UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Infrastructural anxiety and digital sovereignty

The perceived loss of control in Dutch communication networks

Jansen, F.; ten Oever, N.; Vorndran, S.; Maxigas

DOI
10.5210/fm.v31i3.14530

Publication date
2026

Document Version
Final published version

Published in
First Monday

License
CC0

Link to publication

Citation for published version (APA):
Jansen, F., ten Oever, N., Vorndran, S., & Maxigas (2026). Infrastructural anxiety and digital sovereignty: The perceived loss of control in Dutch communication networks. *First Monday*, *31*(3). https://doi.org/10.5210/fm.v31i3.14530

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

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

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

Download date:13 Nov 2026

f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Infrastructural anxiety and digital sovereignty: The perceived loss of control in Dutch communication networks

by Fieke Jansen, Niels ten Oever, Sarah Vorndran, and Maxigas

Abstract

This paper examines how Dutch citizens and civil servants experience and respond to perceived loss of control over communication infrastructures. Combining a representative survey (*N*=2,154), 69 semi-structured interviews with 89 participants gathered around an art intervention, and seven elite interviews with civil servants, we develop the concept of infrastructural anxiety: a situated, anticipatory unease about infrastructural governance that encourages actors to externalize responsibility upward (from citizens to the state) and outward (from the state to market and standards fora). We show that data safety and security dominate public concerns, that citizens employ limited privacy tactics but feel unable to affect systemic change, and that civil servants view governance pathways as constrained by global standards and market concentration. In this mixed-method study, we straddle the fields of science and technology studies, media studies, and infrastructure studies to provide insights in the relation between citizens and technology and the state and technology, where these normally are researched in separation. We discuss theoretical implications for digital sovereignty and propose practical measures to better align citizen expectations with institutional capacities.

Contents

Introduction
Infrastructure, power, and sovereignty
Methods
Findings
Discussion
Conclusion

Introduction

Once celebrated for shrinking space and time (Postman, 1986), communication technologies are increasingly criticised for absorbing attention and reshaping everyday life (Crary, 2022). The debate about

technology, control, and power is by no means a new one, but it is reinvigorated through debates in academic and policy circles about digital sovereignty and industrial policy (Calderaro and Blumfelde, 2022; Flonk, *et al.*, 2024; ten Oever, *et al.*, 2024). Several authors have noted that policy debates about digital sovereignty are largely of a discursive, not material, nature (Baur, 2024; Lambach and Oppermann, 2022; Adler-Nissen and Eggeling, 2024). In this paper, we contribute to the understanding of digital sovereignty by moving beyond the seeming dichotomy of the discursive and the material and explore how citizens and civil servants in the Netherlands experience their ability to exercise control over communication infrastructures and how this experience is shaping their actions. The relationship between citizens, the state, and technologies is regularly assessed along different axes, instead of tracing and connecting them. To more profoundly understand the dynamics that emerge when global infrastructures meet a local context of state institutions and private citizens, we look at the sum of the relationships. This broader lens illustrates how citizens engage with infrastructures through individual experiences and tactics, whereas the government responds strategically to structural social, political, and economic challenges through a market-based policy agenda. Despite the differences, a dynamic materializes at all levels of society that we characterize as infrastructural anxiety; where subjects experience an increased sense of loss of control and respond with the externalization of responsibility to third parties.

In this paper, we explore the relation between citizens, civil servants, and communication infrastructures within the Dutch context. Since the advent of the Internet, the Netherlands has occupied a disproportionately influential place in the operation and governance of communication infrastructures. In 1988, the Dutch Center for Mathematics and Informatics (CWI) gained early access to the NSFnet in the United States and in 1989, the first (and still functioning) Regional Internet Registry, Réseaux IP Européens, was established in Amsterdam. Subsequently, other academic and research institutions were connected and in 1993 could dial into bulletin board systems such as De Digitale Stad (The Digital City) and get connected to the Internet service provider XS4ALL. The increasing need for interconnection led to the establishment of the Amsterdam Internet Exchange (AMS-IX) in 1994. Bolstering a lively community of pioneers who contributed to the development of the stack and the rollout of the commercial Internet. High penetration of land and later mobile Internet connections propelled the Dutch population to the forefront of Internet access.

Like other governments, the Dutch government sees a role for itself in shaping communication infrastructures. There are a number of Dutch Internet policies that outline the approach of the government to Internet governance. All recognise that a secure and stable *Internet* is essential for the Dutch economy and society as a whole. A sharp distinction is made between governance on and of the *Internet*. In this paper, we engage with their approach to governance of the Internet, its infrastructure, also referred to as the public core. The *Internet's* technical architecture, comprised of institutions, protocols and standards, has become the informational backbone of the world, making it critical for societal, economic, and political well-being. Historically and in its current policies, the government operated on the belief that the market, and its private Internet governance fora, are best suited to ensure that the *Internet* stays open, free, and secure, and thus defend Dutch interests. However, the Netherlands' direct control and, hence, ability to protect these values, is waning in the face of shifting power dynamics, such as the centralization of power in the hands of non-Dutch companies. Similar to other European contexts, these pressures put the Dutch engagement with communication infrastructures to the test, manifesting in concrete concerns and governance challenges.

First, this paper lays out recent academic debates on infrastructures, sovereignty, and anxiety to investigate the perceived role of communication infrastructures in society. By departing from an infrastructure perspective, we formulate a relational understanding of how infrastructures distribute power and control in society. Thus, we define communication infrastructures from the perspective of how they are experienced across different strata of Dutch society, by both citizens and the state. Citizens engage with digital communication infrastructures primarily as the Internet and telecommunications networks that provide access to online services. Civil servants, by contrast, experience it as the set of institutions, protocols and standards, values and norms that together form the technical backbone of communication. We then turn to the ongoing debate of digital sovereignty to show that key questions of autonomy, agency, and control have

primarily been discussed in relation to the state-market or the user-market nexus. These siloed approaches can in themselves not explain the unease and uncertainty experienced by people and institutions in relation to our communication infrastructures. We end with Winner's (1978) notion of infrastructural anxiety as an analytical lens to establish a common ground for the comparative discussion of different groups and their engagements with communication infrastructures.

To investigate the overarching question of how different actors experience and engage with communication infrastructures, we will answer the following research question:

> *RQ1*: What are the concerns of the Dutch population with regard to communication infrastructures?
>
> *RQ2*: How does the general public experience communication infrastructures and their avenues of engagement?
>
> *RQ3*: What is the perceived role of standard-setting in engaging with the shaping of communication infrastructures according to civil servants in the Netherlands?

Infrastructure, power, and sovereignty

To understand the relation between individuals, the Dutch government, and communication infrastructures, this paper departs from an infrastructural perspective. Infrastructures are theorized as large, relational systems that make other things possible and through which social arrangements are naturalized (Larkin, 2013; Hesmondhalgh, 2021). In the context of systems of power, Bowker and Star (1999) conceptualized infrastructures through their ability to categorize and organize social and economic activity. Infrastructures organize actors by enabling certain practices and thoughts while restricting others (Plantin, *et al.*, 2016; Bowker and Star, 1999). The embeddedness of infrastructures in social, economic, and political structures shapes how people connect to, experience, and engage with the world (Jameson, 2009; Galloway, 2012). Since infrastructures operate globally, they tend to influence local practices according to dominant values, norms, and standards (Hesmondhalgh, 2021; Galloway, 2012). It is in these local encounters of global infrastructures that conflicts and contradictions become visible (Jameson, 2009), which is why we engage with the governance of communication infrastructures through analyzing local encounters in the Netherlands.

We build on Mann's (1984) understanding of infrastructural power, namely that it originates from the state, but "diffuse[s] outwards from the particular power organizations that invented them" [1]. This implies that the state's infrastructural power may very well be moving towards other actors, subjecting the state, market, and citizens to a new hegemonic configuration. To understand the implications of these changing power constellations, our analysis seeks to address the relation between different scales (Graham and Marvin, 2001). By switching between the individual and the state level, we can outline how power in and power over communication infrastructures are experienced within the Dutch context. Urban life, as it spans citizens, infrastructures, and civil servants, serves as one of those scales that reflects changes in global dynamics through communication infrastructures. This scale highlights pressing questions around privatization, deregulation, and control, and has inspired us to rethink the relationship between the Dutch state, its citizens, and infrastructures in a changing geopolitical landscape.

The debate on cybersovereignty (Fang, 2018) and digital sovereignty (Musiani, 2022) is the latest iteration of debates and studies on infrastructure governance and describes the ongoing struggle to control digital assets and information flows (Couture and Toupin, 2019). Although sovereignty can be understood in many ways, it is commonly defined as a contestation of, or at the very least, a response to outside interference [2].

In the Netherlands, like in other European countries, there are concerns about the non-European corporate control of communication infrastructures (Pohle and Thiel, 2020; Maxigas and ten Oever, 2023). This lack of national or regional influence over infrastructures is perceived as a threat to a country's economic independence, ownership of national resources, and decision-making power (Pohle and Thiel, 2020). Academic debates conceptualize digital sovereignty as a relationship between either the state and market or the user and the market. State-market research has historicized digital sovereignty in relation to national security (Deibert, 2008), territory (Catanzariti, 2024), ideologies (Pohle and Thiel, 2020; Carr, 2015; Maxigas and ten Oever, 2023), and control (Beniger, 1986; Chun, 2005; Easterling, 2014; Winner, 1978). Several studies into state responses to technologies found that digital sovereignty policies are largely discursive practices, lacking the political will, investments, and enforcement needed to reclaim autonomy in an interconnected world (Baur, 2024; Lambach and Oppermann, 2022; Adler-Nissen and Eggeling, 2024).

Digital sovereignty debates that centre the user primarily engage with concepts such as privacy, agency, and autonomy (Couture and Toupin, 2019; Haché, 2017). The assumption is that much of the engagement of citizens with communication infrastructures hinges on a desire for autonomy and agency. User autonomy calls for individual self-determination [3], such as being able to act independently and design, build, and distribute technologies and relationships that are good and meet local needs [4]. Contrastingly, current corporate ownership of infrastructures, platforms, and data limits user agency [5]. We will contribute to these debates on digital sovereignty by excavating and connecting citizens' and civil servants' experiences and attitudes toward communication infrastructures and argue that the underlying anxiety shapes a governance dynamic where responsibility is externalized to other actors.

Infrastructure and anxiety

Following Winner [6], we understand infrastructures as socially sedimented technologies that form large-scale networks, which host a wide range of contemporary anxieties present in society. Anxiety can be described as a preemptive reaction to unknown future risks [7]. As part of the urban space, infrastructures narrate anxiety on multiple levels. Kimari and Lesutis (2022) argued that infrastructural megaprojects mediate geopolitical influence at the level of ordinary citizens, non-citizens, domestic and foreign politics. Infrastructural developments serve as a site of both aspiration and conflict, placing them at the center of the human experience. While megaprojects usually carry a promise, such as progress as the primary logic of modernity [8], they simultaneously generate contradictions and conflicts in the everyday lives of communities. Anxiety not only represents a sense of unease but also encompasses a desire to act and pre-emptively respond to a risk that has not materialized yet. We will build on these conceptualizations to argue that the term infrastructural anxiety allows us to understand the misalignment between global infrastructure, local values, and agency.

Chettri and Venhovens (2024) argued that infrastructures "condense the past, present and future into their materiality" [9]. Anxieties do not materialize out of nowhere, they are also historically determined, building on top of and morphing with pre-existing anxieties. They further advocate for anxiety in the singular, not to make a universal claim on human experiences, but to foreground object-specific anxiety. How individuals and the state experience the distribution of power and control through infrastructures depends on its importance to social and economic activity, its governance structure, and the ability to respond to outside interference. While the term anxiety is more commonly used to describe the human experience in relation to automation (Goffey, 2019) or in postwar society (Schuldenfrei, 2012), we will use the concept to capture the profound sense of unease with the economic and geopolitical configuration of our communication infrastructures. Through a population-wide survey and semi-structured interviews with citizens and experts, we will tease out how infrastructural anxiety manifests in relation to communication infrastructures. As we will come to argue, infrastructural anxieties are shaped by individual and collective experiences and inform a particular type of agency, on the individual and structural levels, one that externalizes responsibility to a third party.

Methods

This research draws on both quantitative and qualitative methods to compare and connect experiences of different actors regarding communication infrastructures in the Netherlands. We base our argument on insights from three datasets. The first is a representative survey of the Dutch population that aims to identify citizens' concerns regarding communication infrastructures. We conduct secondary analysis on the results of a survey produced by Ipsos I&O in collaboration with one of the authors of this paper (Driessen, *et al.*, 2024) in order to establish how people in the Netherlands perceive communication infrastructures. The second dataset that we draw on in this paper is a set of interviews with members of the general public, which was undertaken to understand how these concerns manifest in people's lived experiences. This also generated insights into individual avenues of engagement and their limitations. The third source of data is expert interviews with civil servants that we have conducted in order to understand government engagement with communication infrastructures. Thus, we deepen and contextualize the findings of the survey with the examination of interviews with members of the general public and with experts. Considering the experiences of citizens and civil servants in the framework of the same research makes sense because as we show later, citizens refer their concerns to the civil servants, so that such a research design allows us to follow the issue itself as it unfolds across the experiential domains of multiple actors, allowing us to understand the problematic better than any one of these actors, or researchers who studied them individually.

Data collection

The three datasets were collected through three methods: a representative population survey (*N*=2,154), 69 semi-structured ethnographic field interviews with members of the general public (*N*=89), and seven semi-structured elite interviews with civil servants.

The representative survey (Wolf, *et al.*, 2016) was undertaken in the framework of the IN-SIGHT research project [10] and implemented by I&O Research (cited as Driessen, *et al.*, 2024). It explores how digital technologies are experienced and problematised by Dutch citizens. Invitations were sent to 4,191 members of the I&O Research panel, followed by two reminder rounds to address underrepresentation in specific demographic groups. In total, 2,154 panel members completed the questionnaire, yielding a response rate of 51 percent. To ensure representativeness, the results were weighted for age, gender, level of education, region, and voting behaviour in the 2021 Dutch parliamentary elections, following the Golden Standard guidelines of the Dutch Central Bureau for Statistics (CBS). These procedures ensure that the dataset reflects the composition of the Dutch voting population across key demographic variables. The survey thus provides a robust empirical basis for examining nationwide concerns and perceptions of agency surrounding digital technologies. Nevertheless, while the survey allows for the identification of broad trends and attitudes, its design and descriptive analytical approach limit the contextual and interpretive depth that can be achieved through quantitative data alone.

To address the limitation of mere quantitative analysis, the authors co-produced the interactive sculpture "Antennas and Us" with the media artist collective Weise7 (Figure 1). It was showcased at a popular public library. This interactive representation of a 5G antenna invites general public responses that we captured through ethnographic field interviews over a two-week period. In February 2023, after two days of developing and trialling a script, we recorded 69 semi-structured interviews with 89 participants at the central Public Library of Amsterdam (the OBA Oosterdok). We used the artwork as a prompt for interviewees to reflect on their relationship to communication networks, and in particular on the role of the next generation 5G mobile phone network in their lives. As a result of the collaborative design process, the installation brought antennas, as emblematic artefacts of communication infrastructures, from the rooftops down to the line of sight of people in public space. We consciously staged the encounter without a particularly dark and dystopic, or bright and utopian framing any one of which would influence participants' perspectives during the interviews. Participants took advantage of the open framing by taking a wide range of stances while reporting on their experiences. These interviews ground survey concerns by

providing deeper insights into the experiences of members of the general public.

Figure 1: "Antennas and Us" artwork simulation of a 5G base station beamforming antenna module (work of the authors)

Participants were recruited through convenience venue-based sampling [11], which qualifies library visitors from various backgrounds with a shared interest in the antenna. Local and foreign library visitors in the city centre of Amsterdam served as a proxy for the general public. Thus, the sampling approach mirrored how communication infrastructures are utilised by a diverse range of individuals who are part of the Dutch public infrastructure at a given moment.

We examine the response of the Dutch government to communication infrastructures by exploring civil servants' roles in standard-setting. Through semi-structured elite interviews with officials from key Dutch ministries, we investigated how communication infrastructures were governed. Using purposive expert sampling (Etikan, *et al.*, 2015), we selected experts involved in Internet governance and standard-making. Taken together with the other datasets, these conversations with policy-makers revealed discrepancies between Dutch Internet governance and citizen concerns.

Data analysis

Interviews were transcribed using intelligent transcription for readability while retaining word choice [12]. Quotes were anonymized by labeling public members as P and civil servants as C. A mixed-methods coding approach (Tashakkori and Teddlie, 1998) balanced deductive analysis with inductive theory-building (Glaser and Strauss, 2012), ensuring both descriptive detail and analytical clarity (Hruschka, *et al.*, 2004). During the second coding stage, codes such as "justification of concerns" were refined with those suggested by participants until saturated descriptions of data were achieved [13]. Thematic analysis identified patterns (Braun and Clarke, 2006), organizing findings around concerns, agency, values, engagement, and the governance of technology.

The three studies bring together prominent themes around communication networks as they are experienced

in the Dutch context by members of the general public and civil servants. Based on the data, this research provides insights into concerns and engagements with communication infrastructures and the perceived role of state governance.

Findings

Citizens are concerned

This section draws on the representative survey and interviews with the general public to foreground the type of concerns that Dutch citizens have, their sense of agency, and their perceived influence on technology by asking: *What are the concerns of the Dutch population with regard to communication infrastructures?*

Above all, the survey shows that Dutch citizens are worried; only "one in ten people have few concerns while over half have (a lot of) concerns" [14] as can also been seen represented in Figure 2. However, this does not hamper their enoyment in the usage of digital technologies as can be found in Figure 3. Citizens are concerned that unwanted access and use of data by criminals, companies, and governments will lead to a loss of control over their personal data and that this will negatively impact their lives (see Figure 4). How these harms are experienced becomes evident in the general public interviews, where comparisons between technology and weapons foreground the temporal and intangible nature of these concerns. Harms are understood as uncertain future risks rather than immediate impacts:

> The antenna gives a big possibility to people to do harm to others, and that's a bad thing. Like weapons do, but even with weapons, we don't have a lot of values. [...] Apparently, within the Liberal Society we're not very much aware of the harm technology can do till it's too late. (P28)

Despite their concerns, citizens are unwilling to disengage from technologies (see Figure 3); they have become indispensable to their personal and professional lives [15]. The silent trade-off between concerns about future risks and use of technology also materialized in the interviews with the general public "I just think it is probably okay, and if not, at least I can use my phone before I die" (R2–R3). This contradiction between concern and use has been often theorised about as the privacy paradox (Gerber, *et al.*, 2018) which primarily focussed on attitudes and behavior, but as we are interested in experiences of communication infrastructure, this observation necessitates a better understanding of how citizens' relationship with technology shapes their sense of agency.

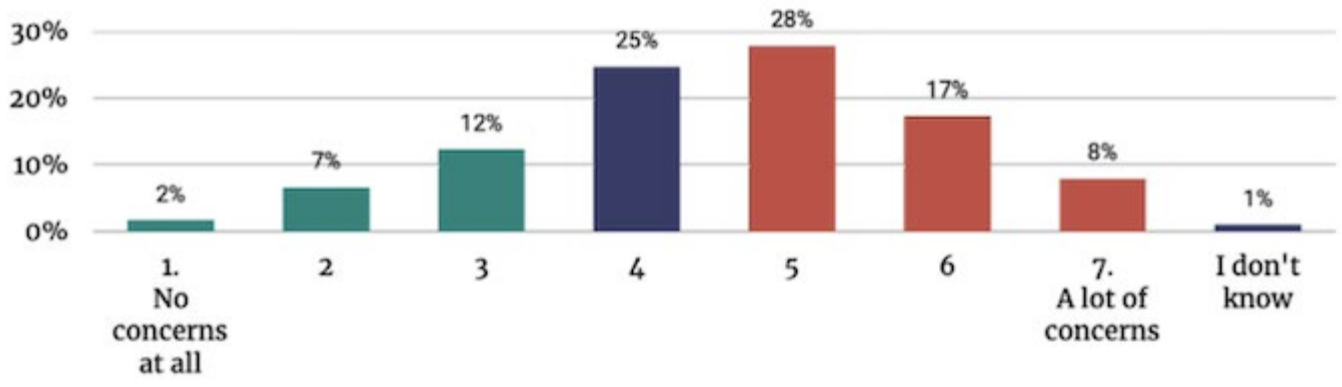

Figure 2: '*How concerned are you about the role that digital technologies play in our society? Where would you place yourself on the spectrum, if 1 means you have no concerns at all and 7 means that you have a lot of concerns?*' Basis: whole sample (*N*=2,154). From: Driessen, *et al.*, 2024.

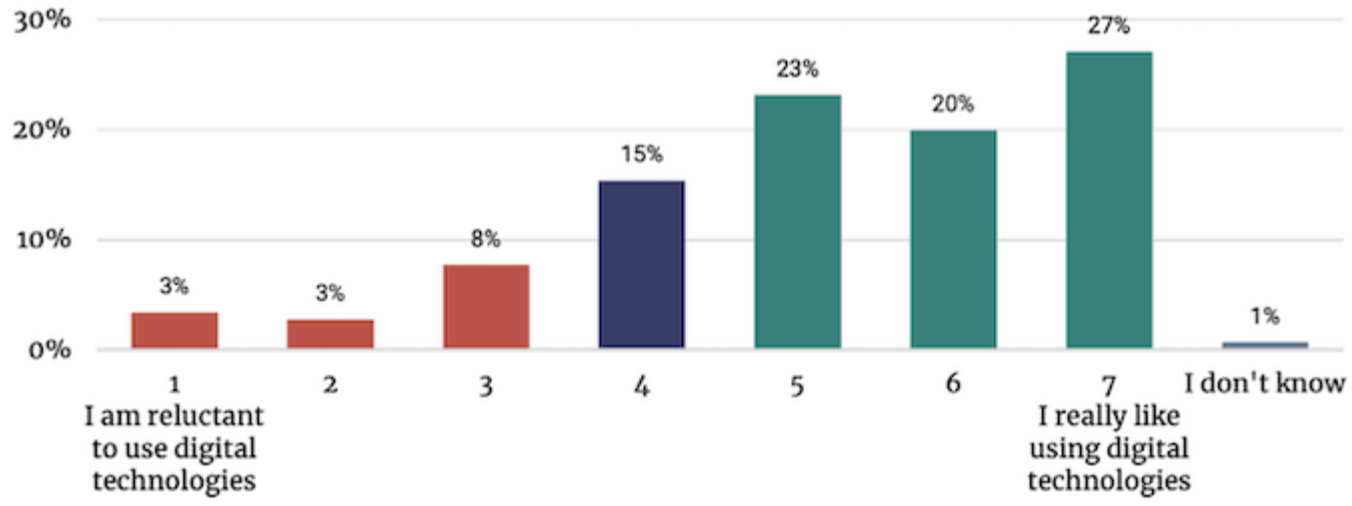

Figure 3: '*Where would you place yourself on the spectrum, if 1 meant that you are reluctant to use digital technologies and 7 meant that you really like to use digital technologies?*' Basis: whole sample (*N*=2,154). From: Driessen, *et al.*, 2024.

A recurring sentiment is the sense of loss of control. In this survey, the ability to exercise agency over technology is measured through a combination of knowing where to express their concerns and being able to make well-informed decisions about digital technologies. We found that the majority of citizens feel that they have little agency over technology. Particular citizen groups, namely young people, women, and higher educated people, report a lower sense of agency [16] and experience fewer opportunities for self-determination. The loss of control is echoed in the interviews: "there should be the ability to opt out of it anytime. The user should always be in control" (P89). Simultaneously, citizens feel they are increasingly controlled by technologies. "I don't like the nature of the surveillance economy and how it shapes my behaviour" (P79), which can go as far as to become a "distraction from things that matter in life" (P78). These findings show how citizens experience technologies as an entity that shapes their lives beyond their control.

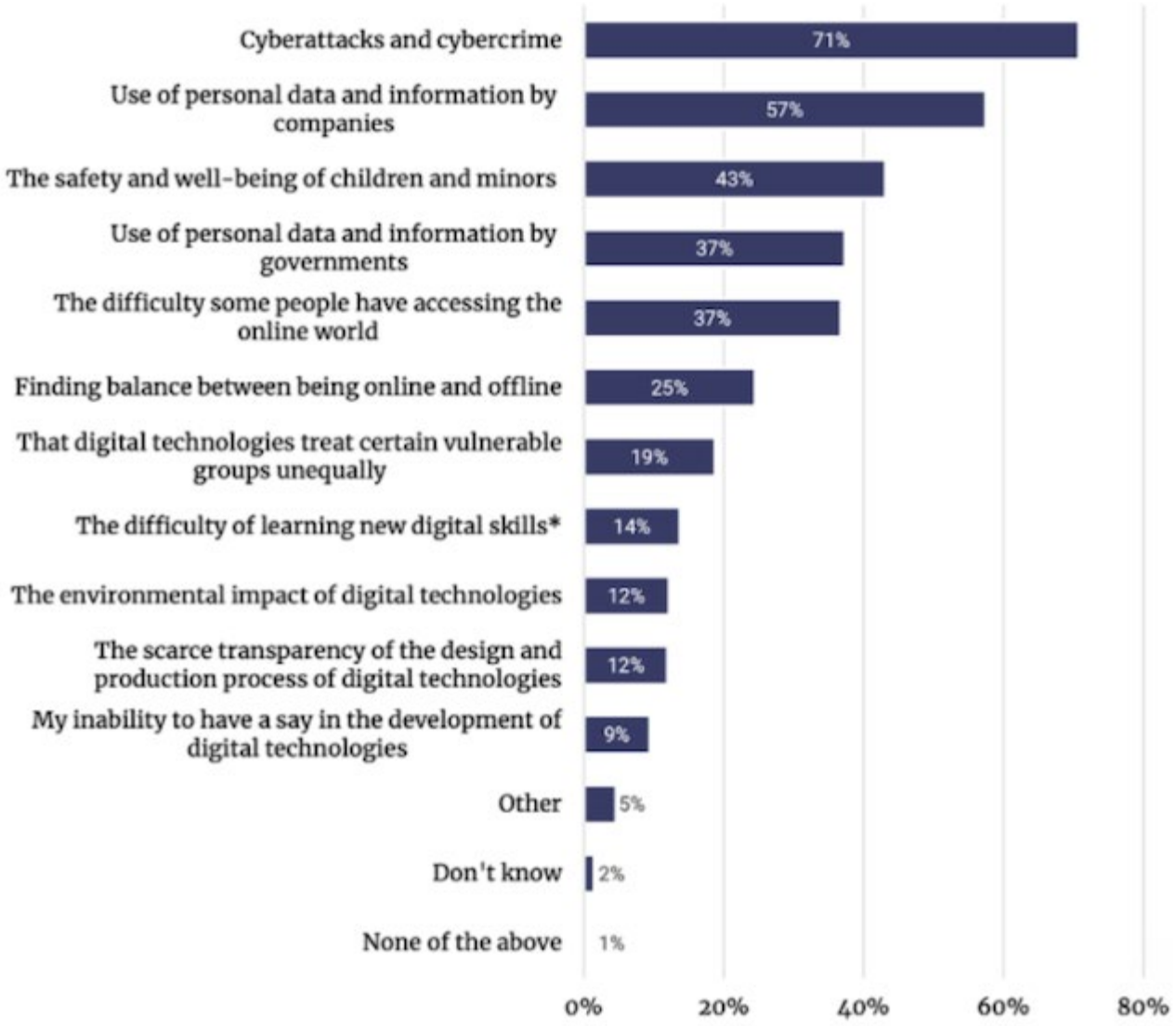

Figure 4: '*What is your biggest concern when it comes to the role that digital technologies play in our society?*' Maximum 4 answers possible. Basis: has (some) concerns about the role of digital technologies (*N*=2,101). From: Driessen, *et al.*, 2024.

General public avenues of engagement

We draw on general public interviews and survey results to answer the research question: *How does the general public experience communication infrastructures and their avenues of engagement?* First, we elaborate on citizens' tactics of dealing with communication infrastructure in their own capacity. Then, we evaluate the limits of their engagement and how these tensions manifest in an externalization of responsibilities to others, such as the government.

The scale at which one conceptualizes communication infrastructures determines how the general public experiences its avenues for engagement. When asked who has the biggest influence on how technologies work, citizens point to other actors, primarily companies. Particularly with newer technologies, such as 5G, there is a sense that companies develop and states regulate, beyond the ordinary citizen's reach [17]. Although citizens do not feel they have direct influence on the development or regulation of technologies,

when communication infrastructures are scaled down to their immediate environment half of the interviewees and survey respondents indicate they make informed choices and enact agency through privacy-preserving practices, from installing a virus scanner to changing passwords [18].

Next to these privacy-preserving measures, interviewees described different ways to break free from the influence technology has in their lives: “once in a while, it’s good if you at least in some parts of your life, you can shut it up” (P22). They purposely turning off their phone, data, or Wi-Fi in order to reinforce a divide between their lives and technology. This reinstatement of control through boundaries is particularly visible when people choose to leave their phone behind: “I’ve recently started doing walks and I just leave my phone, just leave it in the house because then I really rest” (P72). Interviewees argued that the act of disengaging with their devices would limit the ability of companies and the state to surveil them and increase their online-offline life balance.

Despite tactics to protect their privacy, citizens feel powerless in the face of technology. The sense of powerlessness is explained in the survey to a lack of technical knowledge and insights into its governance processes [19]. In the interviews, we furthermore observe a pessimistic sentiment around the ability of individuals to enact change to their technological environment: “we’re literally like little ants running around, it’s like the big problems are way too big for one single mind” (P39–40). Interviewees state that their tactics cannot sufficiently solve concerns because technology has outrun human ability to control it: “technology will be, is already faster than human beings are, [...] you cannot control it anymore” (P22). These quotes indicate that the governance of communication infrastructures are experienced as something that is outside their control. A feeling that is also reflected in their sentiments around their tactics in an age of digitization, which many associate with a sense of overwhelm and powerlessness. The ongoing digitization “turns us into data rather than making us more human” (P92). Not only is influence over technology felt as out of the ordinary citizen’s reach, but there are economic incentives to keep them powerless: “Any advice from me, it doesn’t matter because everything will be used to earn money for some people” (P26). Even when we presented participants with the opportunity to give advice to the government, many people withheld responses. It appears that citizens do not believe that their engagement can sufficiently solve the root of their problems.

Citizens turn to the state to preserve autonomy

Citizens look towards the government and other actors to manage the negative externalities of the technology industry they feel are outside their control. They externalize the responsibility of technological governance to those stakeholders they believe have the power to ensure safety and security. Although tech companies are seen as leaders in tech development, interviews show that citizens believe that the government is the primary caretaker responsible for addressing concerns. People expect the government to put new technologies such as 5G “under some regulations, so it will not be used in a negative way” (P14). European interviewees often believe that “in Europe there are some good laws”, whereas “there are other countries where you would not be so generous with your data” (P89). The perceived levels of protection are considered geographically determined and tie back to how the relationship between the citizen and the state is constituted in a specific location.

A few interviewed people ask for governance that increases citizen autonomy and state sovereignty. They call for increased state engagement to counter the dependence on non-European providers, pointing towards geopolitical tensions that increase the urgency to think “about our sovereignty also as a country, and to make sure to spread your chances and your risks” (P89). This speaks to the digital sovereignty debates, where the state takes up an active role to protect communication infrastructures from outside interference [20]. Infrastructures that are governed by the state should “be accountable to people, and those decisions to be understandable and shapeable by people [...] to factor in things beyond companies’ interest within the implementation of technologies” (P79). Foregrounding that citizens want the Dutch state to protect the public interest over innovation and profit-based interventions. The next section outlines how the Dutch state understands its role in the governance of technology.

Dutch government avenues of engagement

The Dutch government distinguishes between governance "on" and "of" the Internet. In this section, we explore how civil servants experience the ability of the state to exercise control the governance of the Internet by answering the question: *What is the perceived role of standard-setting in engaging with the shaping of communication infrastructures according to civil servants in the Netherlands?* We first outline the Dutch approach to Internet governance and standard-setting, before we provide insights into how the Dutch state experiences its relationship with communication infrastructures.

The cornerstone of the Dutch approach to Internet governance is supporting its multistakeholder model, the open decision-making model where government, industry, civil society, the technical community, and academia participate through open processes, with open archives, and through voluntary standards. The values that inform the Dutch Internet policies are 'open', 'free', and 'secure'. Yet, the different ministries interpret these values in slightly different ways. As one civil servant mentioned, "these terms are guidelines that get a different substance in different fora" (C3). Yet, the Dutch approach to governance of the Internet is in line with the more technical approach, these values are seen as free from political influence, as traffic and packages should be able to move freely and securely from point A to B.

Anxiety, control, and externalization

From more politically-oriented viewpoints, there is an emphasis on limiting restrictions and censorship, safeguarding fundamental rights, and protecting people and Internet infrastructures from cybercrime and state-sponsored attacks. These nuances reflect a broader tension on the question if the state has a role to play in the governance of the *Internet*.

Several interviewees highlighted that the governance of the *Internet* and the strong Dutch position are under threat. As an early adopter, the Dutch influence on Internet infrastructure and its governance is disproportionately large compared to the size of the country. One expert referred to its positioning as "punching above its weight" (C2). Since the early days of the *Internet*, the Netherlands has become a critical node in the transnational Internet infrastructure, and its technical community has contributed to important communication protocols, such as DNS, WiFi, and IMAP. The Dutch approach to Internet governance is aimed at not losing this standing.

However, geopolitical and economic shifts are raising a number of concerns. There is anxiety that other states will control the shape of the public core. Interviewees are concerned about efforts by other states to transfer power and decision-making away from multistakeholder to multilateral models, where countries and not technical experts, have the final say in how the *Internet* is governed. Experts mention trends of economic consolidation that favour American and Chinese corporations, which decreases the presence and influence of European governments and technology and telecommunication champions. This trend can be observed in standards bodies, such as the International Telecommunication Union (ITU):

> If you look at the ITU, in the last 10 years, you see fewer and fewer European companies affiliated with it and instead many more, for example, Chinese companies. (C2)

Additionally, some civil servants are concerned that integrating human rights frameworks into the governance of the *Internet* will politicize a technical system, by requiring the network to become a gatekeeper of what is allowed to be sent over the network. These concerns foreground the desire to protect the public core against fragmentation, but more importantly, express a sense of loss of control over global infrastructures, and in its wake, the loss of the ability to shape communication infrastructures.

Civil servants perceive a number of challenges in regaining control, or at least ensuring that Western values of open, free, and secure remain the north star (C3) for the governance of the *Internet* in this changing geopolitical context. There is an inherent conflict between the longevity of standardisation processes and

the relatively shorter time span of the democratic political cycle, *i.e.*, the four-year mandate of governments. Beyond the temporalities of Internet governance, the development that political processes have become very technical, and many technical processes have become very political, is considered a risk. The way the NEW-IP proposal was brought forward by Huawei and its subsidiary Futurewei to the ITU was given as an example of the merging of political and technical processes. These proposals need the state to have technical experts who understand the system they want to regulate and political generalists who understand the geopolitical landscape and the consequences of specific interventions (C4). Bringing technical and political expertise together is not without strife; there are capacity issues, a lack of knowledge, and cultural differences that hamper the ability of diplomats to fully participate in the standardisation discussions. Similarly, these challenges materialize when technical experts engage in political processes. These challenges feed the argument and imaginary that the state has a limited role in the governance of the *Internet*, which has been the Dutch government's line since its inception.

The Dutch state continues to externalize responsibility for the functioning of the public core to the private multistakeholder model. Historically, the notion that the state has a limited role in governance of the *Internet*, primarily to shield the market from political distortion, has guided the Dutch approach to public core. Despite or because of these changing geopolitical times, some civil servants argued that we need to continue to shield the governance of the public core from government interference. Here, non-interference represents the desire to keep states with diverging interests away from changing the way the Internet has always worked. It is “not about interfering more with what we have” (C6) but about preserving the *Internet* “with all its flaws” (C3). This attitude has put the Netherlands into a defensive position, countering proposals from other actors to keep things as they are.

Citizens, state, and infrastructures

To gain insight into how global communication infrastructures shape experiences and actions in a local context, we traced the relationships among citizens, state institutions, and infrastructure. Taken together, these relationships reveal a dynamic characterized by an increased sense of loss of control and a consequent externalization of responsibility to third parties. The overall end result is a circular logic where the market ends up being responsible for the governance of communication infrastructures, despite the fact that it is this very actor that has created the conditions for contemporary insecurities in the first place. Thus, if this self-perpetuating dynamic is left unchecked, then it is likely to lead to even greater experiences of uncertainty.

We found that citizens are concerned about, and experience a loss of control over their digital environment, which they fear will negatively affect their everyday lives in the future. Their central concerns are data safety and security, and they act out these concerns by exercising their agency over their end-user devices, which they themselves see as a necessarily limited response. Thus, the survey results and interviews suggest that citizens primarily conceptualize global communication infrastructures as the networks that provide them access to digital services. This narrow framing of communication infrastructures in terms of access rather than a much broader field of governance issues explains why citizens feel that their action potential is limited when it comes to addressing their genuine concerns. They are dependent on continued access to the digital services that mediate their everyday lives and the scale of the infrastructures behind the services go beyond the confines of their life worlds in which they can act out their concerns. The response to such a mismatch between the scale of the actor and the future risks that nontheless demand a response is that individual citizens and families externalize responsibility upward to the stakeholder they believe has the power to regulate global communication infrastructures, which they believe is the state. In turn, our research shows that the state frames communication infrastructures in terms of the institutions, processes, and political economy that govern them. As such, civil servants who should respond to citizens’ concerns also experience a loss of control, but in a different way. Their concerns lie in how changes to global communication infrastructures may negatively impact social, political, and economic activity at the scale of the national polity. Civil servants reflect that since the advent of the *Internet*, the Dutch state has largely adopted a stance of political non-interference, which proved beneficial when the influence of the country over the *Internet* was disproportionately large. As this influence wanes, however, the state increasingly

faces uncertainty and fears about unknown future risks to society grow.

How each actor responds to the experience of powerlessness points to different conceptualizations of communication infrastructures and their perceived influence and power over it. Citizens externalize responsibility upward to the state as they have come to expect, as part of the social contract, that this actor can operate at scale and holds the power and duty to ensure safety and security. By contrast, civil servants externalize responsibility outward to the market and internet standard-setting bodies operating within a private multistakeholder model that have historically contributed to economic prosperity and have aligned with Dutch interests, but have also created the conditions of contemporary insecurity. While they acknowledge that the market is part of the problem, they simply can not envision a different way to govern communication infrastructures. In the next section, we will conceptualize these situated, anticipatory unease about communication infrastructures as infrastructural anxiety, and argue that understanding the problematic in this way and through this term offers insights into the limitations of digital sovereignty approaches, as well as how to overcome them.

Discussion

Although governance of global communication infrastructures involves multiple actors and scales, discussions often focus on only one level of analysis. Academic research has examined how norms and values get inscribed in our infrastructures in Internet governance fora (Abbate, 1999; DeNardis, 2020) or how the discourse of digital sovereignty represents a struggle over global networks in national territory (Couture and Toupin, 2019). Yet, little is known about how citizens and institutions are experiencing communication infrastructure and how this directs (self)governance approaches. In this paper, we look across the different scales of society, the individual and the state, to gain insight into how the relationship with global infrastructures is experienced and acted upon. By shifting scales between Dutch citizens and civil servants, we highlight the frictions arising from misalignments between global systems, local values, and agency. They experience a loss of control in their relationship to global communication infrastructures and respond by externalizing responsibility to an outside actor. In this section, we deepen Winner's (1978) concept of infrastructural anxiety, who argues that large-scale networks like communication infrastructures are a "host of contemporary anxieties" in society [21], to explain how these situated experiences become intertwined with infrastructural power and produce a specific type of digital sovereignty.

Unlike fear, which triggers an immediate reaction [22] or moral panic, that leads to a disproportionate and collective response to crises [23], anxiety describes an individual's or state's lingering experience with technology that leaves room for a specific type of (self)governance approach. Anxiety, in response to the perceived immediate and future risk to economic and social well-being, emerges in the relationship between citizens, the state, and global communication infrastructures. Citizens feel they have limited control over their devices, data, services, and rights, which creates a new sense of powerlessness. Their infrastructural anxiety can be traced back to what Beniger (1986) terms a 'crisis of control'. Rather than a governable object that allows citizens to exercise control, communication infrastructures become ungovernable objects, which direct citizens' behaviour into certain directions outside their span of influence. As these seemingly autonomous technological systems grow in both scale and complexity, they foster powerlessness and diminish self-determination.

On a state level, the crisis of controls stems from the observation that there is a global reconfiguration of power happening, which can diminish the Dutch influence in the global governance arena and its ability to exert "purposive influence toward a predetermined goal" [24]. Megaprojects (Kimari and Lesutis, 2022) like Internet infrastructure gave the Netherlands progress and geopolitical influence, and allowed it to exercise control beyond its size. However, economic consolidation that favours American and Chinese corporations and their influence in Internet and telecom governance spaces produces anxiety about the country's future standing in the world order. This crisis is experienced as an 'ontological insecurity'

(Giddens, 1991), a term originally coined to explain how an individual's sense of insecurity in the world and their place within it shapes their behavior and relationships with institutions. Steele (2008) extended the concept to the state, describing how ontological insecurity emerges when a state's existence or geopolitical standing is perceived as threatened. The dynamic in which the Dutch state no longer recognizes itself as occupying its former position as a small but relatively influential international player in technology and communications, yet is unable to adopt an alternative posture, can be understood as a form of ontological insecurity.

We view experience as relational. Like Chettri and Venhovens described it, anxiety and infrastructures exist in a generative, cyclical relationship [25] — one that we argue also encompasses actors, institutions, and networks at different scales. To cope with the loss of control over communication infrastructures, actors do not respond immediately or disproportionately through panic or destruction; rather, they externalize and delegate responsibility to others whom they perceive as better positioned to address the cause of their anxiety. The process of externalization as a response to infrastructural anxiety aligns with Mann's (1984) concept of infrastructural power, which originates from the state and radiates outwards from the state to civil society. However, rather than shifting to civil society, power moves to the market. We found that citizens delegate responsibility to institutional governance mechanisms that they expect to match the scope of our communication infrastructure. Yet, the state looks toward the tech community and the industry, as civil servants feel their influence is naturally limited by the global nature and lack of Dutch ownership of communication infrastructures, the belief that these networks are best governed through global governance regimes, and Dutch underrepresentation in standard-setting bodies. As a result, governments look for governance mechanisms that match this complexity (Beniger, 1986; Winner, 1978), which places governance outside direct state control. Consequently, the government continues to externalize responsibility to governance spaces that are skewed to market interests. Not only does this dynamic assume good governance from actors whose *raison d'être* is to turn a profit and are first and foremost accountable to their shareholders and not citizens, but it also makes companies that generate infrastructural anxieties responsible for fixing the problems.

A final characteristic of infrastructural anxiety is the temporality of infrastructures. Technologies have been said to shrink time and space (Postman, 1986); we build on Chettri and Venhovens (2024) to argue that they do so in distinct ways. For Chettri and Venhovens (2024), anxiety about infrastructure is historically determined and emerges from and gets intertwined with pre-existing anxieties. The fear of the Dutch state losing geopolitical standing can be traced back to colonialism, where countries at the periphery were exploited and oppressed, or to the Cold War, where those third-world countries became the battleground for global conflict. Postwar anxiety scholars noted that global infrastructures amplified anxiety during periods of political instability (Schuldenfrei, 2012), as is the case presently. While civil servants did not directly speak to colonialisation or the Cold War, they spoke about losing geopolitical and economic standing. For example, civil servants expressed that the state considers its digital sovereignty to be under attack and witnesses a growing conflict between the aligned, non-allied, and hostile countries over the governance of our communication infrastructures. Preserving the 'original' values of the *Internet* — open, free, and secure — is aimed at keeping the ideology of openness (Maxigas and ten Oever, 2023) centre stage. An infrastructural ideology that has largely replaced U.S. military power with U.S. economic power (Carr, 2015; Russell, 2014). A liberal agenda of 'openness' is pushed in response to the anxiety of a global reordering, but its call rings hollow because the reordering is already happening and the Dutch state is not (yet) ready to exert digital sovereignty.

Conclusion

Digital sovereignty claims are the loudest when states feel that their authority is contested (Couture and Toupin, 2019). Sovereignty is about having the final decision-making power over what happens in a specific territory, which hinges on ownership of national resources and infrastructures (Pohle and Thiel,

2020). We contribute to these debates by looking at the relationship between the citizen and the state with communication infrastructures through the lens of experiences. This approach provides new insight into why sovereignty claims often fall short in governing the conflicts and tensions that arise when global communication infrastructures intersect with local contexts. Contemporary societies are caught in a self-reinforcing loop. The experience of loss of control does not lead to actions that would allow citizens — or the state — to regain agency. Instead, fear of unknown future risks triggers a preemptive externalization of responsibility, citizens upward to the state, and the state outward to the market. In doing so, these actions reinforce the hegemonic configurations of global infrastructures that originally produced the experience of loss of control.

These insights show that infrastructural anxiety produces digital sovereignty as a specific type of self governance, one that can not be achieved by itself but that needs to be outsourced by citizens to the state, and in turn by the state to standards bodies and the market. Yet, none are well-equipped or positioned to produce digital sovereignty that guarantees the state's decision-making power and restores citizens' self-determination. This raised a philosophical question: 'Can an actor produce sovereignty for another one?' These anxious dynamics around infrastructure governance empower corporations that produce the (out-of-control) technologies for profit, and provide Sovereignty-as-a-Service (Grohman and Costa Barbosa, 2025). Ultimately, the externalization of responsibility to actors that operate within a set incentive structure in a competitive environment may not favor the public interest nor improve actually improve the sovereignty of states or citizens.

About the authors

Fieke Jansen is a postdoc researcher at the media studies department and a co-principal investigator with the critical infrastructure lab at the University of Amsterdam. She is part of the 'Exploring sustainability and environmental resilience: Sustainable AI Futures' research project, led by Professor Samantha Walton, Bath Spa University and a member of the advisory group for the Internet Infrastructure Climate Resilience Coalition: Action Research in Aotearoa New Zealand project.
E-mail: fieke [at] criticalinfralab [dot] net

Niels ten Oever is an assistant professor of AI and European democracies and co-principal investigator with the critical infrastructure lab at the University of Amsterdam. He is a visiting professor with the Centro de Tecnologia e Sociedade at the Fundação Getúlio Vargas. Niels teaches courses in politics and technology, has implemented technology projects on five continents, and has participated in many governance and standard-setting processes, such as in the IETF, ICANN, ITU, ICANN, and 3GPP.
E-mail: niels [at] criticalinfralab [dot] net

Sarah Vorndran was a research assistant at the critical infrastructure lab with an interdisciplinary background in area and media studies. Her soft spot for design and its socio-technical dimensions manifests in creative explorations of urban infrastructures and digital interfaces.
E-mail: captivatesarah [at] gmail [dot] com

Maxigas is an assistant professor at the media department at Utrecht University. He is interested in hacker culture, cybernetic ideologies, infrastructural imaginaries, and the materiality of the digital. He uses media ethnography and digital methods to answer philosophical questions about contemporary social conflicts.
E-mail: maxigas [at] criticalinfralab [dot] net

Notes

1. Mann, 1984, p. 194.

2. Couture and Toupin, 2019, p. 2,317.

3. Pohle and Thiel, 2020, p. 11.

4. Haché, 2017, p. 5.

5. Couture and Toupin, 2019, p. 2,316.

6. Winner, 1978, p. 7.

7. Yousseff, 2012, p. 18.

8. See Chettri and Venhovens, 2024, p. 2; Yousseff, 2012, p. 5.

9. Chettri and Venhovens, 2024, p. 2.

10. This research is supported by Dutch Research Council (NWO) through the Responsible Innovation research project (grant MVI.19.032) under the title “Making the hidden visible: Co-designing for public values in standards-making and governance.” This research is supported by Dutch Research Council (NWO) through the Responsible Innovation research project (grant MVI.19.032).

11. Etikan, *et al.*, 2015, p. 2.

12. McMullin, 2023, pp. 144–145.

13. Lewins and Silver, 2014, p. 30.

14. Driessen, *et al.*, 2024, p. 13.

15. Driessen, *et al.*, 2024, pp. 11–12.

16. Driessen, *et al.*, 2024, p. 16.

17. Driessen, *et al.*, 2024, p. 13.

18. Driessen, *et al.*, 2024, p. 14.

19. *Ibid.*

20. Couture and Toupin, 2019, p. 2,317.

21. Winner, 1978, p. 7.

22. Chettri and Venhovens, 2024, p. 2.

23. Critcher, 2008, p. 1,132.

24. Beniger, 1986, p. 7.

25. Chettri and Venhovens, 2024, p. 2.

References

J. Abbate, 1999. *Inventing the Internet*. Cambridge, Mass.: MIT Press.

R. Adler-Nissen and K.A. Eggeling, 2024. “The discursive struggle for digital sovereignty: Security, economy, rights and the Cloud Project Gaia-X,” *JCMS: Journal of Common Market Studies*, volume 62, number 4, pp. 993–1,011.
doi: https://doi.org/10.1111/jcms.13594, accessed 4 February 2026.

A. Baur, 2024. “European dreams of the cloud: Imagining innovation and political control,” *Geopolitics*, volume 29, number 3, pp. 796–820.
doi: https://doi.org/10.1080/14650045.2022.2151902, accessed 4 February 2026.

J.R. Beniger, 1986. *The control revolution: Technological and economic origins of the information society*. Cambridge, Mass.: Harvard University Press.

G.C. Bowker and S.L. Star, 1999. *Sorting things out: Classification and its consequences*. Cambridge, Mass.: MIT Press.
doi: https://doi.org/10.7551/mitpress/6352.001.0001, accessed 4 February 2026.

V. Braun and V. Clarke, 2006. “Using thematic analysis in psychology,” *Qualitative Research in Psychology*, volume 3, number 2, pp. 77–101.
doi: https://doi.org/10.1191/1478088706qp063oa, accessed 4 February 2026.

A. Calderaro and S. Blumfelde, 2022. “Artificial intelligence and EU security: The false promise of digital sovereignty,” *European Security*, volume 31, number 3, pp. 415–434.
doi: https://doi.org/10.1080/09662839.2022.2101885, accessed 4 February 2026.

M. Carr, 2015. “Power plays in global Internet governance,” *Millennium: Journal of International Studies*, volume 43, number 2, pp. 640–659.
doi: https://doi.org/10.1177/0305829814562655, accessed 4 February 2026.

M. Catanzariti, 2024. *Disconnecting sovereignty: How data fragmentation reshapes the law*. Cham, Switzerland: Springer.
doi: https://doi.org/10.1007/978-3-031-60734-9, accessed 4 February 2026.

M. Chettri and M. Venhovens, 2024. “Infrastructural anxieties: An introduction,” *Roadsides*, number 12, pp. 1–7.
doi: https://doi.org/10.26034/roadsides-202401201, accessed 4 February 2026.

W.H.K. Chun, 2005. *Control and freedom: Power and paranoia in the age of fiber optics*. Cambridge, Mass.: MIT Press.
doi: https://doi.org/10.7551/mitpress/2150.001.0001, accessed 4 February 2026.

S. Couture and S. Toupin, 2019. “What does the notion of ‘sovereignty’ mean when referring to the digital?” *New Media & Society*, volume 21, number 10, pp. 2,305–2,322.
doi: https://doi.org/10.1177/1461444819865984, accessed 4 February 2026.

C. Critcher, 2008. “Moral panic analysis: Past, present and future,” *Sociology Compass*, volume 2, number 4, pp. 1,127–1,144.
doi: https://doi.org/10.1111/j.1751-9020.2008.00122.x, accessed 4 February 2026.

R.J. Deibert, 2008. “The geopolitics of Internet control: Censorship, sovereignty, and cyberspace,” In: A. Chadwick and P.N. Howard (editors). *Routledge handbook of Internet politics*. London: Routledge, pp. 323–336.
doi: https://doi.org/10.4324/9780203962541-30, accessed 4 February 2026.

L. DeNardis, 2020. *The Internet in everything: Freedom and security in a world with no off switch*. New Haven, Conn.: Yale University Press.

doi: https://doi.org/10.2307/j.ctvt1sgc0, accessed 4 February 2026.

M. Driessen, M. van de Koppel, D. Hollander, S. Milan, J. de Vos, and N. ten Oever, 2024. “Public values concerning digital technologies,” *IN-SIGHT.it* (20 February), at https://openresearch.amsterdam/en/page/105731/public-values-concerns-and-agency-regarding-digital-technology, accessed 4 February 2026.

K. Easterling, 2014. *Extrastatecraft: The power of infrastructure space*. London: Verso.

I. Etikan, S.A. Musa, and R.S. Alkassim, 2016. “Comparison of convenience sampling and purposive sampling,” *American Journal of Theoretical and Applied Statistics*, volume 5, number 1, pp. 1–4.
doi: https://doi.org/10.11648/j.ajtas.20160501.11, accessed 4 February 2026.

B. Fang, 2018. *Cyberspace sovereignty: Reflections on building a community of common future in cyberspace*. Singapore: Springer.
doi: https://doi.org/10.1007/978-981-13-0320-3, accessed 4 February 2026.

D. Flonk, M. Jachtenfuchs, and A. Obendiek, 2024. “Controlling Internet content in the EU: Towards digital sovereignty,” *Journal of European Public Policy*, volume 31, number 8, pp. 2,316–2,342.
doi: https://doi.org/10.1080/13501763.2024.2309179, accessed 4 February 2026.

A.R. Galloway, 2012. “Software and ideology,” In: A.R. Galloway. *The interface effect*. Cambridge: Polity Press, pp. 54–77.

N. Gerber, P. Gerber, and M. Volkamer, 2018. “Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior,” *Computers & Security*, volume 77, pp. 226–261.
doi: https://doi.org/10.1016/j.cose.2018.04.002, accessed 4 February 2026.

A. Giddens, 1991. *The consequences of modernity*. Cambridge: Polity Press.

B.G. Glaser and A.L. Strauss, 2012. *The discovery of grounded theory: Strategies for qualitative research*. Originally published in Chicago by Aldine in 1967. Piscataway, N.J.: Aldine Transaction.

A. Goffey, 2019. “Automation anxieties and infrastructural technologies,” *New Formations*, number 98, pp. 29–47.
doi: https://doi.org/10.3898/NEWF:98.03.2019, accessed 4 February 2026.

S. Graham and S. Marvin, 2001. *Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition*. London: Routledge.
doi: https://doi.org/10.4324/9780203452202, accessed 4 February 2026.

R. Grohman and A.C. Costa Barbosa, 2025. “Sovereignty-as-a-service: How big tech companies co-opt and redefines digital sovereignty,” *Media, Culture & Society* (11 November).
doi: https://doi.org/10.1177/01634437251395003, accessed 4 February 2026.

A. Haché (editor), 2017. *Technological sovereignty*, volume 2. Barcelona: Descontrol, at https://sobtec.gitbooks.io/sobtec2/en/, accessed 4 February 2026.

D. Hesmondhalgh, 2021. “The infrastructural turn in media and Internet research,” In: P. McDonald (editor). *Routledge companion to media industries*. London: Routledge, pp. 132–142.
doi: https://doi.org/10.4324/9780429275340-13, accessed 4 February 2026.

D.J. Hruschka, D. Schwartz, D.C. St.John, E. Picone-Decaro, R.A. Jenkins, and J.W. Carey, 2004. “Reliability in coding open-ended data: Lessons learned from HIV behavioral research,” *Field Methods*, volume 16, number 3, pp. 307–331.

doi: https://doi.org/10.1177/1525822X04266540, accessed 4 February 2026.

F. Jameson, 2009. “Ideological analysis: A handbook,” In: F. Jameson. *Valences of the dialectic*. London: Verso, pp. 315–367.

W. Kimari and G. Lesutis, 2022. “Infrastructure as symbolic geopolitical architecture: Kenya’s megaprojects and contested meanings of development,” In: S. Schindler and J. DiCarlo (editors). *The rise of the infrastructure state*. Bristol: Bristol University Press, pp. 58–70.
doi: https://doi.org/10.1332/policypress/9781529220773.003.0005, accessed 4 February 2026.

D. Lambach and K. Oppermann, 2022. “Narratives of digital sovereignty in German political discourse,” *Governance*, volume 36, number 3, pp. 693–709.
doi: https://doi.org/10.1111/gove.12690, accessed 4 February 2026.

B. Larkin, 2013. “The politics and poetics of infrastructure,” *Annual Review of Anthropology*, volume 42, pp. 327–343.
doi: https://doi.org/10.1146/annurev-anthro-092412-155522, accessed 4 February 2026.

A. Lewins and C. Silver, 2014. Using software in qualitative research: A step-by-step guide. Second edition. Thousand Oaks, Calif.: Sage.
doi: https://doi.org/10.4135/9781473906907, accessed 4 February 2026.

M. Mann, 1984. “The autonomous power of the state: Its origins, mechanisms and results,” *European Journal of Sociology*, volume 25, number 2, pp. 185–213.
doi: https://doi.org/10.1017/S0003975600004239, accessed 4 February 2026.

Maxigas and N. ten Oever, 2023. “Geopolitics in the infrastructural ideology of 5G,” *Global Media and China*, volume 8, number 3, pp. 271–288.
doi: https://doi.org/10.1177/20594364231193950, accessed 4 February 2026.

C. McMullin, 2023. “Transcription and qualitative methods: Implications for third sector research,” *Voluntas*, volume 34, number 1, pp. 140–153.
doi: https://doi.org/10.1007/s11266-021-00400-3, accessed 4 February 2026.

F. Musiani, 2022. “*Infrastructuring* digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices,” *Information, Communication & Society*, volume 25, number 6, pp. 785–800.
doi: https://doi.org/10.1080/1369118X.2022.2049850, accessed 4 February 2026.

N. ten Oever, C. Perarnaud, J. Kristoff, M. Müller, M. Resing, A. Filasto, and C. Kanich, 2024. “Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine,” *Policy & Internet*, volume 16, number 4, pp. 692–710.
doi: https://doi.org/10.1002/poi3.422, accessed 4 February 2026.

J. Plantin, C. Lagoze, P.N. Edwards, and C. Sandvig, 2016. “Infrastructure studies meet platform studies in the age of Google and Facebook,” *New Media & Society*, volume 20, number 1, pp. 293–310.
doi: https://doi.org/10.1177/1461444816661553, accessed 4 February 2026.

J. Pohle and T. Thiel, 2020. “Digital sovereignty,” *Internet Policy Review*, volume 9, number 4.
doi: https://doi.org/10.14763/2020.4.1532, accessed 4 February 2026.

N. Postman, 1986. *Amusing ourselves to death: Public discourse in the age of show business*. London: Penguin.

A.L. Russell, 2014. *Open standards and the digital age: History, ideology, and njetworks*. Cambridge:

Cambridge University Press.
doi: https://doi.org/10.1017/CBO9781139856553, accessed 4 February 2026.

R. Schuldenfrei (editor), 2012. *Atomic dwelling: Anxiety, domesticity, and postwar architecture*. London: Routledge.
doi: https://doi.org/10.4324/9780203142721, accessed 4 February 2026.

B.J. Steele, 2008. *Ontological security in international relations: Self-identity and the IR state*. London: Routledge.
doi: https://doi.org/10.4324/9780203018200, accessed 4 February 2026.

A. Tashakkori and C. Teddlie, 1998. *Mixed methodology: Combining qualitative and quantitative approaches*. Thousand Oaks, Calif.: Sage.

L. Winner, 1978. *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, Mass.: MIT Press.

C. Wolf, D. Joye, T. Smith, and Y. Fu (editors), 2016. *Sage handbook of survey methodology*. London: Sage.
doi: https://doi.org/10.4135/9781473957893, accessed 4 February 2026.

D.M. Yousseff, 2012. “The sanitized city and other urban myths: Fantasies of risk and illness in the twentieth century metropolis,” Ph.D. dissertation in comparative literature, UCLA, at https://escholarship.org/uc/item/4pf6k0gd, accessed 4 February 2026.

Editorial history

Received 16 September 2025; revised 26 January 2026; accepted 4 February 2026.

PUBLIC DOMAIN
To the extent possible under law, this work is dedicated to the public domain.

Infrastructural anxiety and digital sovereignty: The perceived loss of control in Dutch communication networks
by Fieke Jansen, Niels ten Oever, Sarah Vorndran, and Maxigas.
First Monday, volume 31, number 3 (March 2026).
doi: https://dx.doi.org/10.5210/fm.v31i3.14530