Switzerland by Design: The Co-Shaping of Secure Messaging and National Identity Among Geopolitical Controversies

Samuele Fratini, Francesca Musiani

This article is a pre-print of

Fratini, S., & Musiani, F. (2026). Switzerland by Design: The Co-Shaping of Secure Messaging and National Identity Among Geopolitical Controversies. *Geopolitics*, 1–29 (OnlineFirst). https://doi.org/10.1080/14650045.2026.2672607

Switzerland by Design: The Co-shaping of Secure Messaging and National Identity Among Geopolitical Controversies

Samuele Fratini and Francesca Musiani
Centre Internet et Société, Centre National de la Recherche Scientifique, Paris, France

Abstract

This article investigates how a domestic secure messaging platform, Threema, participates in the co-production of Swiss national identity amid rising digital geopolitics. Arguing that infrastructures are not neutral tools but ideological artefacts, the study combines document analysis (N=30) and semi-structured interviews (N=32) to trace how Threema's technical architecture, institutional, and individual adoption encode and reproduce values of neutrality, privacy, and sovereignty. The article has two main sections: firstly, we use the concept of infrastructural ideology (Maxigas & ten Oever, 2023) to show how seemingly technical choices, like randomised user IDs, metadata minimisation, and Swiss data localisation, perform (geo)political work by materialising and reproducing national identities. Empirically, the article identifies three interrelated mechanisms through which Threema materialises and reshapes Swissness: neutrality by design, privacy by infrastructure, and institutional reception and national branding. These mechanisms operate reciprocally: national identity legitimates Threema's infrastructural choices, while the platform's existence and institutional use update and modernise Swiss identity in digital form. In particular, the analysis outlines three components of Swissness: Swiss exceptionalism, the attitude towards foreign dependencies, and the neoliberal statecraft.

In the second part, the study bridges International Relations and Science and Technology Studies to show how identity functions as a strategic resource and how private infrastructures can enact forms of territorial authority normally associated with states. Practically, it reveals a bottom-up pathway to digital sovereignty in which private firms operationalise jurisdictional claims through design rather than relying solely on regulatory instruments. Ultimately, the Swiss case highlights how small states can leverage culturally resonant infrastructures to pursue strategic autonomy, while also underscoring the ambivalence and fragility of sovereignty enacted through private-sector artefacts. This analysis contributes to debates on techno-nationalism, digital sovereignty, and the political life of infrastructures by showing that code, servers, and protocols are central arenas where identity and geopolitics are produced and contested.

Keywords
Digital sovereignty; national identity; infrastructural geopolitics; secure messaging; international relations.

1. Introduction

In an era characterised by escalating tensions and the weaponisation of infrastructures, the interplay between technology, national identity, and state power has become increasingly pronounced. Digital infrastructures, particularly those facilitating communication and data protection, are not merely neutral tools (De Goede & Westermeier, 2022); they actively participate in shaping national cultures and geopolitical strategies. This article investigates the co-production of technology and state identity through the case study of Threema, a Swiss secure messaging platform. By examining its technical design and patterns of adoption, we explore how Threema both reflects and redefines Swiss identity amidst shifting geopolitical dynamics.

Contemporary debates in Science and Technology Studies (STS) emphasise that technologies are not created in isolation but are co-shaped by societal norms, political ideologies, and cultural traditions. Conversely, technologies themselves influence society, reshaping values, institutions, and imaginaries of statehood. In this reciprocal relationship, infrastructures like Threema emerge as powerful loci of identity formation, governance, and resistance (Fratini & Musiani, 2024). As Maxigas and ten Oever (2023) argue, by mobilising the concept of 'infrastructural ideology,' the built environment of technology embeds political values, encoding them into seemingly technical decisions. These design choices, while appearing pragmatic, reveal deeper ideological

commitments and serve to stabilise or reconfigure conceptions of national belonging and autonomy.

Switzerland provides a compelling context for investigating this dynamic. Historically characterised by neutrality, privacy, and economic discretion, the Swiss nation-state has long constructed its identity through legal, financial, and territorial autonomy (Steinberg, 2015). With the rise of digital infrastructures, these traditional values are being recalibrated in the technological domain. Threema, a secure messaging app developed in Switzerland and widely used by Swiss institutions, exemplifies this transition. Its design eschews conventional identifiers such as phone numbers, relies on domestic data centers, and minimises metadata collection. These are choices that not only signal technical robustness but also resonate deeply with the Swiss national ethos of sovereignty, privacy, and neutrality.

This article posits that Threema is not merely a tool for secure communication but a socio-technical artifact that co-produces Swiss national identity in a global landscape where digital infrastructures are increasingly sites of contestation. By analysing interviews with Threema personnel (N=5), Swiss institutional representatives (N=8), individual adopters (N=19), and official documents produced by Threema and by Swiss institutions (N = 30), we trace how the platform's infrastructural ideology aligns with and reshapes Swiss identity narratives. We contend that Threema contributes to a broader geopolitical performance, wherein states seek technological sovereignty as a means of maintaining strategic autonomy in the face of foreign surveillance regimes, platform capitalism, and regulatory entanglements (Couture & Toupin, 2019; Pohle & Thiel, 2020).

Understanding the co-shaping of technology and society necessitates a close examination of how infrastructural decisions are framed and enacted. For instance, Threema's refusal to require a phone number challenges the methodological nationalism embedded in telecommunication systems, which typically tether users to their national telecom infrastructures. This design feature distances users from state-based identifiers, while simultaneously reinforcing Switzerland's image as a sanctuary of individual privacy.

In the current climate, where digital technologies have become instruments of soft power and arenas of conflict, the construction and projection of national identities are of paramount importance (Glasze et al., 2023). Secure messaging platforms like Threema serve as *dispositifs* - a

sociotechnical relation of governing entities (Amicelle et al., 2015) - through which states can perform sovereignty, signal alliances, and articulate resistance. Switzerland's adoption of Threema by state institutions serves not only practical needs for secure communication but also symbolises the outsourcing of state functions to domestic tech companies that embody national values.

Furthermore, Threema's geopolitical positioning reveals the nuanced tensions that define Switzerland's international posture. On one hand, the platform distances itself from US-centric infrastructures like WhatsApp or Signal, both subject to American jurisdiction and influence (fig. 1). On the other hand, it exhibits ambivalence toward EU proposals such as interoperability mandates, which could compromise its commitment to data minimisation. In this way, Threema becomes an infrastructural expression of Swiss exceptionalism, offering a model of sovereignty that is both technological and symbolic.

	Threema	WhatsApp	Signal	Telegram
Privacy by Design: No phone number or email address required	✓	✗	✗	✗
End-to-end encryption of transmitted messages	✓	✓	✓	✗ [1]
Open source	✓	✗	✓	✓
GDPR compliance	✓	✗	✗ [2]	✗
Corporate solution available	✓	✗ [3]	✗	✗
Transparency report	✓	(✓) [4]	✗ [5]	✗ [6]
Funding	App users	Meta/advertising	Donation / Brian Acton	Pavel Durov / subscriptions / advertising
Jurisdiction	Switzerland	USA [7]	USA [7]	n/a

Fig. 1

Fig. 1: A 'Messenger Comparison' posted on Threema's webpage.[1] Classifications are powerful tools for structuring social relations and technical construction based on key categories (Musiani & Ermoshina, 2017). Threema introduces some key categories (e.g., 'jurisdiction') that diminish the reputation of its competitors and reveal the cultural values that shape the company.

[1] Available at: https://threema.com/en/products/private/messenger-comparison.

The implications of such infrastructural nationalism extend beyond the Swiss case. As digital infrastructures increasingly mediate the exercise of power, identity, and governance, their design and control become strategic matters of statecraft. The co-production of technology and national identity is thus not only an analytical lens but also a practical challenge for states navigating a fragmented and competitive geopolitical order. Whether through control over data flows, legal jurisdiction, or infrastructural design, nations embed their identities into the very architecture of the digital world.

This article makes a twofold contribution to the burgeoning literature on digital sovereignty and geopolitics. First, we advance a sociotechnical conceptualisation of digital sovereignty that moves beyond the predominantly discursive frameworks found in recent scholarship (e.g., Couture & Toupin, 2019; Santaniello, 2025). While existing work has mapped the attributes of digital sovereignty as a political discourse, we argue that technical artifacts are not merely outcomes or of sovereign ambitions but are fundamental in *assembling* digital sovereignty as a hybrid, material-political project. By tracing the co-production of Swiss identity through Threema's architecture, we demonstrate how sovereignty is performed.

Second, we contribute to International Relations (IR) and Geopolitics by nuancing the role of identity in state strategy. We propose that in the digital age, national identity functions as a changing and scarce strategic resource. States do not simply have an identity; it is the complex product of multiple factors, such as infrastructural choices. It can then be invested in the international arena to facilitate coalition-building, project soft power, and broadcast national values (such as neutrality) to a global audience. This theoretical proposition travels beyond the Swiss case: it offers a lens to understand how any state might use national tech stacks to materialise a distinct geopolitical brand that serves as an asset in international value projection.

2. Theoretical Framework

The interplay between technology, infrastructure, and national identity has increasingly drawn scholarly attention, particularly within an STS framework and, more precisely, Infrastructure Studies. These fields emphasise how technological systems are not merely neutral tools but are embedded within and constitutive of social, political, and cultural imaginaries. This analytical lens proves especially valuable in understanding how nations construct and perform their identities

through technology. A rich body of literature has explored this nexus, revealing how national and regional identities are co-produced alongside scientific and technological infrastructures.

Switzerland is an exemplary case for observing these dynamics, with a rich history that goes way back to pre-digital technologies and pre-Internet ages, since its national identity has for a long time been closely tied to notions of neutrality, internationalism, and technical competence. Bruno Strasser's (2022) work provides a compelling account of how Swiss neutrality was co-constructed with its scientific endeavors, long before they were applied to what eventually became the new, digital-based, information and communication technologies. During the Cold War, Switzerland leveraged its geopolitical position and scientific infrastructure to position itself as a neutral mediator within the international community. Strasser argues that neutrality in science was not merely a reflection of Swiss state policy but a performative act that reinforced the country's political stance. Through involvement in international scientific cooperation, Swiss actors constructed a vision of science that was detached from ideological conflicts, mirroring the broader national commitment to political neutrality.

This co-production of national identity and scientific neutrality in Switzerland resonates with broader discussions in STS about the performativity of technological systems. Sheila Jasanoff's notion of co-production underscores how scientific knowledge and social order are mutually constitutive (Jasanoff, 2004; see also Hecht, 1998). In the Swiss case, scientific infrastructure (ranging from research institutes to international collaborations) acted as both a symbol and a tool of the national ideology of neutrality.

The same co-productionist logic has been applied to the Bavarian context by Pfotenhauer et al. (2023) to show how technical affordances and national narratives are brought into a stable, reinforcing configuration. As demonstrated in their analysis of how technologies materialise regional identities, innovation projects are not merely technical or economic endeavors, but rather perform and reproduce social identities. Space and automotive technological applications provide the necessary technical evidence to modernise and sustain an imagined social order. While technologies are structurally influenced by their social context, they in turn contribute to defining key elements of the social order, such as citizenships, identities, and cultures (Tsui et al., 2025).

In more recent years, this framing has extended to digital technologies as examined by the authors' previous work (Fratini & Musiani, 2024), addressing how data localisation policies in Switzerland serve as both a security measure and a narrative tool in the context of digital sovereignty. These policies are not merely technical solutions but are deeply embedded in socio-political discourses

that shape and reflect national identity. By analysing the debates and implementations surrounding data localisation, we highlight the contested nature of digital sovereignty and how Switzerland's approach reflects its historical emphasis on neutrality and self-determination, showing how infrastructural decisions are intertwined with national identity and security narratives in the digital age (Fratini, 2025b).

Indeed, the relationship between infrastructure and national identity becomes even more pronounced in contemporary geopolitical contexts, such as the global rollout of 5G networks. Maxigas and Niels ten Oever (2023) argue in this regard that technological infrastructures like 5G are embedded with geopolitical imaginaries. They assert that decisions about infrastructure are not merely technical but are laden with ideological commitments and national priorities. For instance, debates about Huawei's involvement in 5G infrastructure have sparked concerns about national security, sovereignty, and digital independence. These debates reflect broader anxieties about how technological dependencies can compromise national identity and autonomy.

According to Santaniello (2025), digital sovereignty from a constructivist perspective can be regarded as a collection of speech acts used to legitimise state control over digital infrastructures. From this perspective, domestic technologies are often presented as materialisations of national values and drivers of national autonomy. While we welcome the understanding of sovereignty as an unstable construction with (geo)political purposes, the present study moves beyond its exclusively discursive nature. Reducing a constructivist approach to the sole 'linguistic turn' risks overlooking the material dimensions of the legitimation efforts undertaken by nation-states to extend their control over digital technologies. State sovereignty in the digital domain is advanced through a wide variety of discursive, material, and cultural practices, which often recuperate imaginaries of *longue durée* (Stambhøl et al., 2025). For this reason, it must be analysed through a hybrid approach aimed at understanding how these components are held together and harnessed to maximise state power.

The concept of infrastructural ideology introduced by Maxigas and ten Oever represents an important conceptual lens to highlight how national identities and ideologies materialise into technological constructions. Furthermore, it aligns closely with Strasser's observations about Switzerland. In both cases, technology functions as a medium through which national identity is articulated and contested. However, while Strasser focuses on the historical co-production of neutrality through scientific cooperation, Maxigas and ten Oever highlight how contemporary technological infrastructures become sites of geopolitical struggle and ideological expression.

These dynamics are not confined to individual nation-states but also play out at the regional level, particularly within the European Union. The discourse on European digital sovereignty exemplifies how technological infrastructure becomes central to regional identity formation and security politics (Fritsch et al., 2019; Levenda et al., 2019). In this regard, Monsees and Lambach's (2022) work is particularly eloquent, as they argue that digital sovereignty is more than a regulatory objective, but rather a geopolitical imaginary that seeks to define what Europe is and aspires to be. The pursuit of digital sovereignty involves articulating a distinct European identity that is autonomous from both American and Chinese technological hegemonies.

Similarly, Bellanova et al. (2022) explore how digital sovereignty is intertwined with European security integration. They contend that digital sovereignty is both a means and an end in the project of European integration. It serves as a rallying point for collective action while simultaneously reflecting contested visions of what European unity should entail. Infrastructure, in this context, becomes a material and symbolic site where European identity is negotiated and performed.

Drawing these strands together, this study argues for the existence of a continuum from national to regional scales and on to global dynamics, in which infrastructure and technology are central to the articulation of political identities. Switzerland's historical example, as analysed by Strasser, provides a microcosm of how national identity can be stabilised through technological neutrality. The literature on European digital sovereignty shows how regional identities can also be constructed through infrastructural choices, particularly when these are framed as responses to external dependencies and internal aspirations; debates on digital sovereignty show how these identities can then be 'mobilised' strategically in a digital geopolitics context. And finally, the contemporary struggles over 5G infrastructure, as discussed by Maxigas and ten Oever, demonstrate how similar dynamics play out in the face of emerging technologies, in this instance with overt geopolitical stakes and reconfigurations in power balances at the global level.

STS and infrastructure studies offer a robust framework for analysing how technological systems are imbricated in the construction of national and regional identities. Whether in Cold War Switzerland or contemporary Europe, infrastructure is never merely technical; it is deeply political and profoundly symbolic. The co-production of identity and infrastructure is an ongoing process, shaped by historical contingencies, geopolitical pressures, and normative commitments. This study's conceptual apparatus is valuable precisely because it bridges two complementary perspectives on technology and politics: the STS sensibility, which treats technologies as intrinsically political actors, and the infrastructural turn in Internet governance, which examines how institutions strategically co-opt technical systems to secure power and autonomy (Fratini,

2025a; Musiani, 2025). By bringing these lenses together, we can trace how culturally contingent tools like Threema are both shaped by, and in turn reshape, national identities and geopolitical positions. This dual focus reveals the feedback loops through which both domestic norms and situated cultural practices inform technological design and how it is subsequently harnessed.

As the digital age progresses, understanding this co-production becomes ever more crucial for scholars and policymakers alike. In the following section of the article, we elaborate on the scholarly and policy reasons for which this analysis is desirable and relevant, and why it is important to examine in detail lesser-known national contexts where the nexus between digital technology, security, identity construction, and geopolitics is at play.

3. Methodology

Empirical material for this study was gathered through a dual strategy of document analysis (N = 30) and semi-structured interviews (N = 32), both pursued via snowball sampling (Dosek, 2021). Initial contacts were identified through the authors' existing networks; each interviewee then recommended additional participants, allowing us to capture a range of perspectives from developers, corporate managers, and institutional users. The empirical core of this study consists of 32 semi-structured interviews conducted between October 2023 and September 2024. The participants were divided into three primary groups to capture the reciprocal nature of co-production:

1. Group A: Institutional users (N=8). We reached some of the key Swiss institutions that integrated Threema, such as federal officials from Berne, cantonal authorities, and representatives from critical infrastructure sectors (Swiss Army and Police).
2. Group B: Threema's personnel (N=5). After negotiating access to the company, we managed to have conversations covering diverse corporate functions such as marketing, technical capacities, legal, and managing positions.
3. Group C: Individual users (N=19). To avoid the risk of conceptual over-assertiveness based solely on institutional branding, we integrated 19 interviews with individual Threema users. These interviews focused on personal motivations for using Threema and its relationship to their sense of Swiss identity.

While snowball sampling has been clearly effective in building up a robust empirical basis, it came with limitations concerning the sample representativeness. In particular, the corpus is clearly centered on German and Italian-speaking Switzerland. This limits the sample's possibility to account for the diverse cultural attitudes and approaches to data protection and digital sovereignty existing between French and German-speaking Switzerland (Daniore et al., 2025).

In parallel, we collected policy papers, technical specifications, and corporate communications to triangulate our findings and ensure a rich archival base. These sources are accessible in the Annex. All interviews were conducted between October 2023 and September 2024 and were audio-recorded with consent; transcripts were anonymised to protect confidentiality.

We adopted a grounded-theory approach to analysis (Charmaz, 2012), iteratively coding interview transcripts and documents to allow key categories and thematic patterns to emerge inductively rather than imposing a priori frames. Because this research is anchored in a single, in-depth case study, our goal is not statistical generalisability but rather a nuanced, empirically grounded understanding of how Threema's infrastructure co-produces Swiss identity. Detailed information on sampling chains, document inventories, interview protocols, and codebooks is provided in the Annex to facilitate transparency and replication.

4. Swiss National Identity and Threema

STS-inspired analyses have also been blooming concerning digital technologies and security (Fischer & Wenger, 2021). Nevertheless, the field still presents relevant limitations, such as the overfocus on a few prominent case studies. Entities such as China, the European Union, Russia, and the United States have quasi-monopolised the attention of those scholars dealing with the (geo)political use of digital technologies (Fratini et al., 2024). While these subjects deserve scholarly attention, a restricted focus on a few cases has detrimental effects, as it limits the scientific understanding of complex social phenomena.

For this reason, we put forward an analysis of a less explored case study within the European continent: Switzerland. As a tiny alpine state outside of the EU and NATO, Switzerland has comparatively attracted little attention from the international academic community. Yet, we argue that the Swiss context is a particularly fruitful case study, which can bring enhanced value to the

scientific understanding of the relationship between digital technology and state identity. The reason is that Switzerland is characterised both by the challenges that affect other major players and by peculiar identity features. Furthermore, studies suggest that the growingly bipolar competition between China and the US in the digital context may enhance the agency of third-party countries in the international arena, if compared to the previous US unipolar moment (Lehdonvirta et al., 2025).

Firstly, the country displays a pronounced degree of infrastructural dependence on US and Chinese operators. The case of the Swiss Public Cloud is particularly instructive. In 2020, a tender called 'Public Clouds Confederation' was released to equip Federal institutions with cloud services. Furthermore, the tender demanded that '[t]he bidder must have data centers on at least 3 continents' (Benhamou et al., 2023). It thus prioritised foreign hyperscalers over Swiss providers, which were automatically excluded by this requirement. The 5-year project was contracted to Alibaba, Amazon, IBM, Microsoft, and Oracle, which are now in charge of expanding the governmental cloud infrastructure for the 2025-2032 period[2]. This aligns Switzerland and the EU in terms of digital policy agenda-setting, but also in terms of technological vulnerabilities and dependencies. Furthermore, even though the last example may suggest that Swiss authorities have no digital strategy, digital sovereignty is a first-relevance topic in Swiss digital and foreign policy; indeed, it was selected as a guiding principle of the Digital Switzerland Strategy[3].

On the other hand, the cloud story is representative of the Swiss traditional reluctance to state interventionism in industrial policy and trade. Laissez-faire has characterised the Swiss economic model during its genesis in the 19th and 20th centuries and perpetuates it until today (Argast, 2009). While the infrastructural dependencies and vulnerabilities make Switzerland similar to the EU, its anti-regulatory tendency aligns the country with the US neoliberal approach of the last 30 years. Switzerland emerges as a political actor striving to achieve digital autonomy, but is severely limited by foreign dependencies and an institutional system that refuses regulatory activism from the state.

---

[2] Information available at https://www.bit.admin.ch/en/sgc-en.

[3] See https://digital.swiss/en/action-plan/measures/operational-work-streams-on-digital-sovereignty#:~:text=Switzerland%20examines%20which%20political%2C%20legal,of%20international%20openness%20and%20networking.

However, the country is also characterised by peculiar features that historically shaped its identity and approach to technological governance. In particular, these fields have been affected by the concepts of neutrality and privacy. Neutrality is internationally recognised as a long-standing Swiss characteristic, while it is domestically branded as the principle on which national identity and policy-making are centered. In reality, it is both a modern historical construction (Jost, 2009) and the relational product of various international power balances, rather than an unwavering Swiss virtue. Switzerland managed to keep its neutrality in the international arena through a flexible and minimalist understanding of the concept and by profiting from the interest of great powers in keeping the country out of conflicts. This makes it difficult to understand whether Switzerland fought for its neutrality or whether it has been neutralized from the outside (Jorio, 2023).

All this considered, the concept of neutrality did have important effects on the Swiss approach to technological governance. In many ways, it contributed to the reputational construction of the country as a 'haven' and a 'bridge-builder'. Among others, the country played a key role in bringing together the two main telegraphic networks existing until 1865 (the Austro-German Union and the West European Union) into a unique Telegraph Union – today the International Telecommunication Union (Balbi et al., 2014), a United Nations specialised agency. The ability of Switzerland to benefit the international community through its neutral position has been traditionally self-defined as 'good offices' (Fischer, 2002), a term that is still recurrently used by public institutions.

Another key concept in the formation of the Swiss identity is that of privacy. For centuries, the idea of privacy as a national value has shaped institutions and policies such as the well-known banking secret (Guex, 1999). But just like neutrality, privacy as a value has always been negotiated with the outside. While the most famous case is the weakening of banking secrecy due to pressures from the United States, especially during the Obama administration (Munzinger et al., 2022), there are plenty of examples.

At the end of the 19th century, many Italian anarchists found protection in Switzerland. Yet, the increasing Italian pressures pushed Switzerland to change its policy and set up a strict surveillance regime aimed at identifying and expelling anarchist refugees back to Italy (Binaghi, 2002). This appears to be a recurring dynamic. Proton, a company offering privacy-oriented digital services, is an eloquent example of this. Even though it usually markets its cloud and email services by branding the Swiss jurisdiction as privacy-friendly, the company was forced in 2021 to provide the

IP addresses of some French climate activists to the French authorities after the intervention of Europol (Bateman, 2021). On that occasion, Proton's CEO and public statements made clear that under Swiss law the company could be legally compelled to collect and provide metadata, including IP addresses, as part of a criminal investigation if ordered by competent Swiss authorities. Proton emphasised that its end-to-end encryption protects email contents, but that metadata like IP logs can be obtained when a court order is issued; Proton updated its privacy policy after the incident to clarify when and how it may have to log and share data under Swiss law (Bateman, 2021).

However flexible, the concepts of neutrality and privacy have shaped Swiss technological governance and digital companies like Proton. Among the service providers placing great emphasis on the privacy principle, Threema is particularly interesting (Fratini, 2024). It is a Swiss messaging application founded in 2012 and adopted by 12 million individual users and more than 8000 corporate and institutional users. The company is predominantly adopted in the German-speaking area of Europe and managed to gain an important market position by becoming the official communication channel of several public institutions and big corporations. Threema is currently adopted by the Swiss army, some Swiss Cantons and municipalities, some German cities, and Länder. Although its adoption is comparatively limited, Threema is the largest European messaging application and is in open competition with other secure messaging platforms, with regard to Signal and Telegram. Especially to compete with the former, Threema constantly boasts its *Swissness*. According to corporate advertising, the company's Swiss identity unfolds through the principles of 'precision, reliability, and discretion'. Concepts of neutrality and privacy work as discursive support to legitimise Threema from a jurisdictional, technical, and ethical perspective (Fratini & Musiani, 2024).

For this reason, it is legitimate to assume that the Swiss identity shapes and is shaped by Threema's technical construction. In the following analysis, we mobilise the concept of infrastructural ideology to point out how the Swiss identity emerges from Threema's design. We then move forward according to the STS principle of co-shaping to understand how Threema affects the Swiss national identity in turn (fig. 2). Finally, we draw on these results to discuss the relevance of national identities concerning geopolitical competition and technological innovation.

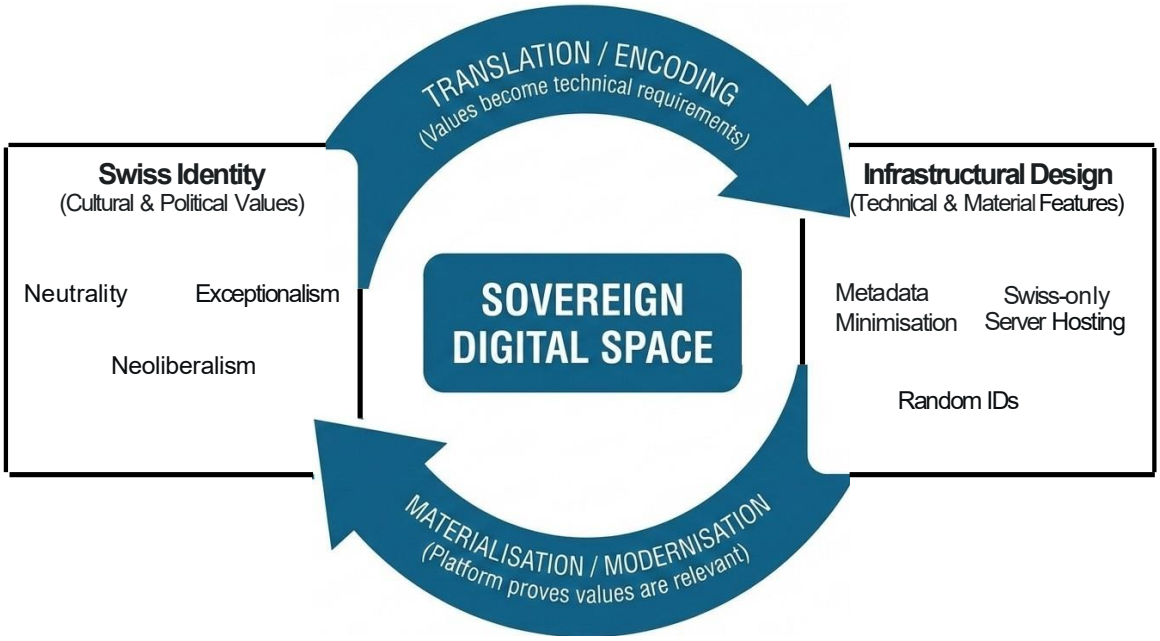


Fig. 2: The co-production of Swiss identity and Threema's infrastructure.

5. How the Swiss Cultural Context Shapes Threema

Building on Maxigas and ten Oever's (2023) analytical strategy, which dissects some key innovations through competing infrastructural ideologies, this section adopts a similar method to investigate Threema's socio-technical composition. Rather than viewing messaging platforms as discrete tools, we understand Threema as part of a situated ideological system where technical design choices are laden with political values and national imaginaries. We understand ideology from a Gramscian perspective, meaning as a '*Weltanschauung*', a dominant worldview that, together with coercion, maintains a specific hegemonic order (Gramsci, 1971). Infrastructural ideology emphasises how paradigmatic visions of communication infrastructure reflect distinct social orders and governance models. Applying this to Threema allows us to trace how its material and architectural configurations materialise Swiss national identity and then reshuffle it in turn.

Threema's infrastructure reveals a deliberate opposition to dominant global paradigms of digital communication. In contrast to the data capitalism epitomised by Meta – owner of WhatsApp

(Santos & Faure, 2018), or the cryptographic cosmopolitanism underlying Signal, Threema crafts a third way rooted in principles of jurisdictional reliance and a culturally-shaped approach to data minimisation. These values materialise through specific choices: refusing to tether user identity to phone numbers, localising data storage within Swiss borders, and minimising metadata retention. Together, these design decisions function as ideological statements. They articulate a model of digital infrastructure that elevates privacy, neutrality, and sovereignty, not as abstract values, but as operational standards embedded into code, protocol, and infrastructure (Fratini, 2024).

Neutrality by Design

Swiss neutrality, historically associated with diplomatic mediation and non-alignment in international conflicts, finds a technological analog in Threema's refusal to bind user identity to national systems of surveillance and control. Rather than requiring SIM-based registration—a norm in both GSM and mobile app ecosystems—Threema assigns each user a random ID, fully decoupled from telecommunication infrastructures and personal identifiers. This architectural choice subverts the methodological nationalism typically embedded in mobile communication standards (Maxigas & Ten Oever, 2023) and affirms a vision of user autonomy aligned with Swiss geopolitical non-alignment. In infrastructural terms, this is a form of embedded neutrality: the system abstains from global digital power blocs not only through discourse but by design.

Furthermore, Threema's refusal to bind user data to national systems of surveillance was also the object of a legal conflict that took place between the company and the Swiss Post and Telecommunications Surveillance Service. The latter decided to reclassify Threema as a telecommunications provider. This classification would have placed Threema under the Swiss BÜPF law (*Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs*), which mandates retention of metadata, real-time surveillance capabilities, and compliance with requests from law enforcement.

Threema opposed this reclassification, arguing that it is not a telecom provider, but an over-the-top (OTT) service like Signal or WhatsApp. The company also pointed out that its infrastructure is not designed to retain metadata or provide real-time access, and reclassification would force major architectural changes and compromise user privacy. After negotiations and a formal legal appeal, Threema won the case in 2023. The Swiss Federal Administrative Court (*Bundesverwaltungsgericht*) ruled that Threema should not be treated as a telecommunications

provider, as it does not provide access to the public telecommunications network but operates over the Internet.

Finally, this non-binding identity infrastructure reflects a deeper commitment to sovereignty as autonomy, not integration. While dominant platforms like WhatsApp and Telegram tie users to state-regulated telecom systems or rely on third-party cloud infrastructures (Santos & Faure, 2018), Threema's architecture is insulated from such dependencies. In doing so, it mirrors Switzerland's Cold War-era diplomacy, where neutrality was maintained not through isolation but through selective engagement and institutional distance (Balbi et al., 2014; Strasser, 2009).

Privacy by Infrastructure

Swiss privacy traditions are particularly robust, shaped by a legacy of banking secrecy, confidential asylum processes, and cautious public bureaucracy. Threema encodes these traditions at the infrastructural level. The minimisation of metadata collection further deepens this ideological entanglement. In contrast to infrastructures that rely heavily on metadata for business intelligence (Srnicek, 2017), algorithmic optimisation (Mager, 2012), or state surveillance (Abrahamsen & Williams, 2009), Threema collects minimal usage data. In particular, it does not collect or store key user metadata, including message timestamps, contact lists, or delivery logs, as learned from the analysed documents and the interviews with its personnel.

This resonates with the Swiss debate over the right to digital integrity[4]. In particular, it proposes to treat citizens not as data-owners, but rather as people who operate in the digital world. This implies their right to total control of the data they produce through their online activities, as part of their personhood. The right was first introduced through popular vote in the Geneva (2023) and Neuchâtel (2024) Cantons. While it started as a French-speaking debate, it spread to German-speaking Cantons, with popular initiatives in Basel and Zurich.

Furthermore, all communications in Threema are end-to-end encrypted, and user-generated data are stored only ephemerally on servers located exclusively within Swiss borders or within end-user devices. Data localisation in Threema is more than a compliance mechanism—it is a geopolitical choice. By hosting servers solely within Swiss jurisdiction, Threema shields its operations from the

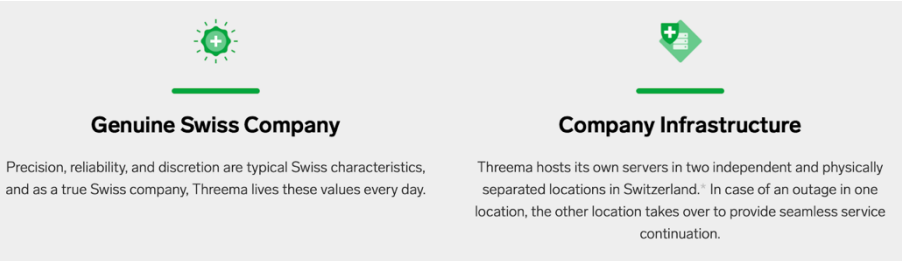
[4] More details available here: https://www.swissinfo.ch/eng/digital-democracy/how-swiss-federalism-is-helping-the-rise-of-a-new-digital-right/89023201.

extraterritorial reach of laws such as the USA CLOUD Act (fig. 1). To Swiss users and institutions, this is presented as the fact that communications are protected not only by cryptography but also by legal context. Importantly, this demonstrates how technical infrastructure and national regulatory environments can reinforce each other both discursively and materially.

Institutional Reception and National Branding

Threema's uptake by Swiss institutions—including the federal army, cantonal governments, and various public services—has reinforced its identity as a national platform, even in the absence of formal state sponsorship. This alignment between public sector adoption and infrastructural ideology reflects a broader logic of national branding.

The company's marketing campaigns emphasise Swissness not only as geographic origin but as operational ethos: 'precision, reliability, and discretion' (fig. 2). These values resonate with both institutional buyers and the public, who see in Threema a digital reflection of Switzerland's identity. In doing so, Threema contributes to a symbolic economy in which technical decisions are interpreted through the lens of national ideology.



Fig, 3: Threema's promotional material posted on the company's website.

Threema exemplifies how national identity can be both expressed through and stabilised by digital infrastructure. By aligning technical features with cultural and regulatory values, Switzerland has produced a communication platform that serves both private and public ends while performing sovereignty through design.

6. How Threema Reshuffles the Swiss National Identity

While the previous section examined how Swiss cultural norms and institutional pressures shaped Threema's architectural and operational modalities, this section turns to the reciprocal process:

how Threema, as an infrastructural artifact, actively reconfigures and revitalises Swiss national identity. Drawing on the concept of co-shaping, we emphasise three intertwined dynamics: the digital reenactment of Swiss exceptionalism; Threema's role in bolstering institutional autonomy and digital sovereignty; and the reinforcement of Switzerland's neoliberal statecraft through strategic public–private partnerships.

Swiss Exceptionalism

Switzerland's self-conception as a neutral and sovereign polity has historically rested upon distinctive institutional arrangements, from its Alpine confederation to its financial secrecy regime. In the context of secure messaging, Threema modernises and 'updates' this exceptionalism by embedding neutrality and discretion into code and infrastructure. Its randomised user-identification scheme, which eschews phone numbers, reinvents the telegraphic vision of Swiss neutrality articulated in the nineteenth century: rather than linking users to national telecommunication monopolies, Threema detaches identity from territorial signifiers, echoing the analysis of Switzerland's Cold War-era scientific neutrality as a performative act grounded in infrastructural design (Strasser, 2022). By digitally anonymising participants, Threema projects a contemporary variant of the Swiss 'good offices' principle, offering a communications sanctuary free from extraterritorial surveillance or corporate data harvesting (Balbi et al., 2014).

Moreover, Threema's metadata minimisation functions as a technological extension of the country's double haven ethos, which was historically applied to banking and asylum, and recasts it for the digital era. Where Swiss banking secrecy once safeguarded capital flows, Threema's refusal to retain contact lists or message logs foregrounds informational discretion as a core national value. This recalibration is not a mere marketing trope but an infrastructural statement: by aligning data practices with the Swiss reputation for precision and reliability, Threema amplifies a national narrative of exceptionalism that transcends financial havens to encompass personal communications.

Through these design choices, Threema does more than reflect Swiss identity: it reinvigorates and updates it. The platform enacts a new chapter of exceptionalism, one defined by cryptographic rigor and localised control rather than Alpine neutrality and financial discretion alone. In doing so, it reaffirms a national mythos of restraint, independence, and technical excellence adapted to twenty-first-century challenges.

Infrastructural Foreign Dependencies

A second vector through which Threema reshuffles Swiss identity concerns its impact on institutional dependencies. The country's Digital Switzerland Strategy[5] underscores digital sovereignty as a guiding principle, yet state actors have historically relied upon foreign hyperscalers to provide public cloud services and other strategic digital resources. Threema offers a countervailing model: by hosting data exclusively on domestic servers, operating under Swiss jurisdiction, and offering a culturally contingent product, it diminishes the leverage of external providers while reinforcing the legal and technical sovereignty of government bodies.

Swiss federal agencies, cantonal administrations, and the military have increasingly adopted Threema to harden their communications against both state-centric and corporate surveillance regimes. This uptake signifies more than a shift in procurement policy; it represents an infrastructural turn in which digital sovereignty is enacted through a private-but-domestic actor rather than top-down regulation. Sovereignty in the digital realm is co-constructed through practice as much as through legislation (Tretter, 2023). Threema's architecture materially actualises jurisdictional control, enabling institutions to bypass US-based endpoints and EU interoperability mandates (Pohle & Thiel, 2020). In effect, the platform becomes a site-bound expression of Swiss territoriality, rendering the nation's borders concrete in servers and encryption protocols.

By reducing institutional foreign dependencies, Threema redefines the contours of Swiss autonomy. It transforms digital sovereignty from an abstract policy goal into an operational capability, one instantiated through routine communications. Consequently, Swiss identity, long anchored in legal and diplomatic autonomy, is reenacted daily in the exchange of encrypted messages, reinforcing a collective self-perception of resilience against external pressures.

Neoliberal Statecraft

Finally, Threema's trajectory illuminates how Swiss neoliberal statecraft leverages private innovation to fulfill public mandates. Switzerland's laissez-faire economic tradition has eschewed heavy-handed industrial policy in favor of market-driven solutions (Argast, 2009). By outsourcing critical communication functions to Threema, the Swiss state enacts a variant of economic statecraft where private firms assume functions traditionally reserved for public agencies.

This dynamic aligns with the STS notion of co-production: corporate and state actors mutually inform and reinforce each other's roles. Threema's positioning as the secure channel for federal orders, cantonal bulletins, and military directives embodies a public–private hybrid governance

[5] Available at: https://digital.swiss/userdata/uploads/strategie-dch-en.pdf.

model. It externalises expertise (cryptographic engineering, server management, metadata policy) to a private entity, while simultaneously delegating symbolic authority to that actor. The result is a neoliberal assemblage whereby market logics and national interests converge: Threema monetises discretion and sovereignty as premium attributes, even as it operates within a competitive platform economy alongside Signal and Telegram.

Such arrangements fuel again Switzerland's characteristic aversion to state intervention, while ensuring that core state functions align with domestic techno-cultural norms. By entrusting a private company with the confidentiality and continuity of official discourse, Swiss institutions reproduce their commitment to minimal regulation and maximal market participation. This reaffirms a self-image of pragmatic stewardship, in which the state orchestrates rather than owns, presides yet refrains from direct production.

Nevertheless, this institutional orientation towards private providers should not be indiscriminately extended to other social groups. Our interviewed individual users often disclosed they have been convinced by the company's data minimisation approach. This also emerged in another study conducted by the authors (Fratini & Musiani, 2024) and resonates with the 2021 rejection of the private-led e-ID. The contrast between the initial e-ID failure and Threema's success is instructive. While Swiss citizens resisted delegating a state-guaranteed identity to the private sector in the e-ID vote, many argued[6] that the second e-ID proposal was accepted in 2025 also because of the introduction of the data minimisation and optionality principle. Future studies should address this aspect, but this suggests that Swiss digital sovereignty is performed through a specific trusted domesticity, where the private sector is welcomed as a provider of tools, but not as the custodian of the legal personhood.

7. Discussion

This study of Threema's design and adoption among Swiss institutions sheds new light on the broader debate over the geopolitical salience of national identities in the digital age. By analysing how infrastructural choices encode, and are in turn shaped by, Swiss norms of neutrality, privacy, and sovereignty, we uphold the long-standing STS thesis that digital technologies are neither politically neutral nor purely technical artifacts. They serve as *loci* where national self-conceptions are actively performed and contested. More precisely, on this basis, the analysis unites the STS view of technology as inherently political with the infrastructural Internet Governance's focus on

[6] See, for example: https://www.swissinfo.ch/eng/swiss-politics/five-lessons-from-swiss-voters-acceptance-of-e-id/90082224.

institutional co-optation, revealing how tools like Threema both reflect cultural norms and actively reshape national sovereignty and global standing. By doing so, it highlights the reciprocal dynamics through which digital infrastructures become instruments of identity and power. In what follows, we situate our findings within three intersecting conversations: the constructivist turn in IR that elevates identity as one of the drivers of state behavior; debates over digital sovereignty and techno-nationalism; and critical infrastructure and STS perspectives on sociotechnical co-production.

National Identity as a Strategic Resource in IR

Traditional realist scholars have long argued that material power and security imperatives govern state actions, relegating identity to a secondary role or even dismissing it as epiphenomenal. According to traditional realist scholarship (Waltz, 2010), the state's behavior is characterised by the self-help principle and power rivalry because it is ultimately determined by the world system's anarchic structure. Our Swiss case complicates this picture. Threema's infrastructural ideology shows that states not only mobilise identity narratives to legitimate domestic governance and foreign policy but that national identities shape the development of strategic technologies.

These technologies then play a key role in steering and pursuing geopolitical strategies. By localising data storage and minimising metadata, Threema not only signals technical robustness but also invokes Switzerland's historical reputation as a double safe haven for banking and asylum-seekers. In doing so, the platform functions as a distributed extension of Swiss sovereignty, much as military alliances or trade agreements do in a realist framework. It allows Swiss institutions to reduce foreign dependencies by excluding external service providers like WhatsApp and Signal in favor of a domestic and localised solution. This case clearly demonstrates the relationship between the maximisation of sovereign power resources through technology and existing imaginaries of *longue durée* (Stambøl et al., 2025). With regard to Signal, it should be explicitly noted that its technical validity and security are not being called into question by Threema (a point that is also reflected in the table that compares it with other secure messaging applications on Threema's website). Rather, the emphasis is placed on the notion of Swissness, which is also highlighted in our interviews. In particular, the Swiss police stress the importance of the location of the data centers. According to the interviews, the contractual arrangement with Threema reportedly includes a clause allowing the authorities to terminate the agreement should the service begin using servers located outside Switzerland.

At the same time, the present study corroborates constructivist claims that state interests are malleable, situated, and socially constructed (Wendt, 1992). The co-production dynamic, whereby Threema implements cultural values in code, and users' expectations of Swiss discretion reinforce those values in corporate strategy, mirrors the 'structure–agency' feedback loops central to constructivist approaches like structuration theories and symbolic interactionism (Wendt, 1994). Building on this perspective, our findings underscore that digital infrastructures are among the most consequential arenas in which national identities are created, circulated, and contested. This expands constructivist analyses in IR through a renewed focus on infrastructures as crucial junctions where identities and strategies are articulated.

The integration of constructivist IR and STS infrastructural ideology lens offers a powerful heuristic for geopolitics and, more broadly, for the social sciences, because it simultaneously foregrounds the discursive power of identity narratives and the material agency of technology. By treating digital infrastructures not merely as backdrops to state action, but as co-producers of norms, practices, and even sovereign authority, our framework bridges IR's concern with how states mobilise ideas of sovereignty and power with STS's insight that technical design choices encode and deploy political values.

This dual perspective reveals, for instance, how a messaging app like Threema can serve as both a symbolic speech act of Swiss exceptionalism and a tangible mechanism of jurisdictional control, thereby demonstrating that geopolitical strategies are enacted as much through code and servers as through treaties and alliances. In doing so, it encourages scholars to look beyond traditional policy instruments and military capabilities, to consider how infrastructures themselves become sites of contestation, identity-building, and strategic autonomy in an era defined by digital interdependence.

Digital Sovereignty and Techno-Nationalism

Scholars of digital geopolitics have increasingly focused on how states pursue 'data localisation,' sovereign cloud policies, and national 5G networks to assert control over data flows and technological standards (Couture & Toupin, 2019; De Goede & Westermeier, 2022). Threema exemplifies a bottom-up approach to digital sovereignty: rather than waiting for state regulation, a private firm integrated jurisdictional and cultural claims into its product design, thereby offering Switzerland an immediate mechanism for asserting autonomy vis-à-vis US hyperscalers and EU interoperability mandates (Fratini, 2025b).

This corporate form of Swissness aligns with what Maxigas and ten Oever (2023) describe as 'infrastructural ideology,' where technical choices articulate a particular vision of the world. Threema's refusal to require phone numbers, its domestic data centers, and strict metadata minimisation all amount to infrastructural materialisations of territorial integrity and individual discretion. By doing so, Threema not only secures communications but also projects Swiss exceptionalism in the global marketplace of messaging apps. In this way, our study contributes empirical weight to debates on techno-nationalism by showing how non-state actors can become emissaries of national identity and policy objectives through design.

Co-Production and STS: Technology as Politics

STS scholars emphasise that technologies embody political values and power relations. Our analysis of Threema's socio-technical configuration illustrates this co-production: Swiss cultural commitments to neutrality and privacy are inscribed into protocols and server architectures, which then reinforce those same values in public perceptions of both the firm and the state. For instance, the ideological framing of 'precision, reliability, and discretion' in Threema's marketing does more than attract users; it re-educates them about what Swiss statehood means in a digital context, effectively updating 'neutrality' for the 21st century. While the Swiss national identity has decisively contributed to the shaping of Threema, its technical and social construction reshuffles and reproduces Swissness in the current digital context.

Moreover, Threema shows how infrastructures can become sites of governance that redistribute authority among corporations, the state, and individual users. By outsourcing secure communications to a Swiss-based company, federal institutions perform a form of 'public-private partnership' in the service of national identity. This reflects a broader trend in Swiss economic statecraft, where the government often relies on private actors to attain policy goals (Feld, 2007). As our study reveals, such arrangements are not merely pragmatic; they are deeply symbolic, fusing technology and identity in mutual reinforcement.

Implications for Geopolitical Competition

The Swiss case holds broader lessons for understanding competition between great powers in the digital age. Just as China leverages the Chinese dream (Creemers, 2020) to frame its rise and Russia

invokes the 'Russian World'[7] to justify regional interventions (Litvinenko, 2021), smaller states can deploy technological sovereignty to maximise their degree of national autonomy in the geopolitical arena (Lehdonvirta et al., 2025). Threema's success suggests that national identity remains a scarce resource in a competitive environment of platform capitalism and surveillance capitalism. States and their national champions will increasingly vie to embed cultural narratives and jurisdictional claims into digital architectures, turning apps and cloud services into instruments of soft power.

At the same time, the study cautions that infrastructural nationalism is inherently ambivalent. Threema's positioning between US and EU regimes, embracing market openness while resisting regulatory interoperability, mirrors Switzerland's historical balancing act. Such strategic ambiguity can protect autonomy in the short term but may create vulnerabilities if global standards shift or if domestic dependencies (e.g., on foreign cloud providers) intensify. Thus, while national identity can bolster sovereignty, it also demands continuous negotiation with external forces and internal stakeholders.

8. Conclusion

The case of Threema offers a rich illustration of how digital technologies are not merely shaped by pre-existing sociopolitical contexts but actively participate in reshaping national identities and state strategies. Far from being a mere communication tool among others in a field – secure messaging – where proliferation and fragmentation have prevailed in the post-Snowden era, Threema embodies and performs a uniquely Swiss infrastructural ideology, which is deeply rooted in values of privacy, neutrality, discretion, and sovereignty. Through deliberate design choices such as metadata minimisation, local data hosting, and the avoidance of phone number identifiers, Threema reflects and reinforces Switzerland's historical self-image as a haven of informational autonomy and institutional discretion.

At the same time, it actively reshapes them by providing the material infrastructure for a new active digital neutrality. It is not merely a reflection of past neutrality but an agent that enables the Swiss state to perform an autonomous geopolitical role, such as the Swiss Army's strategic pivot away from US-based platforms. By materialising privacy as a technical default, Threema shifts Swissness

[7] We use "Russian World" as an English translation for "русский мир" (rùsskiy mir) - a concept which loosely indicates the ensemble of human communities that are historically tied to Russia. Within Russian propaganda, this idea of a Russian world is used to justify Russian expansionism in the neighboring states (Mankoff, 2022: 25).

from a passive historical legacy to an active, exportable technical standard that reinforces the state's strategic autonomy.

This co-production of technology and national identity has several implications for both scholarly and policy communities. First, it affirms the theoretical insights from STS that technologies are embedded in cultural, political, and ideological worlds. As infrastructures become more central to the daily operations of governance, commerce, and interpersonal communication, their design becomes an arena where identity, authority, and power are negotiated. Threema illustrates how even small nations can leverage infrastructural design as a means of articulating geopolitical autonomy and cultural specificity in a highly interconnected world.

Second, our findings nuance traditional understandings of digital sovereignty. Whereas much of the literature has focused on top-down efforts by powerful states to control digital infrastructures through regulation or protectionism, the Swiss case highlights a bottom-up and market-driven pathway. Here, a private firm, guided by both national norms and competitive pressures, materialises sovereignty through infrastructure. The firm's success in aligning its platform with the symbolic and functional elements of Swiss national identity demonstrates the potential of public-private partnerships not just in terms of policy implementation, but also in the very production of political meaning.

Third, the analysis invites a reconsideration of identity as a strategic resource in the international arena. While realists have tended to downplay the role of identity, and constructivists have often bracketed the material underpinnings of identity formation, this study contributes to bridging those gaps. Threema's infrastructure enables and embodies a specific articulation of Swissness, one that resists both the surveillance-driven architectures of US platforms and the regulatory activism from the European Union. In doing so, it becomes a microcosm of Switzerland's broader geopolitical posture: autonomous but interconnected, assertive yet non-aligned.

Moreover, the case of Threema underscores the relevance of small states in digital geopolitics. Often overshadowed by the infrastructural ambitions of larger powers like China, the EU, or the US, Switzerland reveals how smaller actors can carve out distinctive and resilient niches by aligning technological design with national values. In this context, Threema does not merely serve a domestic user base; it also functions as an emissary of Swiss ideology, a digital artifact through which sovereignty, identity, and strategy coalesce.

At the same time, the study cautions against romanticising infrastructural nationalism. While Threema succeeds in offering an alternative model of secure, privacy-preserving communication, its growth and legitimacy remain entangled with global dependencies, such as cloud infrastructure controlled by foreign hyperscalers or cross-border legal pressures. The tensions between self-determination and integration, discretion and transparency, national autonomy and global interdependence are not easily resolved but must be continuously managed. This dynamic reflects the broader challenge of technological sovereignty in the 21st century: the pursuit of autonomy does not occur in a vacuum but within an evolving mesh of legal, economic, and infrastructural constraints.

Finally, the case contributes to a broader understanding of how digital infrastructures act as *dispositifs*—assemblages that simultaneously enable governance and articulate identity. As communication technologies increasingly underpin state functions, their design becomes a strategic terrain not just for functional optimisation but for ideological expression and geopolitical signaling. The study of Threema suggests that secure messaging platforms, often perceived as minor or marginal, can play outsized roles in projecting national narratives and mediating international alignments.

In sum, Switzerland's embrace of Threema is more than a story of technological preference; it is a case of infrastructural identity-making. It reveals how digital artifacts can stabilise, reproduce, and even recalibrate long-standing cultural values under contemporary conditions of technological and geopolitical flux. As global digital infrastructures continue to fragment and reconfigure, the article suggests that sovereignty today is not only a matter of borders and laws but of protocols, servers, and metadata. Identity, likewise, is no longer simply narrated by institutions or constitutions; it is encoded in code, embedded in infrastructures, and performed through platforms.

9. References

Abrahamsen, R., & Williams, M. C. (2009). Security Beyond the State: Global Security Assemblages in International Politics. *International Political Sociology*, *3*(1), 1–17. https://doi.org/10.1111/j.1749-5687.2008.00060.x

Amicelle, A., Aradau, C., & Jeandesboz, J. (2015). Questioning security devices: Performativity, resistance, politics. *Security Dialogue*, *46*(4), 293–306. https://doi.org/10.1177/0967010615586964

Argast, R. (2009). An unholy alliance: Swiss citizenship between local legal tradition, federal laissez-faire, and ethno-national rejection of foreigners 1848–1933. *European Review of History: Revue Européenne d'histoire*, *16*(4), 503–521. https://doi.org/10.1080/13507480903063787

Balbi, G., Fari, S., & Richeri, G. (2014). *Network neutrality: Switzerland's role in the genesis of the Telegraph Union, 1855 - 1875*. Lang.

Bateman, T. (2021). ProtonMail criticised for passing arrested French climate activist's IP address to police. Euronews, September 7, https://www.euronews.com/next/2021/09/07/protonmail-criticised-for-passing-arrested-french-climate-activist-s-ip-address-to-police

Benhamou, Y., Bernard, F., & Durand, C. (2023). Digital Sovereignty in Switzerland: The laboratory of federalism. *Risiko & Recht*, *1*.

Binaghi, M. (2002). *Addio, Lugano bella: Gli esuli politici nella Svizzera italiana di fine Ottocento (1866-1895)*. Armando Dadò Editore.

Charmaz, K. (2012). *Constructing grounded theory: A practical guide through qualitative analysis* (Repr). Sage.

Christakis, T. (2023). European Digital Sovereignty, Data Protection, and the Push toward Data Localization. In *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press.

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Crabu, S., & Magaudda, P. (2018). Bottom-up Infrastructures: Aligning Politics and Technology in building a Wireless Community Network. *Computer Supported Cooperative Work (CSCW)*, *27*(2), 149–176. https://doi.org/10.1007/s10606-017-9301-1

Creemers, R. (2020). China's Conception of Cyber Sovereignty: Rhetoric and Realization. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3532421

Daniore, P., Sedlakova, J., Zavattaro, F., Huber, Z., Knieps, M., Haulotte, M., Agbessi Alangue, T., Faulk, A., von Wyl, V., Benhamou, Y., Gille, F. (2025) Public views on research with publicly available data in Switzerland: Implications for digital research, science communication, and policy. Public Underst Sci. 2025 Nov;34(8):988-1008. doi: 10.1177/09636625251330575.

De Goede, M., & Westermeier, C. (2022). Infrastructural Geopolitics. *International Studies Quarterly*, *66*(3). https://doi.org/10.1093/isq/sqac033

Dosek, T. (2021) Snowball Sampling and Facebook: How Social Media Can Help Access Hard-to-Reach Populations, Political Science & Politics, 54(4), pp. 651-655

Feld, L. P. (2007). *Regulatory competition and federalism in Switzerland: Diffusion by horizontal and vertical interaction* (No. 2006-22). CREMA Working Paper.

Fischer, S., & Wenger, A. (2021). Artificial Intelligence, Forward-Looking Governance and the Future of Security. *Swiss Political Science Review*, *27*(1), 170–179. https://doi.org/10.1111/spsr.12439

Fischer, T. (2002). *Switzerland's good offices: A changing concept, 1945-2002* [Application/pdf,Online-Datei]. https://doi.org/10.3929/ETHZ-A-004445304

Fratini, S. (2024). Performing Privacy Culture. The Platform Threema and the Contestation of Surveillance Made in Switzerland. *Studi culturali*, *1*, 3–26. https://doi.org/10.1405/113065.

Fratini, S. (2025a). Governing (socio) materialities at the intersection of STS and Internet governance: hybridization as a product of necessity. *Tecnoscienza–Italian Journal of Science & Technology Studies*, *16*(1), 109-123. https://doi.org/10.6092/issn.2038-3460/20583.

Fratini, S. (2025b). The Sociotechnical Politics of Digital Sovereignty: Frictional Infrastructures and the Alignment of Privacy and Geopolitics. *Big Data & Society, 12(4),* https://doi.org/10.1177/20539517251400729.

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society*, *3*(3), 59. https://doi.org/10.1007/s44206-024-00146-7

Fratini, S., & Musiani, F. (2024). Data localization as contested and narrated security in the age of digital sovereignty: The case of Switzerland. *Information, Communication & Society*, 1–19. https://doi.org/10.1080/1369118X.2024.2362302

Fritsch, M., Obschonka, M., & Wyrwich, M. (2019). Historical roots of entrepreneurship-facilitating culture and innovation activity: an analysis for German regions. *Regional Studies*, *53*(9), 1296–1307. https://doi.org/10.1080/00343404.2019.1580357.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Goldsmith, J. L., & Wu, T. (2008). *Who controls the Internet? Illusions of a borderless world.* Oxford University Press.

Gramsci, A. (1971). *Selections from the prison notebooks of Antonio Gramsci* (Repr.). Lawrence & Wishart.

Guex, S. (1999). Les origines du secret bancaire suisse et son rôle dans la politique de la Confédération au sortir de la Seconde Guerre mondiale. *Genèses. Sciences Sociales et Histoire*, *34*, 4–27.

Hecht, G. (1998). *The Radiance of France. Nuclear Power and National Identity after World War II.* Cambridge, MA: The MIT Press.

Hellegren, I. (2017). A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom. *Internet Histories*, *1*(3), 1-27. 10.1080/24701475.2017.1387466

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 205395172098201. https://doi.org/10.1177/2053951720982012

Jasanoff, S. (Ed., 2004). *States of Knowledge: the Co-production of Science and Social Order*. London: Routledge.

Jorio, M. (2023). *Die Schweiz und ihre Neutralität: Eine 400-jährige Geschichte*. hier+jetzt.

Jost, H. U. (2009). Origines, interprétations et usages de la « neutralité helvétique »: *Matériaux Pour l'histoire de Notre Temps*, *N° 93*(1), 5–12. https://doi.org/10.3917/mate.093.0002

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025) Weaponised interdependence in a bipolar world: How economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy*, 1-26, https://doi.org/10.1080/09692290.2025.2489077.

Levenda, A.M., Richter, J., Miller, T., Fisher, E. (2019) Regional sociotechnical imaginaries and the governance of energy innovations, Futures, 109, 181-191, https://doi.org/10.1016/j.futures.2018.03.001.

Litvinenko, A. (2021). Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. *Media and Communication*, *9*(4), 5–15. https://doi.org/10.17645/mac.v9i4.4292

Mager, A. (2012). Algorithmic Ideology: How capitalist society shapes search engines. *Information, Communication & Society*, *15*(5), 769–787. https://doi.org/10.1080/1369118X.2012.676056

Mankoff, J. (2022) *Empires of Eurasia: How Imperial Legacies Shape International Security*. Yale University Press: New Haven, CT.

Maxigas, & Ten Oever, N. (2023). Geopolitics in the infrastructural ideology of 5G. *Global Media and China*, *8*(3), 271–288. https://doi.org/10.1177/20594364231193950

Mazzoni, P., Martini, M., Ferrigato, R., Lüthi, E., & Balbi, G. (2024). *Communications, media and internet concentration in Switzerland, 2019-2021* (p. 45). Global Media & Internet Concentration Project.

Möllers, N. (2021). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, *46*(1), 112–138. https://doi.org/10.1177/0162243920904436

Munzinger, H., Obermaier, F., & Obermayer, B. (2022). *Schweizer Geheimnisse: Wie Banker das Geld von Steuerhinterziehern, Foltergenerälen, Diktatoren und der katholischen Kirche versteckt haben - mit Hilfe der Politik* (1. Auflage). Kiepenheuer & Witsch.

Musiani, F. & Ermoshina, K. (2017) "What is a *Good* Secure Messaging Tool? The EFF Secure Messaging Scorecard and the Shaping of Digital (Usable) Security", *Westminster Papers in Communication and Culture*. 12(3). doi: https://doi.org/10.16997/wpcc.265

Musiani, F. (2025). Reassessing "Infrastructuring Digital Sovereignty": Digital Self-determination as a Set of Infrastructure-embedded Practices. *Frontiers in Communication*, 10. https://doi.org/10.3389/fcomm.2025.1562072.

Pfotenhauer, S.M., Wentland, A., Ruge, L. (2023) Understanding regional innovation cultures: Narratives, directionality, and conservative innovation in Bavaria, Research Policy, 52(3), https://doi.org/10.1016/j.respol.2022.104704.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Santaniello, M. (2025) Attributes of Digital Sovereignty: A Conceptual Framework. *Geopolitics*, 1-22.

Santos, M., & Faure, A. (2018). Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. *Social Media + Society*, *4*(3), 205630511879587. https://doi.org/10.1177/2056305118795876

Srnicek, N. (2017). *Platform capitalism*. Polity.

Stambøl, E. M., Sylla, A., & Cold-Ravnkilde, S. M. (2025). Anticolonial Imaginaries in Mali: The *Longue Durée* of Sovereignty, Security, and Geopolitics. *Geopolitics*, 1–26. https://doi.org/10.1080/14650045.2025.2523411.

Steinberg, J. (2015). *Why Switzerland?* (3rd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139051101.

Tsui, S., Pfotenhauer, S., & Bombaerts, G. (2025). Constructing the "Cocreative Citizen": Innovation Subjects, Statehood and the Common Good in Hybrid Public–Private Settings. *Science, Technology, & Human Values*, *0*(0). https://doi.org/10.1177/01622439251394488.

Tretter, M. (2023). Sovereignty in the Digital and Contact Tracing Apps, *Digital Society*, *2*(1). 10.1007/s44206-022-00030-2

Waltz, K. N. (2010). *Theory of international politics* (Reiss). Waveland Press.

Wendt, A. (1992). Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization*, *40*(2), 391–425.

Wendt, A. (1994). Collective identity formation and the international state. *The American Political Science Review*, *88*(2), 384–396.

10. Annex

Tables

Document	Date	Publisher	Language
Blog Post	26.11.2020	Threema	English
Blog Post	04.2021	Threema Work	English
Blog Post	01.2021	Threema	English
Whitepaper	02.11.2021	Threema	English
Blog Post	05.12.2022	Threema	English
Interview	09.07.2022	Frankfurter Allgemeine Zeitung	German
Newspaper Article	11.01.2023	Neue Zürcher Zeitung	English
Blog Post	09.01.2023	Threema	English
Online Article	12.01.2023	Security Week	English
Blog Post	27.07.2020	Threema Work	English
Blog Post	Not Available	Threema Work	English
Privacy Policy	12.01.2022	Threema	English
Terms of Service	08.03.2018	Threema Work	English
Terms and Conditions	23.03.2022	Threema	English
Online Article	10.10.2016	IT Inside.ch	German
Online Article	12.01.2021	Corriere del Ticino	Italian
Online Article	17.02.2022	Tages Anzeiger	German
Federal Document	01.02.2022	Centro Nazionale per la Cibersicurezza	Italian
Blog Post	19.12.2023	Threema	English
Interview	18.03.2021	SRF News	German
Online Article	17.01.2021	Watson	German
Online Article	10.03.2022	Bild	German
Online Article	01.02.2021	Handelsblatt	German
Online Article	20.08.2021	Basic Thinking	German
Online Article	04.09.2020	ZDNet	English
Blog Post	14.01.2023	Danilo Bargen	English
Blog Post	19.01.2023	Schneier on Security	English
Online Article	06.02.2023	Das Netz ist Politisch	German
Web Post	09.09.2020	Afinum	German

11. Table 1.

ID	Institution	Duration	Date
Interviewee 1	Bern City	20 min.	13/03/2024
Interviewee 2	St. Gallen Canton	20 min.	13/03/2024

Interviewee 3	Zurich Canton	20 min.	13/03/2024
Interviewee 4	Polizeitechnik- und Informatik Schweiz	40 min.	25/03/2024
Interviewee 5	Ticino Police	40 min.	10/04/2024
Interviewee 6	Swiss Made Software	80 min.	30/04/2024
Interviewee 7	Swiss CxO Forum	30 min.	10/05/2024
Interviewee 8	Federal Office of Communication	40 min.	10/09/2024

Table 2.

ID	Branch	Duration	Date
Employee 1	Technical	40 min.	15/04/2024
Employee 2	Marketing	50 min.	30/04/2024
Employee 3	Technical	40 min.	06/05/2024
Employee 4	Managing	60 min.	09/08/2024
Employee 5	Legal	40 min.	03/09/2024

Table 3.

ID	Country	Duration	Date
User 1	Austria	60 min.	04/10/2023
User 2	Austria	30 min.	12/10/2023
User 3	Germany	25 min.	13/10/2023
User 4	USA	25 min.	18/10/2023
User 5	Sweden	70 min.	15/10/2023
User 6	Germany	30 min.	18/10/2023
User 7	France	30 min.	25/10/2023
User 8	Switzerland	15 min.	25/10/2023
User 9	Germany	15 min.	27/10/2023
User 10	Germany	30 min.	04/11/2023
User 11	Germany	25 min.	07/11/2023
User 12	Germany	30 min.	08/11/2023
User 13	Germany	20 min.	20/11/2023
User 15	Switzerland	25 min.	21/11/2023
User 16	Germany	30 min.	23/11/2023
User 17	Germany	30 min.	24/11/2023
User 18	UK	60 min.	30/11/2023
User 19	Germany	30 min.	11/12/2023

Table 4.