Information, Communication & Society

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rics20

Interrogating the standardisation of surveillance in 5G amid US–China competition

Christoph Becker, Niels ten Oever & Riccardo Nanni

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2024.2302991

Interrogating the standardisation of surveillance in 5G amid US–China competition

Christoph Becker[a], Niels ten Oever[b] and Riccardo Nanni [c]

[a]Independent researcher, Brussels; [b]Media Studies Department, University of Amsterdam, Amsterdam, the Netherlands; [c]Digital Commons Lab, Fondazione Bruno Kessler, Trento, Italy

ABSTRACT

In this article we show that the 5G competition between the United States and Western Europe versus China is not reflected in the standardisation of lawful interception (LI) technologies in the world's leading telecommunications standardisation body, the 3rd Generation Partnership Project (3GPP). Guided by the concept of infrastructure as a site and tool of political contestation, we develop a new approach to the study of Internet governance and standard-setting processes that leverages web scraping and computer-assisted document set discovery software tools. We bring these methods into conversation with theoretical approaches from material media studies, science and technology studies, and international relations. The 3GPP is the main telecommunications standardisation body and the only consortium developing standards to fulfil the ITU's criteria for the 5th generation of telecommunications technology (5G). The 3GPP therefore is a strategic venue to observe and interpret the politics of standardisation processes. As such, the LI-related work conducted in 3GPP exemplifies public and private actors' capacity to influence global surveillance standards and export their surveillance technologies. While European and United States governments engage in the standardisation of surveillance technologies, the Chinese government does not do this in the 3GPP. This fuels distrust in 5G technologies. We argue that further integration of China in standardisation could function as a trust-building measure.

ARTICLE HISTORY
Received 22 February 2023
Accepted 2 January 2024

KEYWORDS
Lawful interception; China; 5G; Huawei; International relations; Standardisation

Introduction

The introduction of 5G, the fifth generation of telecommunication technologies, has led to a significant amount of controversy. In December 2018, Meng Wanzhou, the Chief Financial Officer of Huawei who was also the daughter of its founder Ren Zhengfei, was arrested and held under house arrest for three years in Canada at the request of the United States (US) Government under suspicion of financial fraud (Wen, 2020), this case was settled out of court later. In 2019 the United States instated sanctions against Huawei and sought to influence European countries to do the same, citing security concerns, with varying levels of success (Poggetti, 2021). The Trump administration states

CONTACT Riccardo Nanni rnanni@fbk.eu Digital Commons Lab, Fondazione Bruno Kessler, Via Sommarive 18, 38123 Trento, Italy

national security concerns as the reason for these actions: specifically, China's potential (though never proven) ability to gain access to US citizens, businesses, and military communications (ten Oever, 2022).

The debate over surveillance and security in telecommunication networks is by no means a new one (Tang, 2020). The Telegraph Convention of 1875 already mentions what one could call 'state surveillance' by today's standards: for comparison, the first transatlantic telecommunications cable was laid in 1865 (Penney, 2015). Some researchers therefore argue that censorship and surveillance are inherent parts of the development of information networks (Wu, 2011).

The production of transnational communication networks happens through a process of standardisation (Drake, 2000; Kammerer, 2010; Russell, 2014; Yates & Murphy, 2019). The standardisation of telecommunication technologies happens in different institutions. In this article, we look at the role of standardisation in producing surveillance techniques in telecommunication standardisation. When the International Telecommunications Union (ITU) declared what technologies lived up to the qualifications for the third generation of telecommunication technologies, also called 3G, there were still three competing standards (TD-SCDMA largely developed in China,[1] CDMA2000 largely developed by North American and Asian actors, and UMTS largely developed by European actors). For 5G, the fifth generation, only the 3rd Generation Partnership Project (3GPP) is left as an umbrella body under which mobile telecommunications get produced to live up to the ITU's IMT-2020 requirements. This is why in this article, we particularly look at the standardisation of so-called 'lawful interception' standards in the 3GPP because this umbrella body is currently the dominant standards organisation that is producing telecommunications standards for mobile telephony networks.

In our interrogation of the practice of standardisation of state surveillance approaches, we ask the question: who standardises 'lawful intercept' approaches to telecommunications technologies in the 3GPP? This question is relevant because many of the claims underpinning the conflict between the United States and China in the case of Huawei and 5G concern the security of the network, and the possible or potential presence of so-called 'backdoors' (Kaska et al., 2019). To critically question this narrative we developed a hypothesis that states that the standardisation of 'lawful intercept' approaches is led by European countries and implemented by all equipment manufacturers. We expected to find that European governmental regulators and their consultants make requests for lawful intercept techniques in the 3GPP and that the United States does not do so in the 3GPP because it does so in the national standards bodies Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA), where they explicitly seek to conform with the United States' The Communications Assistance for Law Enforcement Act (CALEA). Because of the size and importance of the US market, manufacturers will seek to comply with these standards. We expected to find a similar outcome for China.

We build on data science methods and bring them into conversation with theoretical frameworks and approaches from science and technology studies. This allows us to interrogate the role of material infrastructure in the reconfiguration of (geo)politics (Aradau, 2010).

We first provide an overview of the literature that outlines the history of telecommunications and surveillance to then discuss how this is epitomised in the discussions on 5G. Subsequently, we provide a theoretical framework to understand this discussion. After that, we describe our methods and provide an analysis, discussion, and conclusion.

Literature review

History of telecommunications and surveillance

The emergence and following society-wide permeation of telecommunication technology increased the demands of states to ensure surveillance capabilities are deployed for law enforcement agencies (LEAs) to conduct surveillance operations (Lauer, 2011; Zajko, 2016). This produced a two-layer dialectic: privacy vs. public order (broadly defined) on the one hand and public authority (state) vs. private power (private network providers) on the other (ten Oever, 2022; Wen, 2020). First, the limits for governments to intrude on citizens' private lives to combat crime and security threats are blurred (Khan et al., 2020). Second, state authorities and private companies pursue different interests, which can conflict or overlap (Cartwright, 2020).

In the standardisation process of lawful intercept (LI) technologies, governments produce regulatory requests and requirements and companies create a common ground for compliance through international standards (Zajko, 2016). An example of such a process from the 1990s is the US Clipper Chip Initiative. In the conviction that the increased usage of encryption was eroding LEAs' powers, the US government weighed in on standardisation processes and sought to internationalise its lawful intercept standards (Pednekar-Magal & Shields, 2003). While this initiative failed, the US National Security Agency (NSA) has sought to influence international surveillance standards consistent with its mission (Cartwright, 2020). This includes the promotion of US domestic standards, but also covert actions such as the inclusion of backdoors in cryptographic standards later adopted by the International Organization for Standardization (ISO) (Rogers & Eden, 2017). In this process, surveillance gets progressively embedded in technical infrastructures (Gekker & Hind, 2019).

In the history of lawful intercept technologies, two sets of specifications are particularly widespread: the European standard ETSI LI and US-elaborated specifications based on CALEA. The former is the standard elaborated by the European Telecommunications Standards Institute (ETSI), while the latter was elaborated in the US and endorsed by the NSA (Munoz et al., 2015). Meanwhile, other countries developed lawful intercept standards as well. As per this article's focus, the China Communications Standards Association (CCSA) developed technical specifications coherent with Beijing's regulations. While tracing CCSA standardisation work is far from straightforward – not least for non-native Chinese speakers – one can observe LI-related work within CCSA's Technical Committee 260 (TC260) (China Communications Standards Association, 2020).

The spread of mobile communication devices happened in parallel with their increase in functionality. In twenty years, mobile phones have transformed from mere telephony devices to fully-fledged pocket computers with applications for any purpose, from banking to bike rental, making it problematic to live without in most regions of the world (Sicari et al., 2020). This has led to the development and proliferation of a large number of standards and processes pertaining to mobile devices. The increased uptake and functionality have been matched with an interest in the standardisation of LI to access voice and data services. At the same time, societal concerns and debates about privacy and surveillance have also increased, however, this is not necessarily reflected in all standardisation processes.

In short, telecommunications policy has been increasingly incorporated into mainstream politics as telecommunication devices have become part of everyday life. This casts new challenges and perhaps also expectations for the standardisation work of bodies such as the 3GPP (Munoz et al., 2015).

As mentioned above, the 3GPP is chosen as the object of research of this article because it is the main venue for telecommunications standardisation, including the LI-related aspects (Kumar et al., 2012). When the ITU sets the technical and functional requirements for the next-generation telephony infrastructure, several industry consortia entered into action to devise a technology that meets such requirements. For the 5th generation of telecommunications technologies, only the 3GPP is devising standards for recognition by the ITU. When a piece of technology is recognised by the ITU as one of the international standards of next-generation telephony infrastructure, its profitability in terms of royalty increases thanks to the increased likelihood of global implementation. The ITU recognises as a new generation telephony infrastructure standard any proposed standard that meets its requirements, independently of whether all the approved standards are compatible. For example, the ITU recognised three separate 3G standards incompatible with each other. Of the many consortia that feed into this ITU process, 3GPP is historically the main one since 3G, with its technologies always constituting at least one of the ITU-recognised telephony infrastructure standards (Nanni, 2021; ten Oever, 2022). All the main global telecommunication equipment manufacturers, including companies such as Huawei, Samsung, Ericsson, Nokia, and Qualcomm, participate in 3GPP processes. At the current stage, Huawei is one of the main contributors to 5G standardisation on par with companies such as Ericsson and Samsung (Pohlmann et al., 2020), although their role in 3GPP's LI-related work is not as dominant, as the analysis below will show.

The ITU is historically a venue in which China, especially since the early 2000s, has sought to build a strong representation. The Chinese government indicated the ITU as the one legitimate venue in which Internet governance (not only telecommunications) should take place (Negro, 2020). China also aspires to obtain leadership positions in the ITU; until 2022 even the Secretary General of the ITU hailed from China. While the broader field of Internet governance falls outside the scope of this paper, these pieces of information are indicative of China's and Chinese companies' strong positioning and interest vis-à-vis ITU and ITU-aligned processes.

In short, the 3GPP is directly aligned with the ITU and is the main body of telecommunications standardisation. The 3GPP therefore is a strategic venue to observe and interpret the politics of standardisation processes. As such, the LI-related work conducted in 3GPP exemplifies public and private actors' capacity to influence global surveillance standards and export their surveillance technologies (Han et al., 2009). On this ground, the next subsection expands on the politics of 5G among the US, China, and the EU, while the remainder of the article addresses 3GPP's LI-related work as a locus for the making of surveillance standards amid the US–China competition.

Global contestation on 5G security: US, China and the EU

While 5G standardisation is still ongoing at the time of writing, the question of future mobile connectivity standards and infrastructure safety has become part of power politics

(Seaman, 2020). The US protectionist push against Chinese network manufacturers, based on still un-demonstrated security arguments (ten Oever, 2022), opened the way to a new trend against open markets in several technology sectors (Ciuriak, 2019).

The US–China competition in the connectivity sector comes with a major element of tension. On the one hand, standard convergence is visible: radio standards are increasingly compatible at the global level with 5G. On the other hand, the global 5G network manufacturing market is fragmenting along geopolitical lines, with an increasing number of European and North American countries imposing limitations on Chinese manufacturers' presence in the national 5G infrastructure (Poggetti, 2021).

In short, these contrasting trends have been driven by securitisation (ten Oever, 2022) along with economic objectives (Ciuriak, 2019). Huawei's growth opened the way for Chinese companies to carry unprecedented influence in 5G standardisation at the same level as well-established Western manufacturers (Pohlmann et al., 2020), whereas 3G international standardisation was mainly a game among Europe, North America, and likeminded Asian countries such as Japan and South Korea. The relative growth of corporate actors like Huawei compared to US and European industries constitutes a driver in the US's protectionist measures (Ciuriak, 2019; Seaman, 2020; Teleanu, 2021).

The combination of economic and political interests behind standardisation makes the connection between standards and geopolitical power explicit. From a corporate perspective, having a patented technology included in an internationally recognised standard brings royalties, whereas, from a state's perspective, this same aspect brings industrial advantage (Kim et al., 2020). In turn, this is conflated in securitised discourses within the US–China competition.

Rhetoric notwithstanding, the privacy-security/surveillance conundrum is a longstanding one in telecommunications policy (Penney, 2015). Notwithstanding recent media attention, the incorporation of interception technologies in telecommunication infrastructures by design has been a given in standardisation activities (American Enterprise Institute, 2014). With the growing pervasiveness of telecommunications technology, this intrinsic conundrum of LI technologies persists and becomes increasingly evident. Beyond its politicisation in the public international discourse, the making of LI technology is intrinsically untransparent: below the surface level of international standardisation, the details of LI technology functioning need to be inaccessible to the general public for these tools to be workable for LEAs in fighting crime (Munoz et al., 2015).

Notwithstanding these critical elements of opacity, an increasing number of governments are establishing legal requirements for such technologies to be present in the infrastructure. In this, 3GPP has incorporated lawful interception technology standardisation in its work to establish minimum agreed standards for 3G through 5G infrastructures (Munoz et al., 2015). Currently, this work is conducted within the 3GPP working group in charge of architectural security.

Theoretical debates concerning telecommunications and surveillance

The authors depart from debates in Science and Technology Studies (STS) that describe infrastructure as a site and tool of political contestation (Musiani, 2013). This is to say, governments promote standards elaborated by domestic companies internationally for economic gain and to cast national influence (Zajacz, 2019). This takes place in a context of dialectic relations between state and capital, where the latter receives incentives and constraints from the former while trying to shift and influence state policies to pursue market interests (Shen, 2016). In the specific case of lawful interception, the relation between state and capital is one in which the latter has to fulfil the legal requirements of the former while seeking to maximise financial revenues in terms of royalties over the patents that are incorporated in the international standard(s). From the state's perspective, domestic companies can be a tool to promote domestic legal requirements and surveillance technology into internationally adopted standards (Munoz et al., 2015). Furthermore, across and within countries capital is characterised by competition among companies, which may partially overlap with competition among states. In this view, the technological trade competition between the US and China is an example of power politics: limitations established against Chinese companies in 5G networks follow geopolitical lines, with countries closer to the US adopting a stricter stance (Poggetti, 2021). In this context, China's growing participation in the 3GPP is showing its ascendance into the world system (Pohlmann et al., 2020). However, this ascendance is hampered by fears over (geo)political tensions that unfold through economic protectionism. This is not only affecting the integration of China into the world system but also contributing to global infrastructural fragmentation and territorialisation of cyberspace (Drake et al., 2016; Lambach, 2019; Mueller, 2017).

In this article, we observe the aforementioned dynamics in a particular subset of 5G standard-setting, namely lawful interception, which constitutes the basis to contend the narrative on China's attempt to export surveillance through standards.

Methods

To examine infrastructure as a site and tool of political contestation, we developed an approach to the study of Internet governance and standard-setting processes that leverages web scraping and computer-assisted document set discovery software tools. This approach opens up new spaces and enables text-as-data analysis of corpora that goes beyond traditional methods, for example, discursive and thematic analysis methods typical for the social sciences (Grimmer et al., 2022; ten Oever, 2022). What we obtain are new perspectives on participants' involvement, communication, dominance, and absence within 3GPP's standard-setting processes. This informs the study of the governance of communication infrastructures by combining methods hailing from different disciplines, mirroring the interdisciplinary nature of standard-setting itself.

Our findings are based on a text corpus that is composed of 3GPP's LI working group public mailing list[2] (from now on referred to as LI mailing list) and their published standards (www.etsi.org/standards-search). In Internet governance, the study of mailing lists has hitherto found surprisingly little attention, despite their wealth of information (ten Oever et al. 2020). Previous works have explored mailing lists of IETF and W3C (Doty, 2020; ten Oever, 2018; Welzl et al., 2021). However, we are the first to uncover 3GPP mailing lists for its multitude of insights through the expansion of the open-source BigBang software package (Benthall et al., 2021) to allow for the ingress of the particular type of mailing list software used by the 3GPP, namely Listserv 17.0.

While one might think that the use of mailing lists has dwindled, the LI mailing list shows otherwise (see Figure 1). Email is still commonly used in Standard Developing

Organizations, arguably because of the global and interoperable nature of email and the availability of mailing list software that is relatively easy to administer and provides a wide range of options, including archiving features. This makes mailing lists a unique decision-making cloud chamber, as they trace the informal and formal exchange and coordination between actors all the way to decision-making. Using Bigbang (Benthall et al., 2021), we retrieved the mailing list on the 6th of March 2022, which contains 6419 messages and 349 attachments sent since 2000.

Before we bring to the fore relations and associations between involved stakeholders, we group emails into sets of those that address purely managerial and organisational matters (for example meeting reminders and travel advice), and those that focus on legal and technical aspects of surveillance. Thus, from now on we will denote these two sets of emails as S\T and T (to which we will refer as the target set), depending on whether they belong to the former or latter respectively, while the set of all emails in the entire LI mailing list is referred to as S. To partition S, into T and S\T, we apply techniques for unstructured and unlabelled text corpora that rely on both human experts and machine learning algorithms (King et al., 2017). Together, they converge to a list of

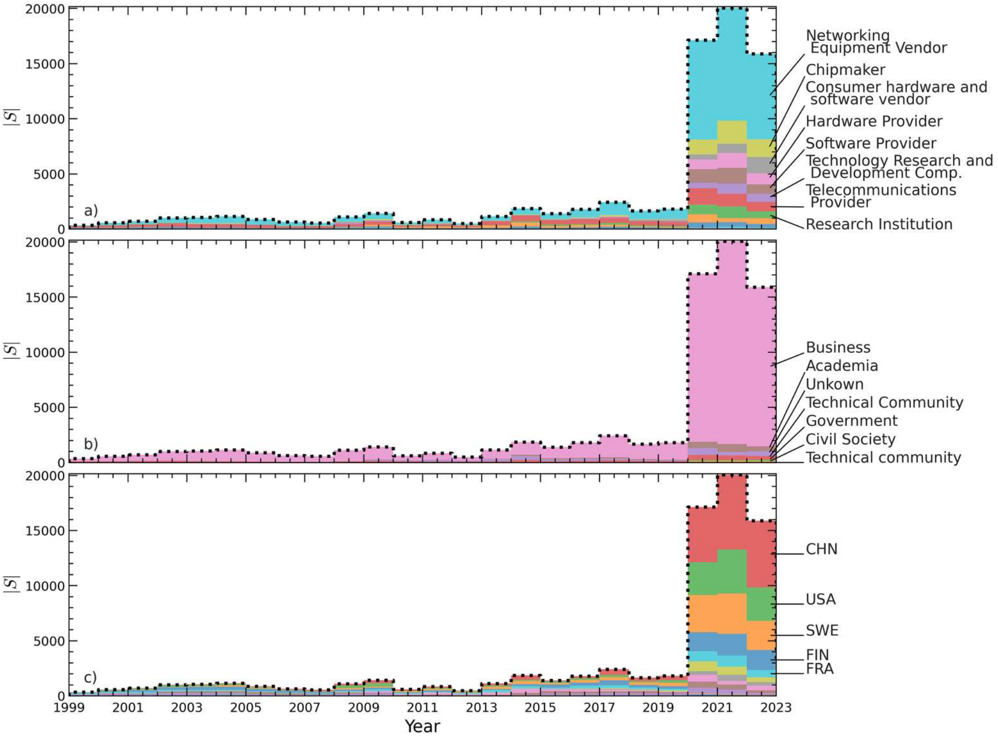

Figure 1. Panels (a), (b), and (c) show the set size of all emails, |S|, sent per year through a black dotted line, that is filled in with colour that indicates the stakeholder's market category, sector, and the headquarter location of (parent) organisation respectively. Panel (d) visualises the relative difference between |S| and |T|, where the latter is the target set size per year. The set T is a subset of S that contains only those Emails that focus on legal and technical aspects of surveillance, excluding all contents of pure managerial and organisational matters.

key terms which we compose into queries using the Boolean OR operator that identifies emails of interest.[3]

The final list of key terms highlights that T is best identified through abbreviations and their long form (for example PoI = 'Point of Interception'). This comes with little surprise, as they are at the core of technical discussions and need to maintain their notation and meaning to ensure effective communication. On the other hand, messages that contain words such as 'conference', 'hotel', and 'reminder' are likely to be of mere managerial nature and are thus discarded. By applying the Boolean query we identify in total 3177 emails that belong to T.

Stakeholder classification

The header information of each email contains valuable information such as sender and receiver email addresses and timestamps. Email addresses contain a local- and domain-part which are separated by the '@' symbol. Using the domain, one can identify from which stakeholder an email was sent/received (for example nokia.com indicates a message was sent on behalf of NOKIA). Only in a few cases do mailing list participants use a private Gmail account which conceals for which stakeholder they work. We have labelled them as 'Unknown' in our analysis. To map communication patterns between stakeholder groups and nationalities, we created a table containing the top 100 domains that send the most messages, their Category(-ies), of whom the companies to whom the domain was registered are a subsidiary, to which stakeholder group they belong, and their nationality based on their Headquarter location. We argue that for our purposes we can equate the nationality of subsidiaries to the parent organisation because one can grosso modo expect the external strategies and approaches of subsidiaries to align with the interests of the parent company in standardisation (Asakawa, 2001; Cantwell & Janne, 1999; Chang et al., 2009).

Analysis

The history of the standardisation of surveillance in the 3GPP

The standardisation of lawful intercept technologies in the 3GPP goes back at least until September 2000, when the LI mailing list started according to the archives. The 3GPP uses the following definition of lawful intercept:

> Laws of individual nations and regional institutions (e.g., European Union), and sometimes licensing and operating conditions define a need to intercept telecommunications traffic and related information in modern telecommunications systems. It has to be noted that lawful interception shall always be done in accordance with the applicable national or regional laws and technical regulations. (3GPP, 2017, p. 4)

In Figure 1, the black dotted line in panels (a), (b), and (c) show the set size of all emails, |S|, sent per year. The historic trend appears similar to a bimodal distribution, with two periods of intensified communication between 2001–2005 and 2015–2022. These peaks can be explained by the standardisation of 3G in the first period, and the development of 5G in the second period. The reason the second period saw even more traffic could be attributed to the fact that during 3G, there were still three SDOs engaged in 3G standardisation, and for 5G only the 3GPP remained. The reason there was less activity during 4G is that this was widely seen as a release with fewer new features than 3G or 5G.

Each of the three panels shows in colour 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) organisation. Starting from the top, we can identify network equipment vendors, public finances and economic policy, and telecommunications providers to be among the main contributors to the standardisation process of LI in 3GPP since its inception. Consulting companies have become a dominant player only since 2020. The three least contributive organisations can be grouped into technology research and development companies, consumer hardware and software vendors, and chipmakers. Judging by the history of stakeholder categories, it comes with little surprise that the dominant stakeholder group comes from the business sector, followed by governmental, technical communities, and academia. In panel (c), we can identify Great Britain, the United States, Finland, France, and Germany to be the countries that host headquarters of stakeholders that are most active in surveillance standardisation. Interestingly, no more than 21 emails, none of them belonging to the target set T, have been sent by stakeholders located in China, namely Huawei and ZTE. In all three panels, the number of emails sent by 'Unknown' stakeholders is small enough to not change the result qualitatively. At the bottom of the same figure, panel (d), we show the relative difference per year between the size of set T and S (emails that explicitly address lawful interception and emails that contain purely managerial and organisational matters, as outlined in Sec. 2) and notice the following trends. Firstly, the time series of |T| follows the set size of all emails, |S|, sent per year. Secondly, generally, less than half of all send emails per year, S, belong to T except in 2018 and since 2020.

Patterns of engagement: stakeholders, market categories, and countries

Figure 2 visualises patterns of engagements through a directional communication graph, Gs, of all emails in T, in which each node represents a different email domain name and each edge a communication channel between sender and receiver. To clarify, all emails are received by all mailing list subscribers (a total of 246 subscribers in May 2022), but they can be directed as replies ('comments-to' header field) to specific senders ('from' header field). As there are 158 unique domain names found in the 'from' and 'comments-to' header fields (showing, that some subscribers do not participate), 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 colour and thickness of an edge are indicative of the number of emails that were sent along it (as quantified by the colour bar at the bottom of the figure). Loops, for example Telstra on the left, indicate inter-stakeholder communication. Straight edges, for example from Telstra to Ericsson on the left, indicate that the receiver has not sent a reply. Curved edges, for example between Nokia and Tridea Works on the right, show that a dialogue has taken place. From the communication graph for 2000–2020 (left), we can conclude that Nokia maintained the biggest number of engagement partners, having had contact with almost double as many stakeholders as any other. Together with BT, Nokia had the highest degree (CD), betweenness (CB) and closeness centrality (CC) compared to any

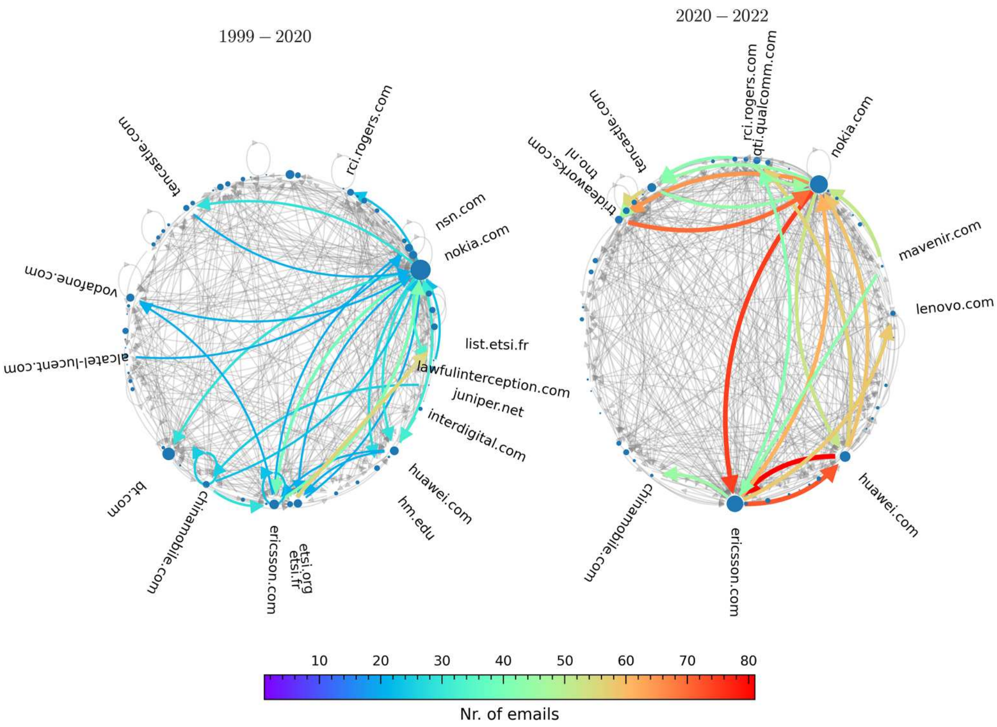

Figure 2. Communication graph, Gs, between domains in the T set. Only the top 20 edges, along with the most emails sent, are shown in colour, all other edges are greyed out to make the figure more readable. Between 2000 and 2020 (left), Nokia is seen to have been a central actor in the standardisation process of surveillance. The centrality of Nokia has to change during the 2020–2022 period (right), but its engagement with Tridea Works experienced an immense uptake.

other stakeholder. From the communication graph for 2020–2022 (right), we see that the communication between Nokia and Tridea Works, which already commenced before 2020, intensified. Tencastle and Tridea Works have upscaled their numbers of engagement partners to an equal height to Nokia, and together they dominate the mailing list activities, having the largest CD, CB, and CC.

Figure 3 shows a quotient graph, Gc, of Gs 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, colour, and thickness conventions as Figure 2. The stakeholder categories that have sent most emails between 2000 and 2020 are telecommunications providers, networking equipment vendors, and consulting, 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 CD, CB, and CC. This situation changed after 2020, when we saw that most email traffic took place between networking equipment vendors and consulting companies. Comparing Gc for that period with Gs shown in Figure 2, we see clearly that those two stakeholder categories are dominated by Nokia and Tridea Works. Consulting companies are on top of the list, followed by networking equipment vendors, for their CD, CB, and CC. Big changes compared to the 2000–2020 period can be observed for law enforcement agencies and cybersecurity companies who have become noticeably more active. For the graphs of both periods,

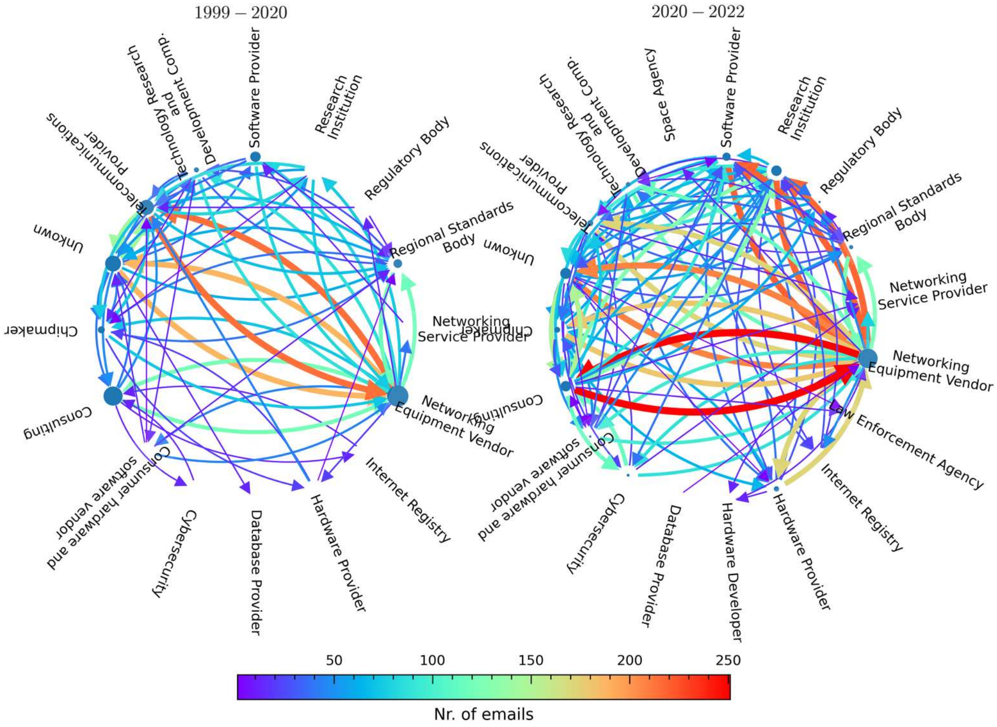

Figure 3. Communication graph, Gc, in which stakeholders in Gs were combined based on their category. Between 2000 and 2020 (left), telecommunications providers, networking equipment vendors, and consulting firms have been among the most active on the mailing list. The communication between the latter two intensified since 2020 (right), reflecting our observation of Figure 2 as they are both dominated by Nokia and Tridea Works respectively.

we verified that the stakeholders without a category attribute (labelled in the figure as 'Unknown') do not change the findings outlined above, by comparing the email traffic of the 'Unknown' to the categories mentioned above.

Figure 4 shows a quotient graph, Gn, of Gs in which all stakeholders and email traffic have been merged based on the stakeholder's nationality (as defined in Sec. Methods). It follows the same node size and edge style, colour, and thickness conventions as Figure 2. The edges along which most emails were sent, in the period between 2000 and 2020, are from Finnish (dominated by Nokia), stakeholders with Canada (mostly with Rogers Communications Inc. and Nortel Networks Corporation), and Great Britain (mostly Tencastle Ltd. and BT). However, compared to the Gs and Gc graph, the email traffic in Gn 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 Nokia and Tridea Works is reflected in Gn by the edges connecting Finland and the US. Secondly, Great Britain occupies a dominant position by having the largest CD, CB, and CC. For the graphs of both periods, we verified that the stakeholders without a nationality attribute (labelled in the figure as 'Unknown') do not change the findings outlined above, by comparing the email traffic of the 'Unknown' to the states mentioned above.

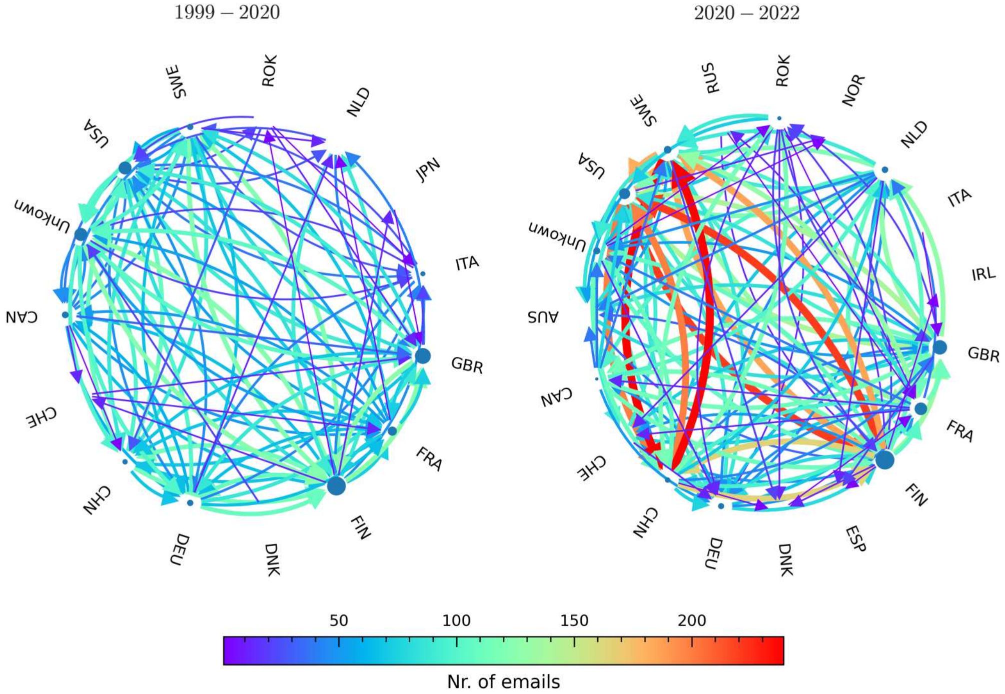

Figure 4. Communication graph, Gn, in which stakeholders in Gs were combined based on their location. Until 2020 (left), the states whose stakeholders were most active on the mailing list were Finland, Canada, and Great Britain. Since 2020 (right), the engagement between Finnish and US stakeholders intensified, while Great Britain is being positioned as a central actor through which much of the email traffic is channelled.

Of companies and (some) states

We have already remarked that in the most recent period of telecommunications standardisation, namely the standardisation of 5G, there is an increase in participation from law enforcement agencies and cybersecurity companies (see Figure 3). In the dynamic on the mailing list, one can differentiate through discourse analysis a distribution which could be described as the requesters of certain functions and actors who implement them. The latter group are the equipment manufacturers and network operators, but the requesters are not always solely government agencies. A paradigmatic example is Tridea Works. Tridea Works is a regular requester for particular surveillance features, that is not itself a government, but a consulting company that works for the US government. On an online government services platform of the US government Tridea Works describes itself as follows: 'Tridea Works has been and continues to be involved in the development of technical requirements on behalf of a government agency in a number of industry forums and standards-setting organizations [*sic*]'.[4] Furthermore, Tridea Works LLC has an ongoing contract with the United States Department of Justice's Federal Bureau of Investigation (FBI).[5] In a presentation to the 3GPP, a Tridea Works employee described themselves as consultants to the CALEA Implementation Unit Technical Implementation Section, which is a section of the FBI. The standardisation of lawful intercept in the US is largely led through preconditions set in CALEA legislation that are subsequently technically standardised in ATIS and TIA. The agreed standards are subsequently absorbed by companies, in part due to the size of the market in the US, and aligned from the national level to the international (from ATIS and TIA to the 3GPP) by Tridea Works. Also other consultants publicly declare their collaborations with law enforcement, such as the Dutch TNO, which is also active in lawful intercept standardisation. This shows some complexity in sectoral categorisation for analysis, however cursory discursive analysis rather quickly provides a relatively easily observable distinction.

Whereas corporations act on behalf of particular state interests, no clear indication could be found of governments acting on behalf of corporations. This could in part be due to the particular state interest in lawful intercept or due to the nature of standardisation itself, which is mostly operationalised through market actors (Yates & Murphy, 2019). What could be observed is that it is largely European governments and the United States government through Tridea Works that engage in the requesting features and functionalities for the standardisation of surveillance techniques in 3GPP to North American, European, and Asian corporations.

Inversely, actors that shine through their absence in the standardisation of lawful intercept techniques in telecommunications standards are Chinese governmental or regulatory actors and civil society organisations. Furthermore, when compared to discussions in other standards fora, such as the Internet Engineering Task Force, relatively little contestation is observed on the mailing lists. This could be attributed to a different standardisation culture or, what is more likely, discussions and agreements that are being made outside of the public mailing lists at meetings or through other backchannels. Because an average of one email per day for the entire mailing list does not allow for extensive technical discussion of complex telecommunication architectures. So whereas public mailing lists might provide more transparency, this by no means equals total transparency of deliberation.

The key to good eavesdropping is not getting caught. Or not?

The analysis of the standardisation of lawful intercept in the 3GPP presented above yields three conclusions. Firstly, it shows that governments are directly influencing the shaping of telecommunication standards through the participation of regulators (for example, see panel b) in (Figure 1), and indirect influence by using consultants that act on their behalf. This verifies the theoretical framework brought forward by Musiani (2013; Zajacz, 2019) that describes network infrastructure figuration as an act of governance. More specifically in the telephony infrastructure, governments identify national 'champions' to financially support in their effort to internationalise their technical solutions (Wen, 2020). When it comes to lawful interception, such effort can be overt or covert as illustrated in the literature review (Rogers & Eden, 2017).

Secondly, there was no direct or obvious reflection of the imposition of trade barriers by the United States or European countries in the standardisation of 5G – all actors present work together to produce interoperable telecommunication networks. However, the lack of interaction by Chinese government regulators in discussions on lawful interception could be identified both as a source and as a consequence of these trade barriers. Since there is a long tradition of state surveillance in telecommunication, the lack of direct Chinese engagement leaves the US and European countries in the dark about the surveillance approaches of the Chinese government. This could be a reason for the imposition of sanctions and subsequently could also dissuade Chinese participation. We identify this as a missed chance because the standardisation of lawful intercept in global bodies could function as a confidence-building measure. The technological standardisation sector provides incentives for collaboration among economic actors in the form of scale economies. In other words, an actor such as Huawei finds it more economically profitable to produce one device and one network on a global scale rather than producing several of each for different markets, as the latter scenario decreases scale economies and hence increases the production cost of each single device (Wen, 2020). Nonetheless, growing competition and mutual mistrust between the aforementioned competing parties increase barriers to cooperation and the likelihood of technological fragmentation, which at this stage is visible only on a market level (Poggetti, 2021).

Thirdly, and building on the previous point, the lack of engagement of Chinese actors in the standardisation of lawful intercept in the 3GPP shows an uneven integration of the Chinese in the world system of standardisation. Whereas Chinese participation in the 3GPP overall is at an all-time high (Pohlmann et al., 2020), this is not reflected in governmental participation, nor is it reflected in the 3GPP working group standardising LI. This could be attributed to Chinese governance approaches that are characterised by long-term strategies, for instance through multiannual plans, the distribution of competencies to local authorities in terms of infrastructure building (Hong, 2017), and anticipatory governance by companies (Wen, 2020). While much of the standardisation of legal intercept for the United States happens in national standards bodies such as ATIS and TIA, traces of such practices in China could be found in the national standards body CCSA, but it was unclear whether these techniques and approaches are integrated into 3GPP standards or international devices. This mismatch could lead to increased distrust in Chinese technologies because of asymmetric strategies that are not conducive to a converging standardisation practice.

One could consider the standardisation of lawful intercept approaches as a process to restore and increase trust and collaboration in communication infrastructures, to ensure other states and actors understand the surveillance needs and capabilities of other states. This point could be elaborated based on the literature on International Relations Theory, which indicates that sharing information through formalised international regimes increases mutual trust (Alter & Raustiala, 2018). In this view, standardisation venues such as 3GPP are globally recognised fora where industry (and, to an extent, states) share information and find common ground on the functioning of strategic technology (Nanni, 2021).

Conclusion

In this article, we interrogated the practice of the standardisation of ‘lawful intercept’, or state-mandated surveillance technologies in the main telecommunications standardisation body in the world, the 3GPP. The analysis shows that governments both directly and indirectly influence the shaping of telecommunication standards, and thus use both standardisation and the figuration of infrastructure as a means of governance. Furthermore, the analysis allows us to conclude that the standardisation of ‘lawful intercept’ technologies for telecommunications networks takes place in the 3GPP and is driven by European and North American governments and their consultants. The requests made by these governments and their consultants are subsequently incorporated into telecommunications standards by the acceptance of all represented equipment manufacturers and network operators.

The fact that the Chinese government is not directly involved in the standardisation of surveillance, at least as far as 3GPP's LI mailing list activities are concerned, possibly is giving rise to the suspicion that Huawei is doing this on their behalf. This suspicion is partly fuelled by indirect control the Chinese government can exercise on the company through ownership affiliations. However, the analysis did not reveal any request made by Huawei to integrate particular surveillance techniques in the 5G standard. This statement is limited to mailing list activities within 3GPP's LI standardisation subgroup, while further research on collaboration between Huawei and the Chinese authorities within Chinese standardisation fora may yield different results.

Finally, the analysis does not show any impact of the sanctions on Huawei on the collaboration between Chinese and other companies. This leads the authors to suggest that further integration of standardisation of lawful intercept technologies could lead to an easing of geopolitical tensions, especially since all actors already work together in the 3GPP.

The methodological innovations made in this article help show how mailinglist data can help shed light on processes of standardisation and other forms of communication governance. While they do not provide a complete picture of state-company or company-to-company relations, mailing lists do help in observing the everyday rollout of standardisation work and the competition and collaboration dynamics thereof. This also underlines the importance of the availability of public data of communications governance bodies to enable researchers and policymakers to validate claims made about standardisation processes and thereby enhance their legitimacy.

Notes

1. While being promoted by the Chinese government, the development of TD-SCDMA involved a large number of international (including European) actors as these were dominant in the Chinese infrastructure market at the time. Indeed, the large presence of foreign manufacturers in the Chinese market is often seen as an early incentive for a company like Huawei to internationalise and seek penetration in foreign markets. For a deeper account, see Wen (2020).
2. https://list.etsi.org/scripts/wa.exe?A0=3GPP_TSG_SA_WG3_LI accessed on May 12, 2022
3. For the code and obtained key term list see: [ANONYMIZED FOR REVIEW]
4. Further contractual information is retrievable from: https://www.gsaadvantage.gov/ref_text/GS35F316AA/0X0FDO.3SQSCD_GS-35F-316AA_TRIDEAPRICELISTWITHNEWPHONEPA0015MARCH2022.PDF accessed on January 20, 2023.
5. For further information on the contract, see: https://govtribe.com/award/federal-idv-award/indefinite-delivery-contract-djfjfbi08236 accessed on May 18, 2022.

Acknowledgements

The authors thank the guest editors of this special issue and the anonymous peer reviewers. Contributions to this paper by Niels ten Oever were made possible through funding from the Dutch

Research Council (NWO) through grant MVI.19.032 as part of the program 'Maatschappelijk Verantwoord Innoveren (MVI)', the Ford Foundation, and the Internet Society (DB1/117723749.1). This work was also supported by the Prototype Fund, a funding program of the Federal Ministry of Education and Research (BMBF) that is managed and evaluated by the Open Knowledge Foundation Germany.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Bundesministerium fÃr Bildung und Forschung [grant number: Prototype Fund]; Ford Foundation [grant number:]; Internet Society [grant number: DB1/117723749.1]; Nederlandse Organisatie voor Wetenschappelijk Onderzoek [grant number: MVI.19.032].

Notes on contributors

Christoph Becker is an independent researcher. He holds a PhD in Physics from Durham University.

Niels ten Oever is a co-founder of the Critical Infrastructure Lab and a postdoctoral researcher with the 'Making the hidden visible: Co-designing for public values in standards-making and governance'-project at the Media Studies department at the University of Amsterdam. In his research, Niels tries to understand how invisible infrastructures provide a socio-technical ordering to information societies and how this influences the distribution of wealth, power, and possibilities.

Riccardo Nanni is Researcher in Data Governance at the Digital Commons Lab of Fondazione Bruno Kessler. He holds a PhD in International Relations from the University of Bologna and his research interest is in the broader field of digital governance. He is active in the Global Internet Governance Academic Network and the Internet Governance Forum.

ORCID

Riccardo Nanni http://orcid.org/0000-0002-2773-4093

References

3GPP. (2017). *Universal mobile telecommunications system (UMTS); LTE; 3G security; Lawful interception requirements* (Technical Specification Group Services and System Aspects TS 33.106 version 14.0.0 Release 14). 3GPP. https://www.etsi.org/deliver/etsi_ts/133100_133199/133106/14.00.00_60/ts_133106v140000p.pdf

Alter, K. J., & Raustiala, K. (2018). The rise of international regime complexity. *Annual Review of Law and Social Science*, *14*(1), 329–349. https://doi.org/10.1146/annurev-lawsocsci-101317-030830

American Enterprise Institute. (2014). *Cyber surveillance regulations: Is the United States asking China to accept a double standard?* American Enterprise Institute. https://www.aei.org/research-products/report/cyber-surveillance-regulations-is-the-united-states-asking-china-to-accept-a-double-standard/.

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491–514. https://doi.org/10.1177/0967010610382687

Asakawa, K. (2001). Evolving headquarters-subsidiary dynamics in international R&D: The case of Japanese multinationals. *R&D Management*, *31*(1), 1–14. https://doi.org/10.1111/1467-9310.00192

Benthall, S., Ten Oever, N., Doty, N., & Becker, C. (2021). *Bigbang* [Computer software]. https://github.com/datactive/bigbang

Cantwell, J., & Janne, O. (1999). Technological globalisation and innovative centres: The role of corporate technological leadership and locational hierarchy. This paper represents one contribution to the TSER project on Technology, Economic Integration and Social Cohesion (contract no. SOE1-CT95-1005).1. *Research Policy*, *28*(2), 119–144. https://doi.org/10.1016/S0048-7333(98)00118-8

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei, and geopolitical struggle. *Internet Policy Review*, *9*(3), 1–19.

Chang, Y. Y., Mellahi, K., & Wilkinson, A. (2009). Control of subsidiaries of MNCs from emerging economies in developed countries: The case of Taiwanese MNCs in the UK. *The International Journal of Human Resource Management*, *20*(1), 75–95. https://doi.org/10.1080/09585190802528383

China Communications Standards Association. (2020). *CCSA Organisational Structure*. http://www.ccsa.org.cn/orgnization?title=%E7%BB%84%E7%BB%87%E6%9E%B6%E6%9E%8

Ciuriak, D. (2019). The US-China trade war: Technological roots and WTO responses. *Global Solutions Journal*, *4*, 130–135.

Doty, N. (2020). *Enacting privacy in internet standards* [University of California]. https://npdoty.name/writing/enacting-privacy/

Drake, W. J. (2000). Rise and decline of the international telecommunications regime. In C. Marsden (Ed.), *Regulating the global information society* (pp. 124–177). Routledge.

Drake, W. J., Cerf, V. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview*. World Economic Forum. https://www.weforum.org/reports/internet-fragmentation-an-overview

Gekker, A., & Hind, S. (2019). Infrastructural surveillance. *New Media and Society*, *0*(0), 1–23.

Grimmer, J., Roberts, M. E., & Stewart, B. M. (2022). *Text as data: A new framework for machine learning and the social sciences*. Princeton University Press.

Han, K., Yeun, C. Y., & Kim, K. (2009). *New key escrow model for the lawful interception in 3GPP*. IEEEXplore.

Hong, Y. (2017). *Networking China: The digital transformation of the chinese economy (Illustrated edition)*. University of Illinois Press.

Kammerer, P. (2010). Off the leash. The european mobile phone standard (GSM) as a transnational telecommunications infrastructure. In A. Badenoch, & A. Fickers (Eds.), *Materializing Europe: Transnational infrastructures and the project of europe* (pp. 202–222). Palgrave Macmillan UK. https://doi.org/10.1057/9780230292314_13

Kaska, K., Beckvard, H., & Minárik, T. (2019). *Huawei, 5G and China as a security threat* (p. 26). The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, *22*(1), 196–248. https://doi.org/10.1109/COMST.2019.2933899

Kim, M., Lee, H., & Kwak, J. (2020). The changing patterns of China's international standardization in ICT under techno-nationalism: A reflection through 5G standardization. *International Journal of Information Management*, *54*, 1–8.

King, G., Lam, P., & Roberts, M. E. (2017). Computer-assisted keyword and document set discovery from unstructured text: Keyword and document set discovery. *American Journal of Political Science*, *61*(4), 971–988. https://doi.org/10.1111/ajps.12291

Kumar, A., Sengupta, J., & Liu, Y. (2012). 3GPP LTE: The future of mobile broadband. *Wireless Pers Commun*, *62*, 671–686.

Lambach, D. (2019). The territorialization of cyberspace. *International Studies Review*, 1–25. https://doi.org/10.1093/isr/viz022

Lauer, J. (2011). Surveillance history and the history of new media: An evidential paradigm. *New Media and Society*, *14*(4), 566–582.

Mueller, M. (2017). *Will the Internet fragment?: Sovereignty, globalization and cyberspace*. Polity Press.

Munoz, A., Uruena, M., Aparicio, R., & Rodriguez de los Santos, G. (2015). Digital wiretap warrant: Improving the security of ETSI lawful interception. *Digital Investigation*, *14*, 1–16.

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*, *2*(4), 1–9.

Nanni, R. (2021). The 'China' question in mobile Internet standard-making: Insights from expert interviews. *Telecommunications Policy*, *45*(6), 1–12. https://doi.org/10.1016/j.telpol.2021.102151

Negro, G. (2020). A history of Chinese global Internet governance and its relations with ITU and ICANN. *Chinese Journal of Communication*, *13*(1), 104–121. https://doi.org/10.1080/17544750.2019.1650789

Pednekar-Magal, V., & Shields, P. (2003). The state and telecom surveillance policy: The clipper chip initiative. *Communication Law and Policy*, *8*(4), 429–464.

Penney, J. W. (2015). The cycles of global telecommunication censorship and surveillance. *University of Pennsylvania Journal of International Law*, *36*(3), 693.

Poggetti, L. (2021). *EU-China Mappings: Interactions between the EU and China on Key Issues*. Mercator Institute for China Studies.

Pohlmann, T., Blind, K., & Hess, P. (2020). *Fact finding study on patents declared to the 5G standard*. IPlytics.

Rogers, M., & Eden, G. (2017). The Snowden disclosures, technical standards, and the making of surveillance infrastructures. *International Journal of Communication*, *11*, 802–823.

Russell, A. L. (2014). *Open standards and the digital age*. Cambridge University Press.

Seaman, J. (2020). *China and the new geopolitics of technical standardization* (p. 34). Notes de l'Ifri.

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G In the internet of things era: An overview on security and privacy challenges. *Computer Networks*, *179*, 1–12. https://doi.org/10.1016/j.comnet.2020.107345

Tang, M. (2020). Huawei versus the United States? The geopolitics of exterritorial internet infrastructure. *International Journal of Communication*, *14*, 4556–4577.

Teleanu, S. (2021). *The geopolitics of digital standards: China's role in standard-setting organisations*. 90.

ten Oever, N. (2018). Productive contestation, civil society, and global governance: Human rights as a boundary object in ICANN. *Policy & Internet*, *11*, 37–60. https://doi.org/10.1002/poi3.172

ten Oever, N. (2022). 5G and the notion of network ideology, or: The limitations of sociotechnical imaginaries. *Telecommunications Policy*, 1–11. https://doi.org/10.1016/j.telpol.2022.102442

ten Oever, N., Milan, S., & Beraldo, D. (2020). Studying discourse in Internet governance through-mailing-list analysis. In L. DeNardis, D. L. Cogburn, N. S. Levinson, & F. Musiani (Eds.), *Researching Internet governance* (pp. 213–229). MIT Press.

Welzl, M., Oepen, S., Jaskula, C., Griwodz, C., & Islam, S. (2021). Collaboration in the IETF: An initial analysis of two decades in email discussions. *ACM SIGCOMM Computer Communication Review*, *51*(3), 29–32. https://doi.org/10.1145/3477482.3477488

Wen, Y. (2020). *The Huawei model*. University of Illinois Press.

Wu, T. (2011). *The master switch: The rise and fall of information empires*. Vintage.

Yates, J., & Murphy, C. N. (2019). *Engineering rules: Global standard setting since 1880*. JHU Press.

Zajacz, R. (2019). *Reluctant power: Networks, corporations, and the struggle for global governance in the early 20th Century*. The MIT Press.

Zajko, M. (2016). Telecom responsibilization: Internet governance, surveillance, and new roles for intermediaries. *Canadian Journal of Communication*, *41*, 75–93.