

# Infrastructural insecurity: Geopolitics in the standardization of telecommunications networks

Media International Australia

1–17

© The Author(s) 2024



Article reuse guidelines:

[sagepub.com/journals-permissions](https://sagepub.com/journals-permissions)

DOI: 10.1177/1329878X231225748

[journals.sagepub.com/home/mia](https://journals.sagepub.com/home/mia)**Niels ten Oever**  and **Christoph Becker**

University of Amsterdam, The Netherlands

## Abstract

This article argues that the production and maintenance of “infrastructural insecurity” is an inherent part of the process of the standardization of telecommunication networks. Infrastructural insecurity is the outcome of intentional practices during the production, standardization, and maintenance of communication infrastructures that leave end-users vulnerable to attacks that benefit particular actors. We ground this analysis in the qualitative and quantitative exploration of the responses to the disclosure of three fundamental security vulnerabilities in telecommunications networks. To research the shaping of communication and infrastructure architectures in the face of insecurities, we develop a novel approach to the study of Internet governance and standard-setting processes that leverages web scraping and computer-assisted document set discovery software tools combined with document analysis. This is an important contribution because it problematizes the process of standardization and asks fundamental questions about the adequacy and legitimacy of the process and procedures of standardization, its participants, and its institutions.

## Keywords

Telecommunications, 5G, standards, governance, infrastructure, STS, insecurity, security studies, media studies, surveillance

## Introduction

This article interrogates the responses in standardization to significant security issues in telecommunications networks that have a transnational impact. We conclude that slow responses by telecommunication equipment manufacturers to address the insecurity—and in one case an outright refusal—reflect geopolitical interests to maintain insecure global communication networks. To explain this we develop the concept of “infrastructural insecurity” to highlight how the standardization of technology is not necessarily optimized to provide security but rather functions as a venue for geopolitical interests, also when it is driven by industry players. This further problematizes the complex relation between states, industry, and technology in the production, standardization, and maintenance of

---

### Corresponding author:

Niels ten Oever, Critical Infrastructure Lab, University of Amsterdam, Amsterdam, The Netherlands.

Email: [mail@nielstenoever.net](mailto:mail@nielstenoever.net)

telecommunication networks. More precisely, it problematizes the process of standardization, which is increasingly looked toward as a trusted process to address societal concerns (ten Oever and Milan, 2022). Most recently in the proposal to delegate authority on “ethical AI” to standard-setting processes in the European Commission’s draft AI legislation (Veale and Borgesius, 2021).

Traditionally, security was one of the primary reasons to engage in standardization, notably the standardization of the wall thickness of steam boilers to prevent future explosions (Yates and Murphy, 2019). However, in 2013 the whistleblower Edward Snowden exposed how the United States government engaged in the “manipulation of technical standards to render communication infrastructures susceptible to surveillance” (Rogers and Eden, 2017: 802). At the time this brought up questions about the adequacy and legitimacy of standard-setting. Responses by industry and standard-developing organizations that increased encryption in protocols did quiet down some of these debates and concerns (Doty, 2020; Wilton, 2017).

Recently discussions about standardization and security have resurfaced in the light of the NewIP proposals by Chinese actors (Hogewoning, 2020; Sharp and Kolkman, 2020), allegations about the insecurities resulting from Huawei’s 5G implementations (Becker et al., 2022; Mascitelli and Chung, 2019; Rühlig and Björk, 2020; Tekir, 2020; Wen, 2020), China’s increased participation in standardization (Baron and Kanevskaia Whitaker, 2021; Baron and Pohlmann, 2018; Pohlmann et al., 2020), as well as Russia’s attempts to build a national internet (Asmolov and Kolozaridi, 2021; Ermoshina et al., 2022; Ermoshina and Musiani, 2017; Stadnik, 2019) which gained even more notoriety through Russia’s war on Ukraine (Fontugne et al., 2020; Limonier et al., 2021; Luconi and Vecchio, 2022). This article aims to contribute to these debates by analyzing responses to three vulnerabilities in transnational communication infrastructures.

Security researchers regularly find vulnerabilities in computer networks, in many cases researchers inform the operator of the network or the producer of the product about the vulnerability (so-called “responsible disclosure”; Cavusoglu et al., 2007), or it is used to exploit this vulnerability to gain access to systems. In yet other cases the identifying of vulnerabilities leads to the reselling of a packaged vulnerability to third parties, as is the case with zero days (vulnerabilities that are not yet publicly disclosed). Yet, there is another possibility, which will be discussed here. Some vulnerabilities are disclosed but are not fixed through updates or patches, thus leaving users open to the abuse of these vulnerabilities. This article traces the responses in standardization to three significant security issues in telecommunication networks, namely (1) a security flaw in Signaling System No. 7 (SS7) that allows for data interception and surveillance, SMS interception, and location tracking by third parties; (2) the lack of encryption of permanent identifiers that allowed for the deployment of rogue base stations, which allowed for man-in-the-middle attacks, resulting in interception of all voice and data traffic in a physical signal vicinity; and (3) the lack of forward secrecy between user equipment and the home network, which allows for the decryption of current encrypted data stream if credentials were obtained in the past. We trace responses to these insecurities in the main Standards Development Organization (SDO) for telecommunications, the 3rd Generation Partnership Project (3GPP). The 3GPP is the main global umbrella organization for the standardization of telecommunication networks, they are the only global organization that develops standards for the fifth generation of telecommunication networks. The main participants in standard-setting in the 3GPP are equipment manufacturers and network operators, but everyone can become a member and partake in decision making via mailinglists and in-person meetings.

## Literature review

For the longest period in the history of telecommunications, namely from 1889 to 1876, signaling was not done by machines, but rather by humans (Dryburgh and Hewett, 2005). Switchboard operators used to use literal switchboards and cables to establish and end calls (Carmi, 2019). This was

needed to ensure that not every phone in the world would need to be connected to any other phone with a physical line—which would be a fully meshed topology.

Organizing routing and information in information networks has been a long-time fascination by cybernetic thinkers who argued that “control and automation were to be enacted on the population through more automatic technologies” (Carmi, 2020: 110), this would create, according to Ernst von Galsersfeld, “an equilibrium in a world of constraints and possibilities.” Another cybernetic, Norbert Wiener, said this: “Throughout the telephone industry, automatic switching is rapidly completing its victory over manual switching. It may seem to us that the existing forms of automatic switching constitute a very perfect process” (Wiener, 1950: 69). In this article, we dissect this “perfect process” by looking at the standardization of telecommunication infrastructures. We problematize the notion of Star that infrastructure “becomes visible upon breakdown” (Star, 1999: 382). By tracing the standardization processes of telecommunication infrastructures, we argue that the breakage of particular parts of infrastructure might be an inherent aim of those engaged in the operation, regulation, and standardization of these networks. This is an important contribution to the study of standards because standardization is widely perceived as a process that produces safety and security, not the opposite. One of the main examples of the modern history of standardization is the setting of the thickness of the walls of steam engines to prevent explosions in riverboats (Yates and Murphy, 2019). Next to that, there are commonly known health and safety standards that enable the certification of goods for national and regional markets (Laurent, 2022). And when Edward Snowden showed that insecurities were introduced through the standardization process (Rogers and Eden, 2017), SDO and governance bodies jointly published the “Montevideo Statement on the Future of Internet Cooperation” to structurally denounce such behavior and announce countermeasures.<sup>1</sup> Since standardization is increasingly popular among policymakers and technologists alike to address issues of ethics (Bryson and Winfield, 2017; Cath, 2018; Veale and Borgesius, 2021) and human rights impact of technology<sup>2</sup> (Cath, 2021) it is very important to understand where the process of standardization might fall short.

We aim to contribute to discussions about the interrelation between power in technology that are paradigmatic for Science and Technology Studies. However, we would like to also contribute to the theorization as to what this means on the scale of geopolitics. We do this by building on conversations and theories of Critical Security Studies, particularly recent contributions to the concept of “infrastructural geopolitics” (de Goede and Westermeier, 2022). These contributions not only explore how power over infrastructures is used to project hegemonic power but rather seek to highlight how infrastructures themselves are used to project power *through*. This discussion reflects debates in Standardization Studies (ten Oever and Milan, 2022; Yates and Murphy, 2019) about power *in* and *through* standardization, as well as longer-running debates in Media Studies (Carey, 1983; DeNardis and Musiani, 2016; Edwards, 2021; Paris, 2020; Söderberg, 2013; Wyatt, 2008) about the role of technology in the exertion of power, the limitations of technological determinism, and the importance of the alignment of visions, materiality, territory, and ownership (Estrada and Lehedé, 2022; Huang et al., 2022; ten Oever, 2022; Zajacz, 2019). In these debates, we often run into the limits of disciplinary boundaries that might limit our ability to understand the role of infrastructures at scale.

The field of Science and Technology Studies (STS) has been very effective in descriptively foregrounding the politics of science and technology (Brown, 2015), epitomized by Jannet Abatte when she argued that protocols are the continuation of politics with other means (Abbate, 1999; DeNardis, 2009), but normative frameworks have not been widely spread within the field of STS. Furthermore, STS has been very effective at looking at particular cases but has fewer methods available to look at larger-scale infrastructures and infrastructures that exist within large timescales. The field of international relations does have ample and extensive normative theories

and framework of power but provides limited frameworks to take the materiality of technology into account (even though scholars like Claudia Aradau (Aradau, 2010; Aradau and Blanke, 2015) have done a lot to connect the two fields). Media studies provide theories and approaches to study material technology but provide limited frameworks to theorize institutional power. Finally, the view from Standardization Studies is limited to the empirical object of standardization and thus struggles to connect methods from the different fields that study standards, such as law, economy, STS, and media studies. Infrastructure studies contribute to overcoming disciplinary boundaries, especially by emphasizing the importance of relationality in infrastructures, but here it inherits some of the ontological flatness and descriptiveness of STS by providing limited frameworks to understand the particular nature of the relations between the different actants in the infrastructure. By no means do we aim to invisibilize the work of excellent scholars who have sought to build bridges and develop new approaches to make infrastructural inversions (Bowker et al., 2010). Critical Security Studies (Krause and Williams, 2002), Feminist Science and Technology Studies (Campbell, 2004; Haraway, 1985, 1988), as well as approaches from Anticolonial Science (Liboiron, 2021), provide strong platforms to further research the complexities of power in transnational infrastructures.

The need to further develop research methods and approaches to study power in infrastructures is increasing in a period of algorithmification of infrastructures (Feamster and Rexford, 2017; Mai et al., 2021) where it becomes ever harder to know in infrastructural environments (although one could easily argue with Fenwick McKelvey infrastructures have always been run by algorithms; McKelvey, 2018). The implementation of machine learning in networking environments combined with the double movement happening with the introduction of 5G—the modularization of functionality communication infrastructures and the converging of internet and telecommunication infrastructures—makes it very complex to understand how communication networks concretely function (ten Oever, 2022). One could even wonder whether there still are vantage points that could explain the shape and flow of a datastream and its determinants. This complexity is why increasingly scholars, policymakers, and industry are looking at the process of standardization, which is the process in which the architecture of transnational infrastructures gets shaped, to understand information societies, influence, and exercise control. The scholar Keller Easterling argues that “[i]f law is the currency of governments, standards are the currency of international organizations and multinational enterprises” (Easterling, 2014: 18). This is what makes the process of standardization not merely important, but also a flashpoint of current geopolitical conflicts.

In this article, we use quantitative methods to foreground trends in standardization that are subsequently qualitatively analyzed. However, we are very aware of the limitations of combining methods from different disciplinary fields. While there is an overall trend toward mixed methods, which we very much applaud, the foundations of mixed methods research can be shaky when the ontological claims that underpin particular methods are not sufficiently aligned. This is by no means a call for researchers to retreat into disciplinary comforts, but rather an invitation to develop interdisciplinary ontologies and connected methods.

There are extensive (and complex) infrastructural assemblages to produce security, of which standard-setting is one, and certification (which guarantees compliance with a particular standard) is another. The production of security has been extensively critiqued, particularly in the field of critical security studies (Burgess, 2019), not in the least because throughout history, security has been used to legitimize particular orderings, epitomized in the Cold War (Edwards, 1996), the responses to 9/11, and recently in the reinstating of trade barriers by countries that for decades have bestowed free market regulations on the world (Maxigas and ten Oever, 2023). This goes to show that when security is produced, this may be security for some, but not for everyone. In this article, we explicitly do not look at practices of surveillance and interception that are commonly known as “legal intercept” (for an analysis of lawful intercept in the 3GPP see: Becker et al., 2022). We also do

not look at cases where secret services aim to weaken security to gain access to data (Rogers and Eden, 2017). We are also not looking at exploitation or the trade in so-called zero-day vulnerabilities. We are looking at a fourth category of insecurity as it is produced through the deliberate maintenance of formally unintended insecurities, which we call the maintenance of infrastructural insecurity.

## Methods

To research the shaping of communication and infrastructure architectures in the face of insecurities, we develop a novel approach to the study of Internet governance and standard-setting processes that leverages web scraping and computer-assisted document set discovery software tools combined with document analysis. We bring these methods into conversation with theoretical approaches from material media studies, STS, and international relations. This methodological approach has been introduced in our previous work (Becker et al., 2022).

Our findings are based on the study and analysis of two main text sources. Firstly, we studied the communication patterns between actors using the mailing lists of 3GPP's TSG SA WG3 on Security and Privacy (from now on abbreviated as WG3 and WG3\_LI; [https://list.etsi.org/scripts/wa.exe?A0=3GPP\\_TSG\\_SA\\_WG3](https://list.etsi.org/scripts/wa.exe?A0=3GPP_TSG_SA_WG3) and [https://list.etsi.org/scripts/wa.exe?A0=3GPP\\_TSG\\_SA\\_WG3\\_LI](https://list.etsi.org/scripts/wa.exe?A0=3GPP_TSG_SA_WG3_LI)) which is focused on further enhancements to the telecommunications system in the field of security and privacy in general and lawful interception in particular. Secondly, we used all reports of the quarterly held 3GPP TSG WG3 plenary meetings that are focused on security ([https://www.3gpp.org/ftp/tsg\\_sa/WG3\\_Security](https://www.3gpp.org/ftp/tsg_sa/WG3_Security)). These files are of interest, as the decision process behind the acceptance or objection (and by whom) to proposed changes on 3GPP specifications is partially revealed.

The text corpora were retrieved using Bigbang (Benthall et al., 2021) in February 2023. At that time the Listserv 17.0 mailing lists of WG3 and WG3\_LI contained 72.834 and 7.148 emails (with some containing attachments). For WG3 the mailing list has been in use since 1999 while WG3\_LI started communicating via email one and a half years later. The first plenary meeting reports of WG3 on security we could access date back to 1999, and we could process 861 meeting reports in total (there are more documents, but not all file formats were processable for us, such as xml, rtf, xlsx).

Before we bring to the fore relations and associations between involved stakeholders, we separate emails into sets of those that address purely managerial and organizational matters (e.g. meeting reminders and travel advice), those that focus on legal and technical aspects of privacy and surveillance in general, and those focused on Case 1 (SS7, diameter, etc), Case 2 (imsi, MCC, MNC, imsi catcher, N32, sepp, nai, suci, supi), and Case 3 (Diffie-Hellman, PFS, "perfect forward secrecy," EAP-TLS, EAP-AKA, SBA, N32) specifically. From now on we will denote the first set as SVT and the last three sets as T (the target set), while the set of all emails in the entire LI mailing list is referred to as S (the search set). To partition S, into T and SVT, we apply state-of-the-art techniques for unstructured and unlabeled text corpora, that rely on both human experts and machine learning algorithms (King et al., 2017). Together, they converge to a list of key terms which we compose into queries using the Boolean OR operator that identifies emails of interest (For the code and obtained key term list see: <https://github.com/Christovis/geopolitics-in-the-standardization-of-secur-telecommunications-networks/tree/main>).

## The production of infrastructural insecurity

In this analysis, we will trace the responses to three vulnerabilities. We will first introduce the vulnerabilities after which we will analyze the responses to these vulnerabilities in the foremost telecommunication standards body, the 3GPP.

## SS7

Since the late 1970s, Signaling System No. 7, more commonly known by its abbreviation SS7, has been underpinning routing and interoperation between telecommunication providers. SS7 was formally standardized in the 1980s in the International Telecommunication Union (ITU) in the Q.700-series, even though much of the work was done in regional standardization bodies such as the European Telecommunications Standards Institute (ETSI). Since the end of the 1990s and the beginning of the 2000s, most of the standardization of telecommunication standards happens in the 3GPP, which is an umbrella organization for seven regional standards organizations.

SS7 is a combination of protocols that allows the establishment of a circuit across different telecommunication networks to establish and maintain a telephone call. This means that SS7 mediated all mobile and fixed-line phone conversations. Because SS7 was far more efficient than its predecessors, it can share a significant amount of information in the process of establishing, managing, and ending a circuit. This allowed for many functionalities to be developed on top of SS7, ranging from call-forwarding to voicemail and conference calls, but later also noncall-associated signaling, which—as the name says—enabled the exchange of information not directly related to calling between networks, such as the geographical location of a device.

In 2008 at Europe's largest hacker conference, the Chaos Computer Congress, Tobias Engel disclosed how a vulnerability in the SS7 allowed for locating every phone number with a precision up to 50 m and in some cases the ability to listen in to phone calls, without anyone knowing about this (Engel, 2009). These vulnerabilities were never addressed and taunt SS7 networks until today. However, when 4G was introduced, it also contained a replacement for SS7, namely the Diameter protocol which was not vulnerable to these attacks. This, however, did not end the vulnerability from occurring. Because the Diameter protocol interoperates with SS7, the vulnerabilities that exist within SS7 exist until today, and will exist until all pre-4G networks are abandoned.

### *Fake base stations*

The emergence of fake base stations, devices that acted like telecommunication masts owned by a telecommunication provider, but technically were man-in-the-middle attacks to obtain information from a mobile device in the physical vicinity of a subscriber, happened in the early 1990s (Parks, 2016). This happened around the same time as the commercial introduction of mobile phones. A wide range of commercial providers in Europe, the United States, and later Asia would provide devices that would enable the surveillance of devices. The most commonly known device is marketed by the firm Harris as the “Stingray,” but this technology is also known as cell-site simulators or fake cell towers. The existence of these technologies has been widely documented, and police departments and secret services around the world use these devices (Hardin, 2017). To protect users from this man-in-the-middle attack, the identifying information of a device should be encrypted to be concealed against attacks. Such encryption for the longest time was optional, and only during the standardization of 5G, specifically in the technical specification 23.501 which was published by the 3GPP in July 2022, such encryption was formally standardized.<sup>3</sup>

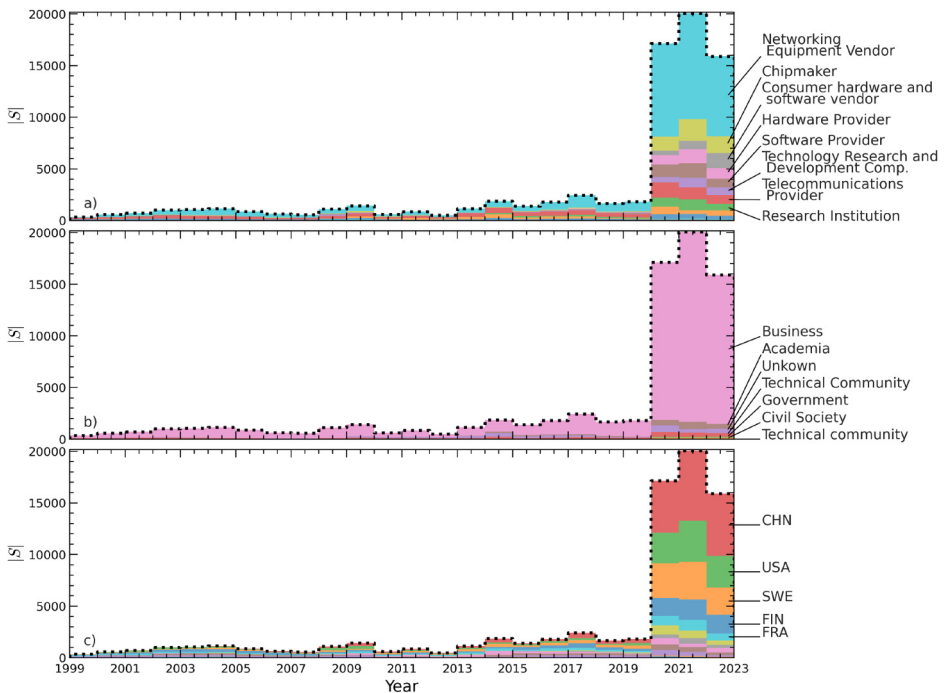
### *Stealing encryption keys*

In 2010 the Dutch firm Gemalto was the largest producer of SIM cards. These cards identify a user against a telecommunication network. To do this, secret encryption keys are stored on the SIM card. The security of these keys is the basis of encryption with the telecommunication provider's network. The United States National Security Agency (NSA) and the British Government

Communications Headquarters (GCHQ) unbeknownst to Gemalto, acquired access to their networks and computers and exfiltrated the secret keys to SIM cards that were being produced by Gemalto (Buchanan, 2020; Wolfe, 2017). Thus allowing access to the encrypted authentication and communications processes initiated by the cards that carried these keys. It was argued by experts that this exfiltration might impact billions of keys.<sup>4</sup> This hack was first reported by Edward Snowden and later confirmed by the firm Gemalto itself.<sup>5</sup> To address this particular incident, all SIM cards issued by Gemalto would need to be replaced. However, this never happened. To address the issue of so-called “static key exfiltration” it is recommended that dynamic keys are used, this makes potential attacks much harder because keys are used for a much shorter time. This “zero trust” approach minimized the impact of a breach or key exfiltration, such as in the Gemalto case. However, the introduction of such protection in the 3GPP, through the introduction of Perfect Forward Secrecy (PFS) in Extensible Authentication Protocol (EAP) authentication was structurally rejected, leaving future users up to today open for this vulnerability.

### Mailinglists

In Figure 1, the black dotted line in all three panels shows the numbers of all emails in ISI send per year (meaning emails sent to both mailing lists). It is clear that since 3GPP has become the main body to standardize 5G the email traffic has exploded. This shows both the interest in 5G as well as the centrality of the 3GPP in its standardization.



**Figure 1.** Panels (a), (b), and (c) show the set size of all emails, |S|, sent per year through a black dotted line, that is filled in with a color that indicates the stakeholder’s market category, sector, and the headquarter location of (parent) organization, respectively.

Each of the three panels shows in color the combined contribution of different sets of stakeholder attributes: panel (a) the market category, panel (b) the sector, and panel (c) the headquarters location of the (parent) organization. Starting from the top, we can identify network equipment vendors, chipmakers, consumer hardware and software vendors, and hardware providers to be among the main contributors to mailinglists. Judging by the history of stakeholder categories, it comes with little surprise that the dominant stakeholder group comes from the business sector, dwarfing the contributions of all others. Interestingly however, of all other groups, actors with an academic affiliation have been the most active in the past 3 years. The contributions by actors which could not be categorized are labeled as “Unknown.”

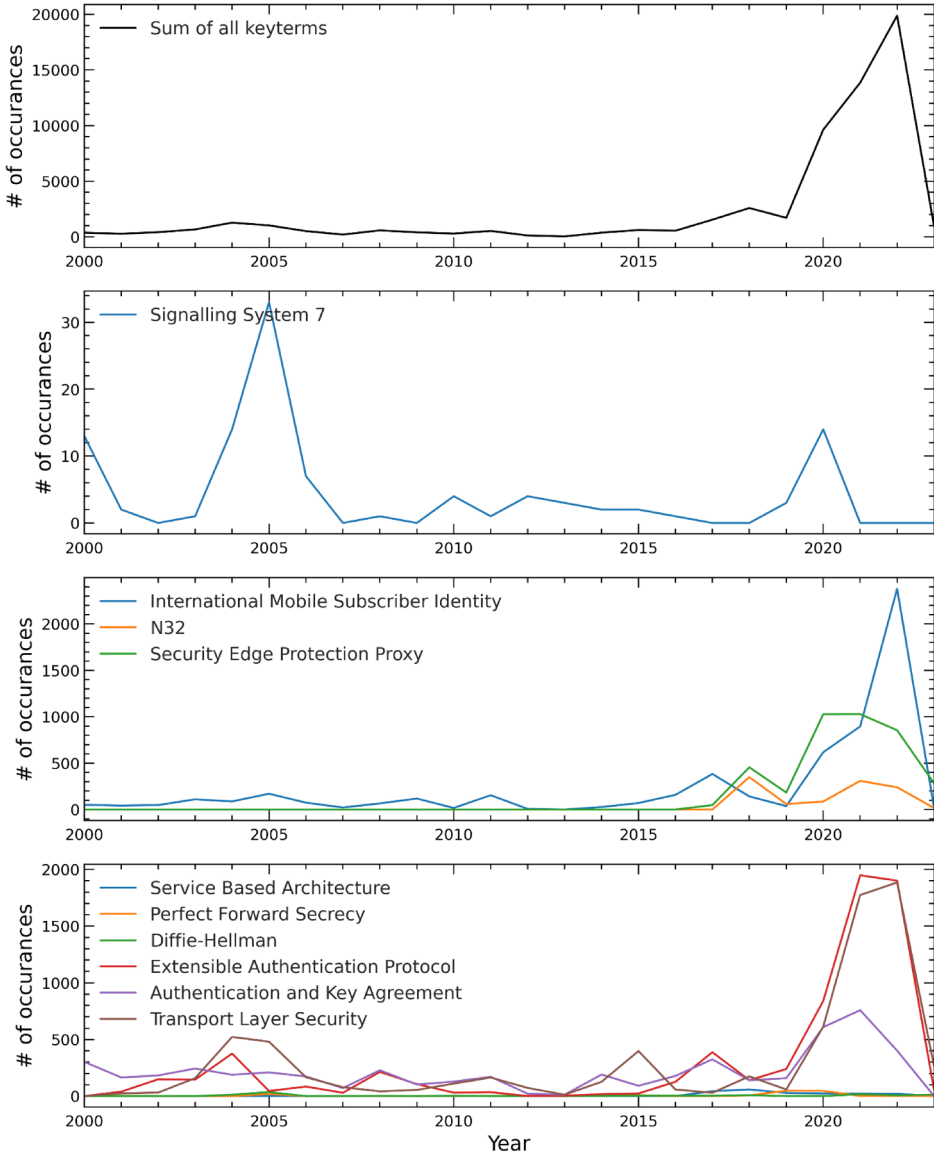
In panel (c), we can identify China, the United States, Sweden, Finland, and France as the countries that host headquarters of stakeholders that are most active in the mailing lists. The figure leaves no doubt that the influence of Chinese stakeholders on matters of security and privacy has increased substantially since the rollout of 5G networks.

Figure 2 shows the cumulative amount of emails (top panel), as well as the keywords mentioned in the bodies of the emails related to the three cases. Figure 3 visualizes patterns of engagements through a directional communication graph,  $G_T$ , of all emails in  $T$ , in which each node represents a different email domain name and each edge is a communication channel between sender and receiver. To clarify, all emails are received by all mailing list subscribers, but they can be directed as replies (“comments-to” header field) to specific senders (“from” header field). As there are 445 unique domain names found in the “from” and “comments-to” header fields of the combined mailing lists, we only highlight the top 20 edges and their associated nodes that experienced the most email traffic between 2000–2020 (left) and 2020–2022 (right) to preserve clarity. The size of a node is indicative of the number of emails sent by those stakeholders, while the color and thickness of an edge are indicative of the number of emails that were sent along it (as quantified by the color bar at the bottom of the figure). Loops, as in chinamobile.com on the left, indicate interstakeholder communication. Straight edges indicate that the receiver has not sent a reply, while curved edges show that a dialogue has taken place. From the communication graph for 2000–2020 (left), we can conclude that Nokia has been one of the most engaged stakeholders. From the communication graph for 2020–2022 (right), we see that the role of Huawei has become more dominant, which has many exchanges with Ericsson and Nokia.

Figure 4 shows a quotient graph,  $G_c$ , of  $G_T$  in which all stakeholders and email traffic have been merged based on their stakeholder category (as defined in the methods section above). It follows the same node size and edge style, color, and thickness conventions as Figure 5. The stakeholder categories that have sent most emails between 2000 and 2020 are networking equipment vendors and telecommunication providers, with most of their email traffic contained within this constellation. So it does not come as a surprise to find that they have the largest  $C_D$ ,  $C_B$ , and  $C_C$ . This situation changes after 2020, when we see that most email traffic took place between networking equipment vendors and consulting firms. Comparing  $G_c$  for that period with  $G_s$  shown in Figure 2, we see clearly that those two stakeholder categories are dominated by Ericsson, Nokia, Huawei, and Trideaworks. Trideaworks is contracted by the FBI to implement United States surveillance standards into global standards. Consulting companies are on top of the list, followed by networking equipment vendors, for their  $C_D$ ,  $C_B$ , and  $C_C$ . Big changes compared to the 2000 to 2020 period can be observed for Trideaworks who have become noticeably more active.

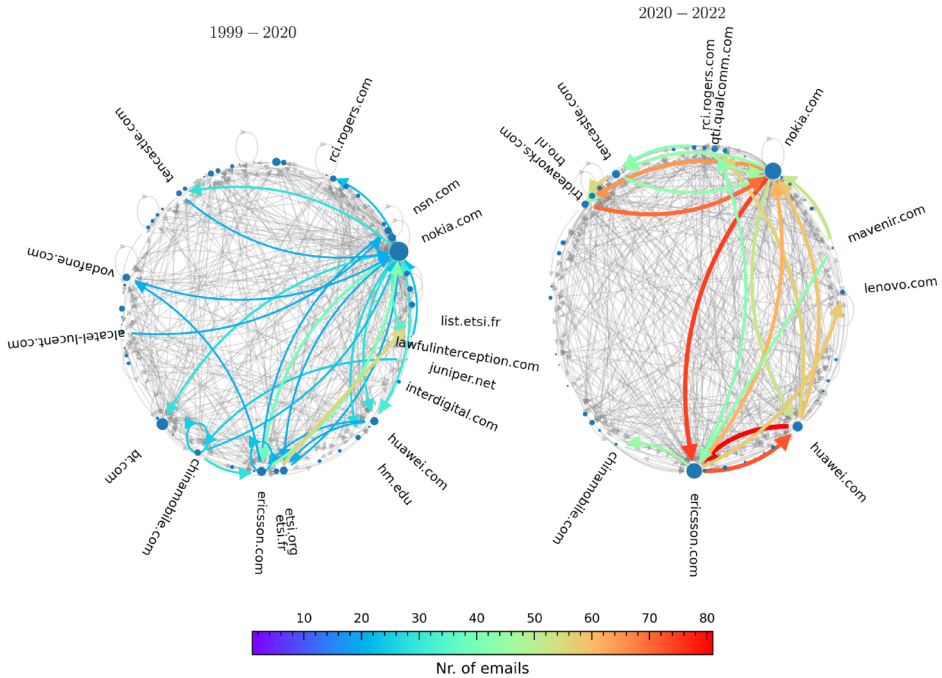
Figure 5 shows a quotient graph,  $G_n$ , of  $G_s$  in which all stakeholders and email traffic have been merged based on the stakeholder’s nationality (as defined in Methods section). It follows the same node size and edge style, color, and thickness conventions as Figure 2. The edges along which most emails were sent, in the period between 2000 and 2020, are from Sweden, Germany, China,





**Figure 2.** The top panel shows the total number of documents (emails including their attachments and meeting reports) that are included in the target set (T) per year. The second to fourth panel from the top filters out documents that relate to cases 1, 2, and 3 respectively.

France, Great Britain, South Korea, and the Netherlands. However, compared to the  $G_s$  and  $G_c$  graph, the email traffic in  $G_n$  is distributed in such a way among the nodes, that a clear dominance over the graph can't be attributed. This changes after 2020, revealed through several observations. Firstly, the intensification of communication between Huawei and Ericsson is reflected in  $G_n$  by the edges connecting Sweden and China. Secondly, China occupies a dominant position by having the largest  $C_D$ ,  $C_B$ , and  $C_C$ .

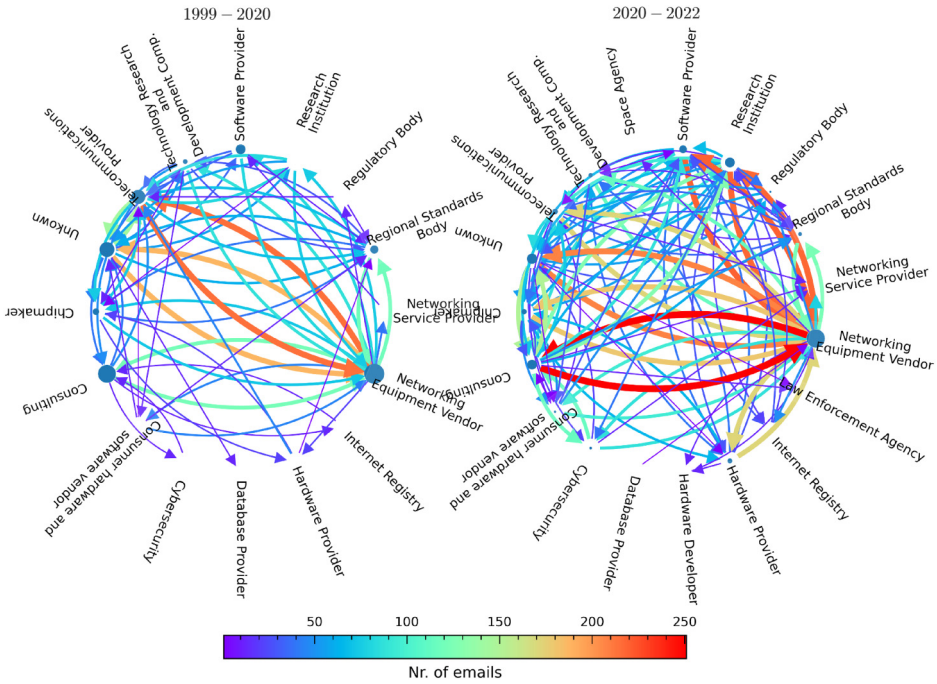


**Figure 3.** Communication graph, GT, between domains in the T set. Only the top 20 edges, along with the most emails sent, are shown in color, all other edges are grayed out to make the figure more readable.

### *Insecurity as a bug... and a feature*

In the 3GPP mailing list activity of the Working Group on Privacy and Security, and the subgroup on Lawful Intercept within the Technical Specification Group on Service & System Aspects, we can find mentions and discussions of the SS7 vulnerabilities, fake base stations, as well as the lack of Perfect Forward Secrecy (Figure 1). This allows us to confirm that the actors in the 3GPP are aware of the existing vulnerabilities. However, upon qualitative analysis of the mailinglists, we do not find a structural discussion of solutions to the insecurities. The only solutions that are offered are based on the development and deployment of new protocols. In the case of SS7, this was done through the introduction of the Diameter protocol, which *eventually* will replace SS7 when all networks preceding 4G will be retired. But since this will likely take quite some time, the insecurities that exist in SS7, and will likely persist for quite some time since SS7 and Diameter are interoperable.

In the case of IMSI catchers, the introduction of encrypted identifiers as protection against fake base stations happened only in 5G protocols. In both cases, no direct response, update, or fix has been developed or deployed in existing and running systems that are more than likely to exist for quite a while. Even though the website of the Working Group on Privacy and Security describes the Technical Specification Group Service and System Aspects “and the 3GPP Mobile Competence Centre have implemented a process to allow suspected or proven vulnerability caused by errors, omissions or ambiguities in our Technical Specifications to be reported and quickly forwarded to the appropriate 3GPP Group, to analyse and resolve the problem.”<sup>6</sup> However, in the first two cases, namely the SS7 vulnerabilities and the vulnerability that allowed for fake base stations, also known as IMSI catchers, the responsibility to fix these issues has been pushed forward to

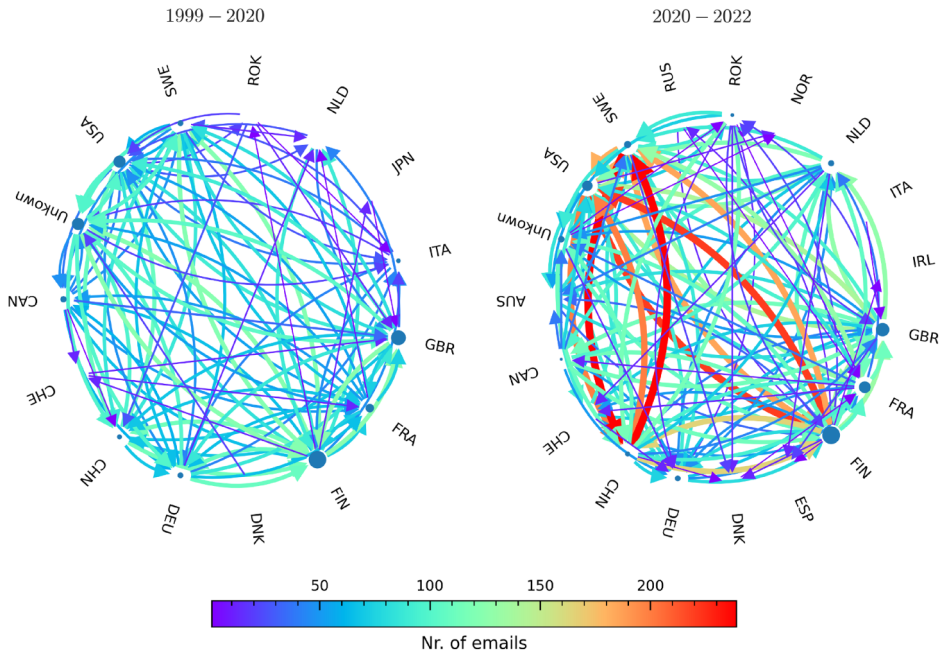


**Figure 4.** Communication graph,  $G_c$ , in which stakeholders in  $G_s$  were combined based on their category. Between 2000 and 2020 (left), and 2020–2022 (right) have been among the most active on the mailing list.

the deployment of the full replacement of the protocol. In the case of SS7, this was the Diameter protocol, and in the case of IMSI vulnerability, this was the deployment of encrypted identifiers in 5G. However, in many cases when 5G is deployed, this is done so in Non-Standalone Mode (5G NSA), meaning it is deployed in conjunction with 4G. In these cases, IMSI catchers still work.<sup>7</sup>

The lack of discussion on concrete solutions, and the continuation of the existence of vulnerabilities in new hybrid deployments, led us to closer analyze meeting reports of the Working Group on Privacy and Security. There we found evidence for actual rejections against the introduction of fixes that are not discussed on the mailinglists. This means that fixes did exist, but were resisted by equipment manufacturers, network operators, and other participants in the standardization process. Here it is important to highlight the changes we saw in Figures 2 and 3. During the period 1999–2020, in which the first two vulnerabilities occurred. The most active participants were network operators and equipment manufacturers. In the period after that, 2022–2022, the composition of the mailinglists changed and many new actors joined the mailinglists. This can in part be attributed to the heightened interest in 5G, which led to an increase in participation from China, but also due to an increase of new stakeholder groups: consultants and research institutions. Most notably TrideaWorks and TNO. In previous work, we have shown that these organizations in this context work respectively for law enforcement agencies in the United States and the Netherlands (Becker et al., 2022).

When one observes the minutes of the discussion of the introduction of Perfect Forward Secrecy in 5G in EAP, during the meeting of the 3GPP Working Group on Privacy and Security in 2019 in Reno, USA,<sup>8</sup> one can observe a recurring pattern. A solution to this existing vulnerability is proposed (in this case by Ericsson), where the Thales representative responds: “it’s been four times



**Figure 5.** Communication graph,  $G_n$ , in which stakeholders in  $G_s$  were combined based on their location. Until 2020 (left), the states whose stakeholders were most active in the mailing list were Sweden, Germany, China, France, Great Britain, South Korea, and The Netherlands. Since 2020 (right), the engagement between Swedish and Chinese stakeholders intensified, while the United States is being positioned as a central actor through which much of the email traffic is channeled.

that this contribution has been brought here and last time there was a show of hands and it was rejected. We still object to the additional complexity that the addition of PFS mechanisms will bring.” Thales publicly advertises itself as a provider of surveillance methods. When Ericsson asked for a vote, the Thales position was supported by IDEMIA, Qualcomm, Orange, and Vodafone. While the introduction of the security feature was supported by Apple, Ericsson, Nokia, ZTE, China Mobile, Huawei, ZTE, HP, and T-Mobile. Here it is particularly interesting to see that hardware and identity providers from the United States, Great Britain, and France are blocking the introduction of safety measures. Specifically, since Great Britain and the United States engaged in the Gemalto hack. A cursory analysis seems to suggest that a persistent insecurity, more popularly called as “backdoor,” is in the interest of particular countries because they have access to these backdoors. What is also interesting is that companies that are contracted to represent government interests, such as TrideaWorks and TNO, do not vote in this instance, even though they work in the field of standardizing Lawful Intercept interfaces. This could indicate that the purposeful maintenance of infrastructural insecurities serves another goal than the standardization of lawful intercept interfaces. One possible explanation could be that it is illegal for national security services to engage in mass surveillance of their populations, and therefore enable other security services of other countries to do it for them.

It might not be a surprise for the reader that transnational communication networks are used to project power (Choudhury, 2010; Hills, 2007), nor that nation-states engage in surveillance through these networks (DeNardis, 2014; Zajacz, 2019). Some authors even argue that surveillance is an inherent part of these networks (Wu, 2011). However, generally international standardization is

perceived as a trust-building activity that produces safety and security (Yates and Murphy, 2019). This is why the introduction of weaker security standards by the NSA of the United States, as was revealed during the Snowden revelations (Rogers and Eden, 2017), brought about such a shock that internet governance organizations took a stance against pervasive surveillance, the IETF even called pervasive monitoring an attack on the internet (Farrell and Tschofenig, 2014). However, within the 3GPP we do not see an active response against exposed vulnerabilities. This maintenance of infrastructural insecurity can be interpreted as an act of infrastructural geopolitics (de Goede and Westermeier, 2022) and as an act of governance by infrastructure (DeNardis and Musiani, 2016).

## **Standardizing and maintaining infrastructural insecurities**

In this article, we have analyzed the responses of the foremost telecommunication standardization body, the 3GPP, to three significant insecurities in telecommunication networks. In none of the cases, the SDO provided a conclusive solution, even though they were aware of the existence of the vulnerabilities. In every case, we did find evidence of the awareness of these vulnerabilities and their discussion in the 3GPP. At the same time, exploitation of the vulnerabilities by nation-state actors and their services were consistently observed and documented in academic literature and trade press. These vulnerabilities were all of an architectural nature, so arguably a standards body that developed the standards was the best body to address these issues. However, responses to the vulnerabilities were very slow and inconclusive in the first two cases—since they would only be solved if the original architecture would be completely phased out and replaced. In the third case, namely, that of the proposed implementation of Perfect Forward Secrecy, a solution to the vulnerability of static key exfiltration from the world’s largest SIM card manufacturer Gemalto by the United States and Great Britain, was structurally rejected by companies from the United States, the United Kingdom, and France, leaving a structural insecurity present in fifth generation telecommunication networks. The inclusion of this security feature was supported by companies from China, Europe, and the United States. This insecurity is of the nature that it can only be used by significantly resourced actors—and has in the past been exploited by the secret services of the United States and the United Kingdom.

The maintenance of infrastructural insecurities in telecommunication networks goes against the widely spread conception that standardization provides safety and security. It suggests that standardization is part of infrastructural geopolitics (de Goede and Westermeier, 2022) and that “standards can be politics by other means” (Abbate, 1999: 179). What this article showed is a way in which this has not been conceptualized before, namely the maintenance of publicly known vulnerabilities. Above we have shown that network insecurities that are regularly exploited by governments for surveillance purposes are maintained even in new-generation telecommunications (5G) networks—and improvements are blocked, in this case by companies from the United States, the United Kingdom, and France.

We contribute to the theoretical debate about communication infrastructures and the role of standardization by introducing the concept of infrastructural insecurities. We coined this term to foreground the work being done to produce, maintain, and standardize insecurities to benefit particular actors. This is a contribution because in policy circles and academic literatures, standard-setting is often conceptualized as a process that produces safety and security, and by default serves in the public interest. In this case, we show the exact opposite and foreground state and industry collusion in this process. This is particularly relevant because the United States and others have accused China and particularly the company Huawei of introducing vulnerabilities in 5G. This article shows vulnerabilities in 5G are maintained by companies from the United

States, Great Britain, and France namely Thales, IDEMIA, Qualcomm, Orange, and Vodafone. No case of Huawei engaging in such acts has been found or documented.

Both research and policymaking could benefit from quantitative and qualitative analysis to further understand security, insecurity, and power in the process of standard-setting of communication infrastructures, and new methods should be developed to better research this sprawling field. This could benefit the understanding of standard-setting, as well as transparency, legitimacy, and trustworthiness of the infrastructure of contemporary information societies.


### Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Internet Society Foundation (contract number DB1/117723749.1), and Ford Foundation (grant number A-202208-06454, 144895).

### ORCID iD

Niels ten Oever  <https://orcid.org/0000-0001-5134-2199>

### Notes

1. <https://www.icann.org/en/announcements/details/montevideo-statement-on-the-future-of-internet-cooperation-7-10-2013-en> accessed on August 8, 2023.
2. <https://www.ohchr.org/en/calls-for-input/2023/call-inputs-relationship-between-human-rights-and-technical-standard-setting> accessed on August 8, 2023.
3. [https://www.etsi.org/deliver/etsi\\_ts/123500\\_123599/123501/17.05.00\\_60/ts\\_123501v170500p.pdf](https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/17.05.00_60/ts_123501v170500p.pdf) accessed on April 7, 2023.
4. [https://mailarchive.ietf.org/arch/msg/emu/mc3iCXqsjbPgu2NK1usxdO\\_vtC8/](https://mailarchive.ietf.org/arch/msg/emu/mc3iCXqsjbPgu2NK1usxdO_vtC8/) accessed on April 7, 2023.
5. <https://www.wired.com/2015/02/gemalto-confirms-hacked-insists-nsa-didnt-get-crypto-keys/> accessed on April 7, 2023.
6. <https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3> accessed on August 15, 2023.
7. <https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-5G-IMSI-Catchers-Mirage.pdf> accessed on August 16, 2023.
8. [https://www.3gpp.org/ftp/TSG\\_SA/WG3\\_Security/TSGS3\\_97\\_Reno/Report/MeetingReport\\_\\_SA3\\_97.docx](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_97_Reno/Report/MeetingReport__SA3_97.docx) accessed on April 7, 2023.

### References

- Abbate J (1999) *Inventing the Internet*. Inside Technology. Cambridge, MA: The MIT Press.
- Aradau C (2010) Security that matters: critical infrastructure and objects of protection. *Security Dialogue* 41(5): 491–514.
- Aradau C and Blanke T (2015) The (big) data-security assemblage: knowledge and critique. *Big Data & Society* 2(2): 2053951715609066.
- Asmolv G and Kolozaridi P (2021) Run Runet runaway: the transformation of the Russian Internet as a cultural-historical object. In: *The Palgrave Handbook of Digital Russia Studies*. London, UK: Palgrave Macmillan, pp.277–296.
- Baron J and Kanevskaia Whitaker O (2021) Global competition for leadership positions in standards development organizations. *SSRN Scholarly Paper ID 3818143*. Social Science Research Network, Rochester, NY. DOI: 10.2139/ssrn.3818143.

- Baron J and Pohlmann T (2018) Mapping standards to patents using declarations of standard-essential patents. *Journal of Economics & Management Strategy* 27(3): 504–534.
- Becker C, ten Oever N and Nanni R (2022) The standardisation of lawful interception technologies in the 3GPP: interrogating 5G and surveillance Amid US-China competition. In: Proceedings of the 50th Research Conference on Communication, Information and Internet Policy (TPRC 2022), Washington DC, USA. DOI: 10.2139/ssrn.4167105.
- Benthall S, Ten Oever N, Doty N, et al. (2021) Bigbang. Available at: <https://github.com/datactive/bigbang>.
- Bowker GC, Baker K, Millerand F, et al. (2010) Toward information infrastructure studies: ways of knowing in a networked environment. In: J Hunsinger, L Klastrup and M Allen (eds) *International Handbook of Internet Research*. Dordrecht: Springer Netherlands, pp.97–117. DOI: 10.1007/978-1-4020-9789-8\_5.
- Brown MB (2015) Politicizing science: conceptions of politics in science and technology studies. *Social Studies of Science* 45(1): 3–30.
- Bryson J and Winfield A (2017) Standardizing ethical design for artificial intelligence and autonomous systems. *Computer* 50(5): 116–119.
- Buchanan B (2020) *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press.
- Burgess JP (2019) The insecurity of critique. *Security Dialogue* 50(1): 95–111.
- Campbell K (2004) The promise of feminist reflexivities: developing Donna Haraway’s project for feminist science studies. *Hypatia* 19(1): 162–182.
- Carey JW (1983) Technology and ideology: the case of the telegraph. *Prospects* 8: 303–325.
- Carmi E (2019) The hidden listeners: regulating the line from telephone operators to content moderators. *International Journal of Communication* 13(0): 19.
- Carmi E (2020) *Media Distortions: Understanding the Power behind Spam, Noise, and Other Deviant Media*. Lausanne, Switzerland: Peter Lang International Academic Publishers.
- Cath C (2018) Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376(2133): 20180080.
- Cath C (2021) The technology we choose to create: human rights advocacy in the Internet Engineering Task Force. *Telecommunications Policy, Norm entrepreneurship in Internet Governance*, 45(6): 102144.
- Cavusoglu H, Cavusoglu H and Raghunathan S (2007) Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Transactions on Software Engineering* 33(3): 171–185.
- Choudhury DKL (2010) *Telegraphic Imperialism: Crisis and Panic in the Indian Empire, C. 1830-1920*. New York City, NY: Springer.
- De Goede M and Westermeier C (2022) Infrastructural geopolitics. *International Studies Quarterly* 66(3): sqac033.
- DeNardis L (2009) *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press.
- DeNardis L (2014) *The Global War for Internet Governance*. New Haven: Yale University Press.
- DeNardis L, Musiani F (2016) Governance by infrastructure. In: F Musiani, DL Cogburn, L DeNardis, et al. (eds) *The Turn to Infrastructure in Internet Governance*. Information Technology and Global Governance. New York: Palgrave Macmillan, pp.3–21. DOI: 10.1057/9781137483591\_1.
- Doty N (2020) *Enacting privacy in Internet standards*. Doctoral Dissertation, University of California, Berkeley, CA, USA. <https://npdoty.name/enacting-privacy/>.
- Dryburgh L and Hewett J (2005) *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services*. Indianapolis, Indiana: Cisco Press.
- Easterling K (2014) *Extrastatecraft: The Power of Infrastructure Space*. London, UK: Verso Books.
- Edwards PN (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.
- Edwards PN (2021) Platforms are infrastructures on fire. In: TS Mullaney, B Peters, M Hicks, et al. (eds) *Your Computer is on Fire*. Cambridge, MA: MIT Press. pp.313–336.
- Engel T (2009) 25C3: locating mobile phones using SS7. In: 25th Chaos Communication Congress, January 10, 2009. <https://fahrplan.events.ccc.de/congress/2008/Fahrplan/events/2997.en.html>.
- Ermoshina K, Loveluck B and Musiani F (2022) A market of black boxes: the political economy of internet surveillance and censorship in Russia. *Journal of Information Technology & Politics* 19(1): 18–33.

- Ermoshina K and Musiani F (2017) Migrating servers, elusive users: reconfigurations of the Russian Internet in the post-Snowden era. *Media and Communication* 5(1): 42–53.
- Estrada MS and Lehuédé S (2022) Towards a terrestrial Internet: re-imagining digital networks from the ground up. *Tapuya: Latin American Science, Technology and Society* 5(1): 2139913.
- Farrell S and Tschofenig H (2014) RFC7258—pervasive monitoring is an attack. RFC-Series. RFC Editor. Available at: <https://tools.ietf.org/html/rfc7258>.
- Feamster N and Rexford J (2017) Why (and how) networks should run themselves. *arXiv:1710.11583 [Cs]*, October. Available at: <http://arxiv.org/abs/1710.11583>.
- Fontugne R, Ermoshina K and Aben E (2020) The Internet in Crimea: a case study on routing interregnum. In: 2020 IFIP Networking Conference, Paris, France. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>.
- Haraway DJ (1988) Situated knowledges: the science question in feminism and the privilege of partial perspective. *Feminist Studies* 14(3): 575–599.
- Haraway DJ (1991) *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York City, NY: Routledge.
- Hardin NV (2017) Uncovering the secrecy of stingrays: what every practitioner needs to know. *Criminal Justice* 32: 20.
- Hills J (2007) *Telecommunications and Empire*. Champaign, IL: University of Illinois Press.
- Hogewoning M (2020) Update on WTSa-20 preparations and new IP. RIPE Labs. October 11, 2020. Available at: [https://labs.ripe.net/author/marco\\_hogewoning/update-on-wtsa-20-preparations-and-new-ip/](https://labs.ripe.net/author/marco_hogewoning/update-on-wtsa-20-preparations-and-new-ip/).
- Huang Y, Huppenbauer N and Mayer M (2022) Infrastructuring cyberspace: exploring China’s imaginary and practices of selective connectivity. *International Quarterly for Asian Studies* 53(3): 413–439.
- King G, Lam P and Roberts M (2017) Computer-assisted keyword and document set discovery from unstructured text. *American Journal of Political Science* 61(4): 971–988.
- Krause K and Williams MC (2002) *Critical Security Studies: Concepts and Strategies*. New York City, NY: Routledge.
- Laurent B (2022) *European Objects: The Troubled Dreams of Harmonization*. Cambridge, MA: MIT Press.
- Liboiron M (2021) *Pollution is Colonialism*. Durham, NC: Duke University Press.
- Limonier K, Douzet F, Pétiinaud L, et al. (2021) Mapping the routes of the Internet for geopolitics: the case of Eastern Ukraine. *First Monday* (April). DOI: 10.5210/fm.v26i5.11700.
- Luconi V and Vecchio A (2022) Impact of the first months of war on routing and latency in Ukraine. *arXiv*. DOI: 10.48550/arXiv.2208.09202.
- Mai T, Garg S, Yao H, et al. (2021) In-network intelligence control: toward a self-driving networking architecture. *IEEE Network* 35(2): 53–59.
- Mascitelli B and Chung M (2019) Hue and cry over Huawei: cold war tensions, security threats or anti-competitive behaviour? *Research in Globalization* 1(December): 100002.
- Maxigas and ten Oever N (2023) Geopolitics in the infrastructural ideology of 5G. *Global Media and China* 8(3): 271–288.
- McKelvey F (2018) *Internet Daemons: Digital Communications Possessed*. Minneapolis, MN: University of Minnesota Press.
- Paris B (2020) The Internet of futures past: values trajectories of networking protocol projects. *Science, Technology, & Human Values* 46(5). DOI: 10.1177/0162243920974083.
- Parks L (2016) Rise of the IMSI catcher. *Media Fields Journal* 11.
- Pohlmann T, Blind K and Heß P (2020) Fact finding study on patents declared to the 5G standard.
- Rogers M and Eden G (2017) The snowden disclosures, technical standards, and the making of surveillance infrastructures. *International Journal of Communication* 11(0): 22.
- Rühlig T and Björk M (2020) What to make of the Huawei debate? 5G network security and technology dependency in Europe. *UI Paper, Swedish Institute of International Affairs*.
- Sharp H and Kolkman O (2020) Discussion paper: an analysis of the ‘new IP’ proposal to the ITU-T. *Internet Society*, April, 13.
- Söderberg J (2013) Determining social change: the role of technological determinism in the collective action framing of hackers. *New Media & Society* 15(8): 1277–1293.
- Stadnik I (2019) Internet governance in Russia—Sovereign basics for independent Runet. In: Proceedings of the 47th Research Conference on Communication, Information and Internet Policy (TPRC 2019), Washington DC.



- Star SL (1999) The ethnography of infrastructure. *American Behavioral Scientist* 43(3): 377–391.
- Teki'r G (2020) Huawei, 5G network and digital geopolitics. *International Journal of Politics and Security* 2(4 (Çin Özel Sayısı)): 113–135.
- ten Oever N (2022) 5G and the notion of network ideology, or: the limitations of sociotechnical imaginaries. *Telecommunications Policy* 47(5): 102442.
- ten Oever N and Milan S (2022) The making of international communication standards: towards a theory of power in standardization. *Journal of Standardisation* 1. DOI: 10.18757/jos.2022.6205.
- Veale M and Borgese FZ (2021) Demystifying the draft EU Artificial Intelligence Act—analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International* 22(4): 97–112.
- Wen Y (2020) *The Huawei Model: The Rise of China's Technology Giant*, 1st ed. Urbana, IL: University of Illinois Press.
- Wiener N (1950) *The Human Use of Human Beings: Cybernetics and Society*. Cambridge, MA: The Riverside Press.
- Wilton R (2017) After Snowden—the evolving landscape of privacy and technology. *Journal of Information, Communication and Ethics in Society* 15(3): 328–335.
- Wolfe HB (2017) The mobile phone as surveillance device: progress, perils, and protective measures. *Computer* 50(11): 50–58.
- Wu T (2011) *The Master Switch: The Rise and Fall of Information Empires*. New York City, NY: Vintage Book.
- Wyatt S (2008) Technological determinism is dead; long live technological determinism. In: E Hackett, O Amsterdamska, M Lynch, et al. (eds) *Handbook of Science and Technology Studies*. Cambridge, MA: MIT Press, pp.165–180.
- Yates J and Murphy CN (2019) *Engineering Rules: Global Standard Setting since 1880*. Baltimore, MD: John Hopkins University Press.
- Zajacz R (2019) *Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century*. Cambridge: The MIT Press.