, Philip M. 2001. *Foundations of Communication Policy: Principles and Process in the Regulation of Electronic Media*. Communication Series. Cresshill, NJ: Hampton Press.

Nottingham, Mark. 2020. "RFC8890 - the Internet Is for End Users." RFC Editor. https://tools.ietf.org/html/rfc8890.

O'Hara, Kieron, and Wendy Hall. 2021. *Four Internets: Data, Geopolitics and the Governance of Cyberspace*. New York, NY: Oxford University Press.

Olson, Mancur. 1971. *The Logic of Collective Action: Public Goods and the Theory of Groups, Second Printing with a New Preface and Appendix*. Cambridge, MA: Harvard University Press. https://doi.org/10.2307/j.ctvjsf3ts.

Oudshoorn, Nelly, and Trevor Pinch, eds. 2003. *How Users Matter: The Co-Construction of Users and Technology*. Cambridge: MIT Press.

Perry, James, and Andreas Nöelke. 2005. "International Accounting Standard Setting: A Network Approach." *Business and Politics* 7 (3): 1–34. https://doi.org/10.2202/1469-3569.1136.

Peters. 2015. *The Marvelous Clouds: Towards a Philosophy of Elemental Media*. Chicago, IL: University of Chicago Press.

Russell, Andrew L. 2014. *Open Standards and the Digital Age: History, Ideology, and Networks*. 1st ed. Cambridge Studies in the Emergence of Global Enterprise. Cambridge: Cambridge University Press.

Scholte, Jan Aart. 2017. "Complex Hegemony: The IANA Transition in Global Internet Governance." Geneva, Switzerland. https://igf2017.sched.com/event/CRB7/the-12th-annual-symposium-of-the-global-internet-governance-academic-network-giganet.

Shijia, Ouyang, and Yang Jun. 2018. "China Joins Top Ranks in Field of 5G Technology." China Daily, March 13. https://www.chinadaily.com.cn/cndy/2018-03/13/content_35837731.htm.

SPRIND GmbH. 2023. "Sovereign Tech Fund." Web page. https://sovereigntechfund.de/en/.

Star, Susan Leigh, and Geoffrey C. Bowker. 2006. "How to Infrastructure." In *The Handbook of New Media*, edited by Leah A. Lievrouw and Sonia Livingstone, Updated Student Edition, 230–45. London: Sage.

Tang, Min. 2020. "Huawei Versus the United States? The Geopolitics of Exterritorial Internet Infrastructure." *International Journal of Communication* 14: 22.

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

Tiqqun. 2012. *The Cybernetic Hypothesis*. The Anarchist Library. http://theanarchistlibrary.org/library/tiqqun-the-cybernetic-hypothesis.

Wang, Yong. 2016. "Offensive for Defensive: The Belt and Road Initiative and China's New Grand Strategy." *The Pacific Review* 29 (3): 455–63. https://doi.org/10.1080/09512748.2016.1154690.

Williams Appleman, William. 1978. "Open Door Interpretation." In *Encyclopedia of American Foreign Policy*, edited by Alexander Deconde, vol. 2:703–10. New York, NY: Charles Scribner's Sons.

Yates, JoAnne, and Craig N. Murphy. 2019. *Engineering Rules: Global Standard Setting Since 1880*. Baltimore, MD: John Hopkins University Press.

Zajácz, Rita. 2019. *Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century*. Information Policy. Cambridge, MA: MIT Press.

critical
Infrastructure
lab