**Selected Papers of #AoIR2023:**
**The 24th Annual Conference of the**
**Association of Internet Researchers**
Philadelphia, PA, USA / 18-21 Oct 2023

# INFRASTRUCTURAL INSECURITY: GEOPOLITICS IN THE STANDARDIZATION OF TELECOMMUNICATION NETWORKS

Niels ten Oever
University of Amsterdam

Christoph Becker
University of Amsterdam

**Abstract**
This paper argues that the production of 'infrastructural insecurity' is an inherent part of the standardization of information networks. Infrastructural insecurity is the outcome of an intentional process within infrastructural production, standardization, and maintenance that leaves end-users of the infrastructure vulnerable to attacks that benefit a particular actor. We ground this analysis in an interrogation of the responses to the disclosure of three security vulnerabilities in telecommunications networks, namely (1) a security flaw in Signaling System No. 7 (SS7) that allows for the 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. 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, science and technology studies, and critical security studies. This is an important contribution because it asks fundamental questions about the adequacy and legitimacy of standardization processes.

## Introduction

This paper interrogates the responses in standardization to significant security issues with telecommunications networks. We conclude that slow responses by manufacturers

Suggested Citation (APA): ten Oever, N., Becker, C. (2023, October). Infrastructural Insecurity: Geopolitics In The Standardization Of Telecommunication Networks. Paper presented at AoIR2023: The 24th Annual Conference of the Association of Internet Researchers. Philadelphia, PA, USA: AoIR. Retrieved from http://spir.aoir.org.

- and in one case an outright refusal to address the insecurity - reflect geopolitical interests to maintain insecure global communication networks. To explain this we develop the concept of infrastructural insecurity to highlight how standardization of technology is not necessarily optimized to provide security but rather functions in geopolitical interests, also when it is driven by industry. This further problematizes the complex relations between states, industry, and technology in the production, standardization, and maintenance of communication networks (Zajacz 2019). More precisely, it problematizes the process of standardization, which is increasingly looked towards as a trusted process to address societal concerns (ten Oever and Milan 2022). A recent example of this is 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, mostly notably the standardization of the wall thickness of steam boilers to prevent future explosions (Yates and Murphy 2019). However, in 2013 whistle-blower Edwards 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). While at the time this brought up questions about the adequacy and legitimacy of standard-setting, responses to increased encryption in protocols did quiet down some of these debates (Wilton 2017; Doty 2020).

Recently discussions about standardization and security have resurfaced in the light of the NewIP proposals by Chinese actors (Sharp and Kolkman 2020; Hogewoning 2020), allegations about the insecurities resulting from Huawei's 5G implementations (Mascitelli and Chung 2019; Wen 2020; Rühlig and Björk 2020; Tekir 2020; Becker, ten Oever, and Nanni 2022), China's increased participation in standardization (Pohlmann, Blind, and Heß 2020; Baron and Pohlmann 2018; Baron and Kanevskaia Whitaker 2021), as well as Russia's attempts to build a national internet (Ermoshina and Musiani 2017; Stadnik 2019; Asmolov and Kolozaridi 2021; Ermoshina, Loveluck, and Musiani 2022). This paper aims to contribute to these debates by analyzing responses to three insecurities in transnational communication infrastructures.

**Method**

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, science and technology studies, and international relations. This methodological approach has been introduced in our previous work [ANONYMIZED].

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 working group three (from now on abbreviated as WG3 and WG3_LI; 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 ) which is focused on further enhancements to the 5G system in general and lawful interception in particular.

Secondly, we used all documents related to the quarterly held 3GPP TSG WG3 plenary meetings that are focused on security (https://www.3gpp.org/ftp/tsg_sa/WG3_Security ), which contain, inter alia, drafts and final versions of reports, invitations, agendas, minutes. 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 mailing lists of WG3 and WG3_LI contained 71.380 and 7027 emails of which 693 and 419 carried attachments respectively. 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. Since then 525 meeting reports have been uploaded to their server which we used in our study (there are more but we focused on meeting reports).

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 (e.g. meeting reminders and travel advice), and those that focus on legal and technical aspects of surveillance.

**Conclusions**

In all three cases, there has been a considerable amount of time between the publication of the vulnerability and responses by Standards Developing Organization 3GPP. At the same time, exploitation of the vulnerabilities by nation-state actors their law enforcement services has been documented (Parks 2016; Rogers and Eden 2017; Welch 2017; Wolfe 2017). These vulnerabilities were all of an architectural nature, so arguably a standards body that maintains the standards is the best venue to address this issue. However, responses were slow and in the third case, namely that of the proposed implementation of Perfect Forward Secrecy, a solution to the security vulnerability was structurally rejected by companies from the United States, the United Kingdom, and France, leaving a structural insecurity present in new generation telecommunication networks. At the same time, 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. This allows us to conclude that (1) geopolitics are an inherent part of standardization, (2) network insecurities are regularly exploited by governments for surveillance purposes, (3) insecurities in 5th generation telecommunications (5G) networks are maintained - and improvements are blocked - by companies from the United States, the United Kingdom, and France, thus producing infrastructural insecurity.

**References**

Asmolov, Gregory, and Polina Kolozaridi. 2021. “Run Runet Runaway: The Transformation o Fthe Russian Internet as a Cultural-Historical Object.” In *The Palgrave Handbook of Digital Russia Studies*, 277–96. Palgrave Macmillan.

Baron, Justus, and Olia Kanevskaia Whitaker. 2021. “Global Competition for Leadership Positions in Standards Development Organizations.” SSRN Scholarly Paper ID 3818143. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3818143.

Baron, Justus, and Tim Pohlmann. 2018. “Mapping Standards to Patents Using Declarations of Standard-Essential Patents.” *Journal of Economics & Management Strategy* 27 (3): 504–34.

Becker, Christoph, Niels ten Oever, and Riccardo Nanni. 2022. “The Standardisation of Lawful Interception Technologies in the 3GPP: Interrogating 5G and Surveillance Amid Us-China Competition.” In *Interrogating 5g and Surveillance Amid Us-China Competition (July 19, 2022)*. Washington DC, United States. http://dx.doi.org/10.2139/ssrn.4167105.

Benthall, Sebastian, Niels Ten Oever, Nick Doty, and Christopher Becker. 2021. “Bigbang.” https://github.com/datactive/bigbang.

Doty, Nick. 2020. “Enacting Privacy in Internet Standards.” California, United States: University of California, Berkeley. https://npdoty.name/enacting-privacy/.

Ermoshina, Ksenia, Benjamin Loveluck, and Francesca Musiani. 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, Ksenia, and Francesca Musiani. 2017. “Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era.” *Media and Communication* 5 (1): 42–53.

Fontugne, Romain, Ksenia Ermoshina, and Emile Aben. 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.

Hogewoning, Marco. 2020. “Update on WTSA-20 Preparations and New IP.” RIPE Labs. October 11, 2020. https://labs.ripe.net/author/marco_hogewoning/update-on-wtsa-20-preparations-and-new-ip/.

Limonier, Kevin, Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian, and Kave Salamatian. 2021. “Mapping the Routes of the Internet for Geopolitics: The Case of Eastern Ukraine.” *First Monday*, April. https://doi.org/10.5210/fm.v26i5.11700.

Luconi, Valerio, and Alessio Vecchio. 2022. “Impact of the First Months of War on Routing and Latency in Ukraine.” arXiv. https://doi.org/10.48550/arXiv.2208.09202.

Mascitelli, Bruno, and Mona Chung. 2019. “Hue and Cry over Huawei: Cold War Tensions, Security Threats or Anti-Competitive Behaviour?” *Research in Globalization* 1 (December): 100002. https://doi.org/10.1016/j.resglo.2019.100002.

Parks, Lisa. 2016. “Rise of the IMSI Catcher.” *Media Fields Journal* 11.

Pohlmann, Tim, Knut Blind, and Philipp Heß. 2020. “Fact Finding Study on Patents Declared to the 5G Standard.”

Rogers, Michael, and Grace Eden. 2017. “The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures.” *International Journal of Communication* 11 (0): 22.

Rühlig, Tim, and Maja Björk. 2020. “What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe.” *UI Paper, Swedish Institute of International Affairs*.

Sharp, Hascall, and Olaf Kolkman. 2020. “Discussion Paper: An Analysis of the ‘New IP’ Proposal to the ITU-T.” *Internet Society*, April, 13.

Stadnik, Ilona. 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.

Tekİr, Gökhan. 2020. “Huawei, 5G Network and Digital Geopolitics.” *International Journal of Politics and Security* 2 (4 (Çin Özel Sayısı)): 113–35.

ten Oever, Niels, and Stefania Milan. 2022. “The Making of International Communication Standards: Towards a Theory of Power in Standardization.” *Journal of Standardisation* 1 (June). https://doi.org/10.18757/jos.2022.6205.

Veale, Michael, and Frederik Zuiderveen Borgesius. 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.

Welch, Bill. 2017. “Exploiting the Weaknesses of SS7.” *Network Security* 2017 (1): 17–19.

Wen, Yun. 2020. *The Huawei Model: The Rise of China’s Technology Giant*. 1st edition. Urbana: University of Illinois Press.

Wilton, Robin. 2017. “After Snowden – the Evolving Landscape of Privacy and Technology.” *Journal of Information, Communication and Ethics in Society* 15 (3): 328–35. https://doi.org/10.1108/JICES-02-2017-0010.

Wolfe, Henry B. 2017. “The Mobile Phone as Surveillance Device: Progress, Perils, and Protective Measures.” *Computer* 50 (11): 50–58.

Yates, JoAnne, and Craig N. Murphy. 2019. *Engineering Rules: Global Standard Setting since 1880*. JHU Press.

Zajacz, Rita. 2019. *Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century*. Cambridge (US): The MIT Press.