International Journal of Communication 15(2021), 2669–2692 1932–8036/20210005

Gateways, Sieves, and Domes: On the Infrastructural Topology of the Chinese Stack

GABRIELE DE SETA[1]
University of Bergen, Norway

This article proposes a topological model capable of accounting for the scale and complexity of China's digital infrastructure. Beginning with the troubled development of a submarine data cable between Los Angeles and Hong Kong, it identifies the limitations of topographical analyses of ICTs and then reviews theorizations of "the stack" as a topological model of planetary computation. To situate the stack model in the Chinese context, I draw on 3 case studies—QR codes, filtering, and cybersovereignty—exemplifying three topological configurations: the gateway, the sieve, and the dome. These configurations expand the conceptual vocabulary of the stack model at different scales, and provide useful tools for the analysis of computational infrastructures in Asia and beyond.

Keywords: China, computation, infrastructure, platforms, sovereignty, stack, topology

Unraveling a 12,971-km Cable

In 2016, Google and Facebook announced a partnership with the Pacific Light Data Communication Co., Ltd. (PLDC), a broadband communications service provider based in Hong Kong. The partnership revolved around a 12,971-km-long submarine cable crossing the Pacific Ocean from Hermosa Beach, a town near Los Angeles, California, to Deep Water Bay, on the south of Hong Kong Island. Once completed, the Pacific Light Cable Network (PLCN) cable would afford a data transmission rate of 144 terabytes per second, connecting the United States to Hong Kong with one of the lowest latencies worldwide (Hecht, 2018). From the PLDC side, this partnership was framed as an important step in Pacific Rim networking, "the initial step in PLCN's construction of a global network" (Moss, 2016, para. 5) that would offer Google and Facebook users in the Asia-Pacific region less latency, more bandwidth and better security.

This kind of infrastructural development is not surprising: In a bid to expand the capabilities of submarine cables connecting their data centers, tech giants like Facebook, Google, Microsoft, and Amazon

Gabriele de Seta: gabriele.seta@uib.no
Date submitted: 2019–11–21

[1] This research was funded by the Machine Vision in Everyday Life project, which has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (Grant Agreement No. 771800).

have joined a worldwide cable spree. As the geography of the global submarine cable network shifts toward Asia's emerging economies (Malecki & Wei, 2009), Hong Kong has emerged as central hub for networking infrastructure in the Asia-Pacific region, becoming a top destination for U.S. cables and a primary gateway to China and its Internet market. Unfortunately, in early February 2020, two years after the PLCN cable's predicted completion date, Google and Facebook announced their partial withdrawal from the partnership, settling for a reduced submarine network that stopped at landings in the Philippines and Taiwan.

This decision was motivated by concerns over the ownership of PLDC (set to control four of the cable's six fiber optic pairs), which had recently passed hands from Hong Kong tycoon Wei Junkang to Dr. Peng Telecom & Media Group, a Beijing-based broadband provider. After evaluating PLDC's new owner, U.S. officials concluded that—while not state-owned or state-controlled—Dr. Peng was involved in sensitive Chinese government projects, including surveillance networks, and hence presented a national security risk. The PLCN cable was physically in place and ready to transport data across half the globe (see Figure 1), but a U.S. national security panel led by the Justice Department has held back final approval to put it into use (FitzGerald & O'Keeffe, 2020). In April 2020, Google has obtained permission to use the cable up to its Taiwan landing, while the Hong Kong branch remains inactive (Chang, 2020).

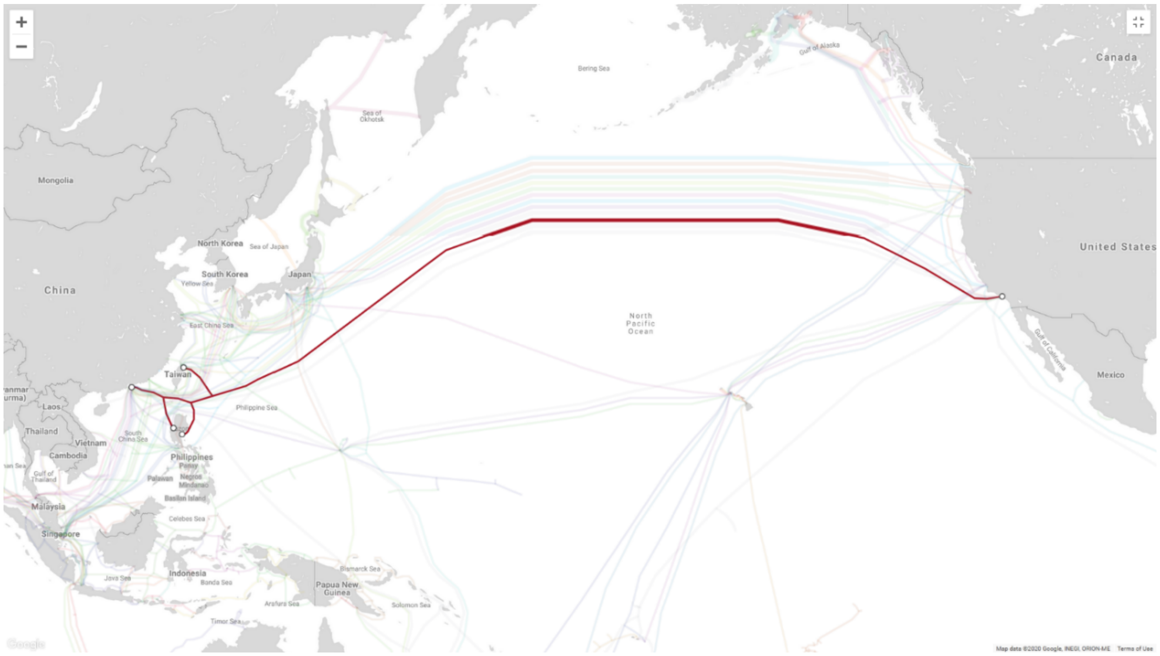

Figure 1. The PLCN cable. Screenshot from TeleGeography's Submarine Cable Map, April 2020.

The geopolitical interests of the actors involved in this partnership extend beyond the undersea cable itself. Since 2009, Facebook has been inaccessible from inside China, and yet the country remains its fifth market for revenue size thanks to a Shenzhen-based advertising partner (Mozur & Lin, 2019); similarly, Google has left the country in 2010 after refusing to submit to the regulatory requests of Chinese authorities, and yet it maintains an active foothold in China (Julienna Law, 2020). On the other side of the Hong Kong S.A.R. border, the Dr. Peng Telecom & Media Group has established 200,000 square meters of data centers in Beijing, Shanghai, Shenzhen, Guangzhou, Wuhan, and Chengdu, positioning itself as one of the major data center providers in China, with a clientele including major Chinese services such as Alibaba Cloud, Tencent Cloud, Huawei Cloud, and Baidu Cloud (Dr. Peng Group, 2019).

Pulling this proverbial "loose thread" unravels a complex and layered weave of companies and regulatory bodies invested in the operation of the PLCN cable. The fraught partnership between American platform companies and a Chinese infrastructural provider, all interested in expanding their capacity to move data across the Pacific, clashes with U.S. national security concerns around Chinese telecom providers amidst an ongoing trade war centered around networking infrastructure, and results in unforeseen shifts in flows of data, computing power, and market access. The case of the PLCN cable is only one among countless examples of how the development of communication infrastructure is shaped by geopolitical interests and policy decisions, challenging both global and national imaginations of the Internet. What does the unraveling of an undersea data cable reveal about the layering of communication technologies and sovereign actors? This article conceptualizes a model capable of accounting for the complexities of planetary-scale digital infrastructure, and does so by proposing a shift from topographical analyses of communication networks to a topological inquiry into the geopolitics of computation.

In the first half of the article, I review three decades of topographic metaphors through which analysts, policy-makers and government officials have narrated the development of the Internet in China, evidencing how these topographic imaginations have substantially obfuscated the interrelations and layering of information and communication technologies. To propose a more accurate representation of the development of Chinese ICT infrastructures, I draw on the concept of "stack" and its articulation across disciplines and contexts, identifying its contributions and shortcomings as a geopolitical model of transnational communication. Theorizing communication infrastructure through a stack model allows the tracing of how different actors operate across multiple sociotechnical layers and at a topological scale that challenges existing paradigms of sovereignty. The goal of this article is to situate China—with its techno-nationalist policies, expanding tech industry, and burgeoning platform companies—within discussions of the stack as emergent planetary-scale computation.

In the second half of this article, after questioning the simplistic idea of a "red stack" neatly superimposed with China's national borders, I outline three topological configurations that characterize China's entanglement with planetary computation: gateways, sieves, and domes. My move from topographical imaginations to topological configurations is inspired by the resurgence of topology in social and cultural theory (Lury, Parisi, & Terranova, 2012), where it is increasingly adopted to map sociotechnical assemblages characterized by dynamic shifts in scale, density, and layering. After illustrating gateways, sieves, and domes by way of three case studies drawn from the Chinese stack, I conclude that these three topological configurations provide a more accurate understanding of China's role in planetary computation and, conversely, of planetary computation's impact on existing political structures and territorial sovereignty.

Topographies of China's Digital Infrastructure

The development of digital infrastructure in China has been narrated through different, and at times incommensurable, topographical imaginaries. In post-Mao China, "information" was one of the main keywords driving Deng Xiaoping's reform and opening up (X. Liu, 2019, p. 3). Deng's push for "informatization" (*xinxihua*), admittedly inspired by Alvin Toffler's vision of a civilizational "Third Wave" (G. Chen, 1988), signaled a will to move beyond industrialization and to usher a postindustrial "information society" (Austin, 2014, p. xv). Informatization has remained a central keyword of China's development policy, and the series of Golden Projects initiated in the late 1980s aimed at developing a communication network infrastructure capable of supporting national economy, governance, and security (Dai, 2002, p. 145). Through the integration promised by projects like the Golden Bridge, the Golden Customs, or the Golden Shield, China could catch up with the rest of the developed world on the "information superhighway," much touted by leaders during the 1990s (p. 146).

The information fantasies underpinning policy visions of global connectivity and postindustrial economy did not last long: as soon as Internet access started becoming available to increasing numbers of Chinese citizens, authorities began to impose regulations and oversight on the data flowing in and out of the country. While Deng Xiaoping had promoted the benefits of informatization, he had also famously warned that, when opening a window, a screen was needed to keep the flies out (Hartford, 2000, p. 259). The earliest attempts at monitoring the exchange of sensitive information and controlling expressions of dissent were famously envisioned as the building of a "Great Firewall"—a metaphor that combined the symbolic barrier of the Great Wall of China with the technical term for a network security system (Barme & Sang, 1997). Over the years, the Great Firewall has grown into an increasingly unwieldy assemblage of keyword filters, address blacklists, content regulations, and surveillance tools that has prompted unsatisfied users to engage in a cat-and-mouse-game with the authorities (Endeshaw, 2004). Portrayals of the Chinese Internet as a giant cage, a walled garden or an authoritarian panopticon (see Figure 2) have prompted critical evaluations of the potential of networked communication as a public sphere or democratizing force (Tsui, 2007).

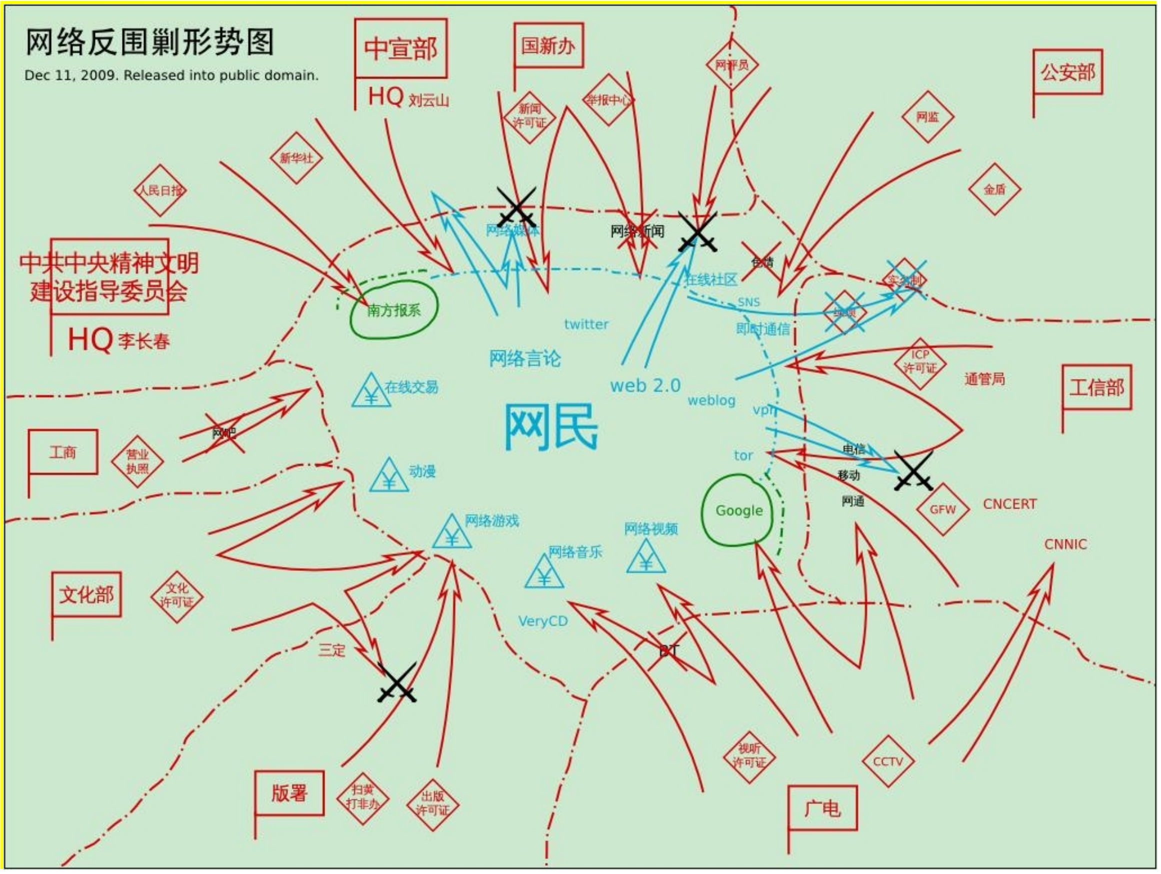

Figure 2. Topography of authoritarian enclosure: An Internet anti-encirclement situation map pitching **wangmin** *("netizens," users) and their platforms (Twitter, blogs, video games, etc.) besieged by the forces of the propaganda department, state television, and Public Security Bureau, among others.*

As pointed out by communication scholar Yu Hong (2016), a focus on the enclosure metaphor comes with the risk of missing "the intertwining between the territorial and capitalist logic of power" (p. 103) that drives the geopolitics of ICTs in China. The importance of communication technologies for national sovereignty has not been lost on the Chinese leadership of the post-Mao era: Since the early 2000s, as informatization moved from futuristic fantasies to pragmatic efforts in policymaking and infrastructure building, catching up with the world's burgeoning digital economy and staking a claim to standard-setting and regulatory frameworks has become a geopolitical priority (Hartford, 2000, p. 255). Behind the architectures of information control put in place by the state there is a techno-nationalist model that has steered China's "digital leap forward" toward securing a strategic position in the global market while also reinforcing the state's territorial sovereignty (Zhao, 2007).

China's massive post-2008 investments in ICT development have helped Chinese companies compete with global market leaders, further entrenching the country's reliance on export-oriented manufacturing and its centrality in transnational supply chains (Schiller, 2008, p. 112). Driven by a consistent distrust of the country's dependence on American technologies, government officials and policy makers have promoted concepts like *wangluo zhuquan* (cyber sovereignty), *zizhu chuangxin* (indigenous innovation), and *wangluo qiangguo* (strong Internet nation), which all index a concerted push for the "Chinese *national, as opposed to foreign*, control over information network infrastructure" (Zhao, 2010, p. 267, italics in original). In Yuezhi Zhao's (2010) analysis, this techno-nationalist agenda is intrinsically contradictory, as it pitches national control of core technologies as the solution to the dependence from an increasingly interconnected market (p. 269).

By the mid-2010s, following global industry trends and arguably sheltered by techno-nationalist policies keeping their foreign competitors at bay, a few Chinese Internet companies—hailed by the government as "national champions"—have grown into massive platforms. Baidu, Alibaba, and Tencent, identified as an emergent BAT trio, challenge Google, Facebook, and Amazon's oligopoly on the provision of computational services (ranging from search engines and social networking to e-commerce and the gig economy) in both the domestic and regional market (Jia & Winseck, 2018). Concurrently with this "platformization" of the Chinese Internet (de Kloet, Poell, Guohua, & Yiu Fai, 2019), there has been a parallel process of "infrastructuralization" (Plantin, Lagoze, Edwards, & Sandvig, 2018), through which Chinese digital platforms have started providing services in domains like transportation, logistics, and finance (J. Y. Chen & Qiu, 2019; Plantin & de Seta, 2019; L. Zhang, 2020). This slippage between platforms and infrastructures has further complicated China's techno-nationalist agenda: On the one hand, the provision of both cloud-based computation and networking equipment requires global competitiveness and integration in transnational supply chains; on the other, China's increasingly strict regulations on data flows and critical information infrastructure anchor these companies' operations to national law and sovereign territory (Webster, Sacks, & Triolo, 2019).

In the span of three decades, the Internet in China has been described in terms of ubiquitous information requiring global linkages, as a walled garden to regulate, as a techno-nationalist project of geopolitical importance, and as an expansive cloud hovering above society. From highways to walls and from national borders to transnational flows, China's ICTs have been mapped through wildly different and at times conflicting topographies, which continue to be pervasive in both academic analyses and media reporting. As the distinctions between platforms and infrastructures, technology transfers and supply chains, data flows and capital flows become increasingly porous, deforming the established topographies of information and stretching the definitions of global, national, regional, and local, a different approach is needed to conceptualize the scale and complexity of China's digital infrastructure. Topology, I argue, offers a way forward.

Toward a Topology of the Chinese Stack

As of 2020, it is apparent that national informatization has moved beyond aspirational network building, and that the "Chinese Internet" is no longer just a Web-centric enclosure or merely a thriving ecosystem of platforms and startups. The topographies outlined in the previous section—while all faithful representations of specific aspects of ICTs in China—are no longer sufficient to conceptualize layered issues such as the geopolitical wrinkles around a submarine cable. Rather than proposing one more topography of the Chinese Internet, I argue for the necessity of developing a topological model capable of encompassing multiple topographies (the information superhighway, the walled garden, the cybersovereign platform economy) while also allowing for other emergent configurations of infrastructural assemblages to be recognized and identified. Actor-network theorists have extensively repurposed the mathematical science of topology to model the different spaces and rules according to which sociotechnical configurations are deformed or stabilized (John Law & Mol, 2001). Topology, being both a representational device and a method of analysis, emerges from "the practices of ordering, modelling, networking and mapping that co-constitute culture, technology and science" (Lury et al., 2012, p. 5), and is hence central to articulating models of complex infrastructural assemblages.

One of such topological models is that of the stack. Media theorist Benjamin Bratton (2015) has formulated the concept of "the Stack" (capitalized to distinguish it from specifically technical or everyday uses of the term) to describe how computation has coalesced into a "planetary-scale infrastructure that is changing not only how governments govern, but also what governance is in the first place" (p. xvii). In Bratton's (2015) theorization, various kinds of computation "form an accidental megastructure called The Stack that is not only a kind of planetary-scale computing system; it is also a new architecture for how we divide up the world into sovereign spaces" (p. xix). This Stack is "a machine that serves as a scheme as much as it is a schema of machines" (p. 5). Like the topological thinking proposed by Celia Lury, Luciana Parisi, and Tiziana Terranova (2012), it is as much a concept as it is a method (p. 19), both a *topos* (space) and a *nomos* (law). For Bratton (2015), the Stack represents a challenge to Westphalian sovereignty (p. 6), as its composite layers of computational and noncomputational elements—ranging from rare earths and fiber optic cables to data centers and user experiences—undo and transform state jurisdiction. Platforms and infrastructures vie with nation-states over jurisdictional boundaries, while states adapt to the emergent order by developing new forms of exclusion and governance (p. 110).

For analytical purposes, the Stack is segmented in six layers, which Bratton (2015) terms Earth, Cloud, City, Address, Interface, and User: As abstracted topographies of sociotechnical entanglements, these layers help grasping "the multiplication and superimposition of . . . sovereign claims over the same site, person, and event" (p. 111). The emergence of planetary computation as an accidental megastructure upends flattened geographies of technological development and nodal representations of communication networks, for "there is no geography without first topology, and . . . no *nomos* without *topos*: no stable geopolitical order without an underlying architecture of spatial subdivision" (p. 24). According to Bratton's extensive description of this megastructure, the Stack is both the *topos* and the *nomos* of computational modernity, and grasping its implications requires a thorough overhaul of theories of sovereignty and governance.

Before Bratton's (2014) capital "S" theorization, the stack has been transported from its role as a software structure to a conceptual model to understand the layered and recursive topology of computational media. Rory Solomon's (2013) work tracks how the stack has become a "meta-concept" used by computer scientists to design and represent the architecture of various computational systems (p. 8). From the OSI stack hierarchy of system networking to the countless stack-like diagrams designed to explain the layered structures of computational systems, this metaphor has become a pervasive, if arbitrary, topological model of the digital (p. 9). Shannon Mattern (2014) reaches a similar conclusion in her investigations of the black boxes constituting the "smart city," identifying an "urban stack" hidden behind the layered interfaces of city technologies. Other authors develop Bratton's idea to model systems ranging from the Git version-control (Straube, 2016) to urban data infrastructures (Shapiro, 2017).

From technical analyses to speculative investigations, most discussions of the stack respond to broad systemic changes in communication infrastructures and networked systems. Bratton (2014) himself concludes his topological inquiry by imagining a "Black Stack" that looms large in the near future, a "computational totality-to-come" that could arise from the ongoing reconfiguration of governance and sovereignty. Responding to this vision of a seemingly unavoidable technological totality, Tiziana Terranova (2014) proposes to reclaim the relationship between algorithmic automation and capital flows by actively constructing a "new nomos for the post-capitalist common," a "Red Stack" that could function as an infrastructure for autonomist politics and an escape route from the neoliberal paradigm of computation. A similar yearning for alternative stack models motivates Nick Dyer-Witheford's (2013) genealogical excavation of "red plenty platforms" from socialist experiments. When it comes to China, positing the emergence of a "red stack" (de Seta, 2018) risks conflating the aspirational gradient of post-Marxist politics with the much more official color palette symbolizing the Chinese Communist Party's technocratic governance (Xiang, 2019). More than superficial differences in geopolitical coloration, what demands further analysis is the topology of these emerging infrastructural assemblages.

After reviewing this body of literature, I argue that the recurring use of the term "planetary" as a less charged synonym for "global" in theorizations of the stack often reinforces an equivalence between American platforms and the emergence of computational megastructures, reinforcing the normative implications of previous models. To their credit, both Terranova and Bratton recognize that the Stack traverses an increasingly multipolar context in which transnational bodies, international coalitions, and private companies stake their claims over governance and sovereignty—with China being an increasingly central actor. For Terranova, *shanzhai* innovation offers an example of infrastructural commoning, while for Bratton the "Sino-Google conflict" of 2009 functions as a case study in clashing territorial logics. And yet, despite its centrality in infrastructural networks and its imbrication in global supply chains, China has been remarkably absent from discussions of the stack, and at best only hinted at. Given the pressing sociotechnical —and even cosmotechnical (Reed, 2019)—implications of this emerging topology of computation, situating the stack in China, and China in the stack, becomes an urgent theoretical and analytical task.

Three Configurations of the Chinese Stack

After conceptualizing computational infrastructure through stack models, the question moves to situating China in this context. Is China absorbed into the emerging informational megastructure and enrolled in its autopoietic unfolding? Or has China instead developed a national "red stack" buttressed by homegrown ICT industries and shaped by authoritarian state control? Is Chinese state jurisdiction reinforced or challenged by the increasingly central role played by the country in the meshes of planetary computation? My contention is that these questions cannot be answered by topographical representations, which are useful to shed light on individual layers but fail at accounting for their overlap and articulation. Instead, it is necessary to model a topology of the stack by following the "tracings" (Straube, 2016, p. 7) of different technologies and practices of use. Rather than remapping individual layers of the stack to the Chinese context—a strategy that would likely merely confirm the overall heuristic validity of this model—I draw on individual case studies to outline three configurations of technologies and practices that intersect or traverse multiple layers at once.

In Bratton's (2015) model, the six layers of the Stack—Earth, Cloud, City, Address, Interface, and User—are traversed by "columns," communicational structures inspired by the way messages travel through the OSI stack or via the TCP/IP protocol (p. 61). The column is a U-shaped trajectory initiated by a user (either human or nonhuman) that tunnels up and down across layers, enrolling the entire stack in each interaction (p. 67). Throughout its path, different actors lay claim to individual layers, but are never able to control the whole structure (p. 69). The aim of the following sections is to expand the repertoire of topological configurations beyond the column by drawing on case studies of the Chinese stack. The three configurations proposed below articulate layers at different scales and from different perspectives, being at the same time descriptive models and analytical tools: the gateway, the sieve, and the dome.

The Gateway

Always activated as part of a column, the gateway is not an integral part of any specific stack layer, but functions as a shortcut between layers and across jurisdictional boundaries. In infrastructure studies, a gateway is usually understood as an element that allows the integration of two or more systems. In large technical systems, gateways succeed in virtue of their initial flexibility, but subsequently undergo processes of standardization and gradually solidify, resulting in their "sociotechnical entrenchment" and their possible replacement by more flexible competitors (Egyedi, 2001, p. 41). Gateways are a central subject of infrastructural analyses because they function as interfacial components that are "crucial to the move from isolated systems to genuine infrastructure" (Edwards, Bowker, Jackson, & Williams, 2009, p. 367). Typical examples of infrastructural gateways include socket plugs and ISO containers; once computation draws infrastructures into a stack, gateways become even more indispensable, as "pivot points" that "translate between technological time-spaces" (Straube, 2016, p. 8).

The Quick Response (QR) code is an example of a gateway technology being accidentally enrolled into the stack and successfully becoming a new industry standard. Originally designed in Japan in 1994 for the tracking of components in the automotive industry, the QR code is a machine-readable matrix barcode capable of storing different kinds of data while affording rapid read times and greater redundancy than UPC (Universal Product Code) barcodes. For around two decades, the QR code was used for purposes ranging from item tracking to novelty marketing, but it did not function as an infrastructural gateway outside of isolated or specialized systems. In the early 2010s, inspired by its popularity in Japan and Taiwan, Tencent's instant messaging app WeChat introduced the possibility to generate a personal QR code through which users could connect by simply pointing their mobile device's camera to someone else's screen. Once users were familiarized with this sort of encoded mediation—which was rapidly appropriated by numerous other apps—QR codes became the technology of choice for the deployment of digital payment systems by platform companies like Tencent and Alibaba.

In the span of a few months, smartphone users in China could scan QR codes not only to add social media contacts or participate in platform-sponsored lucky draws but also to exchange money between digital wallets and to pay for services and commodities in shops. Tencent and Alibaba—the two players that as of 2020 control the large majority of China's digital payment market—pioneered a two-pronged strategy that relied on the flexibility of the QR code to lock both consumers and businesses in their platform ecosystems, bypassing competing payment infrastructures and encouraging users to carry on monetary transactions into their proprietary apps by linking their credit cards and bank account (Plantin & de Seta, 2019, p. 265). Easy to scan on both screens and physical supports, portable and reproducible, instantly recognizable and capable of being interpreted by most mobile device cameras, the QR code has become one of the defining artifacts of the Chinese stack, and its popularity has in turn sustained its adoption in an even broader range of use cases. Besides being lined up over the counters of stores and stalls across China, indexing the proliferation of digital wallets and membership platforms, the iconic square matrixes are currently used to unlock shared bikes, verify tickets, book appointments, and even dispense toilet paper in public bathrooms.

In the context of China, the QR code is an exemplary case study of how the flexibility of a gateway technology is exploited to replace competing systems and becomes entrenched in the same process of consolidating infrastructure—in this case, the one supporting commercial and financial transactions. As Paul Edwards and coauthors (2009) have noted, societies are constantly transformed by their infrastructures (p. 372), and this is nowhere more evident than in the profound effects that QR codes have on Chinese society: By creating a shortcut between users (consumers and businesses) and the financial institutions taking care of their transactions (banks and platform companies) through widely available devices (smartphones and printed labels), this technology crossed over from being a "market infrastructure" (Kjellberg, Hagberg, & Cochoy, 2019) to becoming a veritable infrastructural gateway to the stack (see Figure 3). Reportedly, QR code usage in China accounts for more than 90% of global use (Y. Liu, 2019), and market research has traced the impacts that QR codes—and the stack they are gateways to—have had on the development of e-commerce and the overall financialization of Chinese society (Jia & Winseck, 2018).

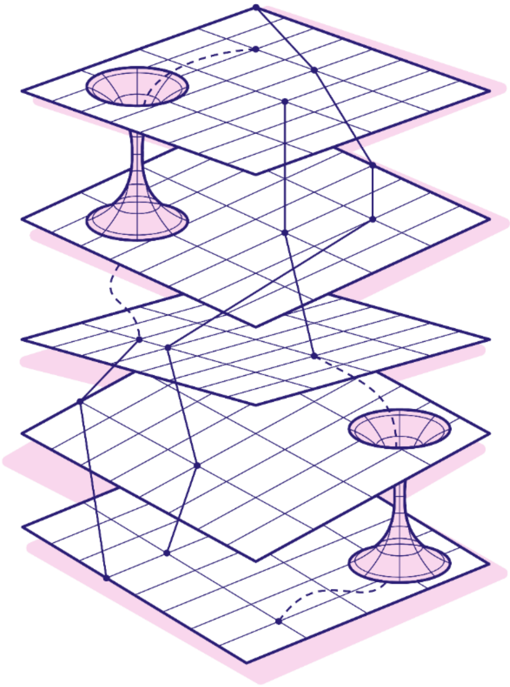

Figure 3. Gateways function as shortcuts between layers of the stack.

The portability and reproducibility of QR codes allows these gateways to extend beyond the jurisdictional domain under which the companies and institutions they connect fall under. For example, the proliferation of businesses accepting payments via Alipay, WeChat Pay, and similar platforms outside of China (first in East Asia, then all over the world) evidences how the flows of tourism and economic migration transport these gateways outside of the national territory, where commercial actors are encouraged to enroll in the various payment systems favored by Chinese consumers, thereby extending the reach of the platform companies controlling them and further entrenching the gateway as a standard. In 2017, the EMVCo consortium (which has members including American Express, Mastercard, RuPay, and Visa) published the first version of the industry standard for QR code payments under the leading role of Chinese financial service corporation UnionPay (Ren, 2017). In 2019, the People’s Bank of China released a three-year plan for a regulatory framework detailing the interoperability of QR code payment services, that will allow merchants to display a universal code for different payment service providers and challenge the Alibaba-Tencent duopoly (Y. Zhang, Yuan, Qu, Liu, & Han, 2019).

In a bid to upend the U.S. dominance on addressing systems, standardization has been a key driver of China’s techno-nationalist informatization policy (Suttmeier & Yao, 2004), and policy pushes for the country's active involvement in standard-setting processes have led to standard wars around protocols like WAPI or 3G (Qiu, 2010) and struggles to achieve a leading position in the standardization of IPv6 and 5G (Zhao, 2010). Gateways like the QR code, based on publicly available specifications, demonstrate how unassuming technologies can find unexpected use cases exploiting their flexibility to scale up entire infrastructural systems out of situated local needs (Edwards et al., 2009, p. 370) and later become industry standards. In the more abstracted terminology of Bratton's (2015) Stack, the QR code is a gateway nested between the Interface and Address layers, a "technical-informational machine, compressed into graphical or objective formats, that links or delinks *Users* and the *Addressed* entities up and down columns within the Stack" (p. 220). With their minimal matrix of machine-readable black and white squares, QR codes exemplify the gateway: a topological configuration of the stack that allows transactions between users to articulate new intersections of the Cloud layer of platform economy and the City layer of computational urbanization.

The Sieve

The sieve also operates in-between layers of the stack, but—in contrast to the gateway—its main purpose is not infrastructural articulation but rather the splitting and redirecting of columns. Anthropologist Paul Kockelman (2013) has extensively unpacked the concept of "sieve" in his work on the Bayesian equation, which is at the core of "an algorithm that underlies various computational technologies—most notably spam filters, but also data-mining tools, diagnostic tests, predictive parsers, risk assessment techniques" (p. 33). For Kockelman, the sieve is both a physical device and an analytic concept (p. 34) useful to understand various constructs ranging from laws to infrastructure and from border checkpoints to prescriptive grammars (p. 35). Algorithms are sieves, and so are the multitude of filters, blacklists, verification systems, terms of consent, and state regulations that determine a user's experience of initiating any column that passes through the territorial jurisdiction of the People's Republic of China. The sieve is an integral component of the Stack, but its centrality and legibility (arguably in part purposefully promoted by authorities) has made it a defining component of the Chinese stack—especially as it is imagined from the User position.

The sieve metaphor has been a constant presence from the early years of informatization. Deng Xiaoping's call to swat out informational "flies," the idea of a Great Firewall to keep selected content out of reach, and Fang Binxing's comparison between data and polluted river water challenging the geographical sovereignty of downstream countries, all respond to this sifting imperative. While being infamously known as the chief developer of the Great Firewall, Fang Binxing's theory of network security extends beyond the censorship of online content: His "five fours" articulate a security stack consisting of four layers (physical, operation, data, and content) with four basic attributes (availability, confidentiality, identifiability, and controllability), four goals, four assurances, and four basic rights of network sovereignty (Fang, 2011). Sifting is a necessarily layered operation: The stack includes Cloud-level filtering at different horizontal scales, and the flows passing through data centers are only global in principle, since they can be "filtered or unfiltered by both national and international authorities (including mass interception of all traffic, national firewalling and keyword sorting, targeted deep packet inspection, or . . . complete blocking of a national top-level domain)" (Bratton, 2015, p. 123).

Besides the most widely discussed sieves—keyword blacklists regularly released by state authorities, the DNS poisoning and filtering happening at the ISP or backbone level—there are other sieves operating at every layer of the Chinese stack. Common experiences of split or redirected columns span across the Earth layer (geoblocked content, national app stores), City layer (lack of network access or slow connection speed), Cloud layer (selective unavailability of services, limitations on crossing between competing platforms), Address layer (unresolvable addresses, inaccessible content, personal identification through registered mobile number or document), Interface layer (peer pressure, delegated platform censorship), and, finally, at the User layer (self-censorship and internalized norms). One of the advantages of understanding sifting as something happening at multiple points throughout a stack is that the role of state authorities is put into relation to platform responses to regulations, market economy compromises, and user practices. Moreover, the effects of the multiple sieves crossed by every column are not necessarily additive: as Kockelman (2013) notes, the superimposition of sieves can be counterproductive, and even shape the information that passes through them with the features they were designed to screen out (p. 36). The multitude of strategies through which Chinese Internet users foreground and mock the absurdity of certain occurrences of censorship, ranging from linguistic codes to technical workarounds, is a clear example of this phenomenon.

Another property of sieves is that, in splitting columns and dividing data flows, they not only shape the experience of users but also generate and feed data back to their designers or owners. Sieves produce "patterns and hence predictability" (Kockelman, 2013, p. 38), and it is not surprising that their use for the preemptive policing of information and the maintenance of platform sovereignty is part of the picture. Rogier Creemers (2017) suggests that the reconfiguration of Internet governance under Xi Jinping has redirected surveillance toward the automation and big data analytics, largely made possible by the ubiquity of mobile devices and cloud computation; from the state's point of view, this has meant a shift from a panoptic mode of surveillance to a "panspectral" one, in which technology is used to render society "legible and predictable" (p. 89). Sieves shape how columns travel through the stack, and what the users initiating them lose in legibility is gained by other sovereign actors residing at multiple layers: smart city systems, cloud platform companies, state authorities, quantifying interfaces, and even other users interpreting each other's interactions with the structure, all partake in this redistribution of legibility.

Sieves are an integral part of the stack, and operate at every layer of computation (see Figure 4). China is commonly described in terms of its far-reaching Internet censorship, but the prominence of filtering in the experience of users suggests that sieves are not necessarily more pervasive than other national contexts as much as they are purposefully and selectively made more or less visible—for example, through state propaganda and disciplinary campaigns, or through platform companies' self-criticism, and moderation measures. The actors responsible for different sieves (including filtering algorithms, state policies, market segmentation, and so on) are required to continually update and redesign them according to their emerging desires and unpredictable composite effects (Kockelman, 2013, p. 48). The push and pull happening on sieves from contiguous layers also undermine their efficacy, and two examples of this tension are observable in the politics of data flows and the negotiation of platform governance.

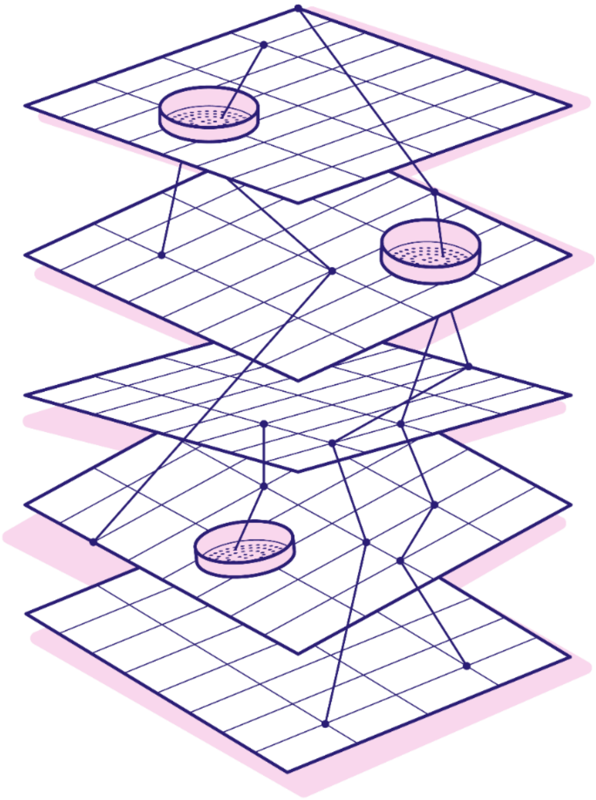

Figure 4. Sieves split and redirect columns as they travel through the stack.

In the first case, the Chinese regulations regarding the geographical location where data should be processed and stored are offset by market pressures, and their implementation is delayed to safeguard the business of cloud computing providers (Hong & Goodnight, 2019, p. 14). Sieves are put in place and then loosened, as data keep precariously flowing between protectionist measures and market demands. In the second case, the governance of platforms is fragmented by the conflicting demands of global digital capitalism and the state's attempts to safeguard public interest and national security (Hong & Xu, 2019). As Chinese platform companies expand internationally, authorities renegotiate their legal liability to maintain control over the social effects of this consolidating economy. Operating between all layers of the Chinese stack, sieves of multiple kinds split and redirect columns according to the intersection of heterogeneous norms, regulations, and interests; single-layer topographies of filtering miss the sometimes counterproductive and generative effects of sieves, and a topological account helps foregrounding their composite effects on legibility, governance and sovereignty.

The Dome

While gateways and sieves operate between layers, articulating their interaction and channeling columns across them, domes segment planetary computation in self-representational enclosures that seek to project their sovereignty vis-à-vis the rest of the Stack. In social and cultural theory, domes are most often associated with the enveloping reach of imagined communities and the protection warranted by geopolitical spheres of influence (Latour, 2009). Simon Marvin's (2015) work on volumetric urbanism identifies the popularity of the dome as a model for the enclosure of city spaces, indexing a shift "from two-dimensional to three-dimensional forms of secure enclosure" that are "less about the control of a boundary and more about the control of volumetric space" (p. 239). Given how Bratton's model of the Stack posits an underlying contiguousness of planetary computation, domes become useful to comprehend how local, national, and regional projects externalize the securitization of "digital territories" and commensurate their sovereign claims beyond national borders (Möllers, 2020).

Chinese digital infrastructure is a paradigmatic example of how domes intersect with the stack. In 1992, when the Internet still approximated an American projection of globality, the United States declined China's request to connect to the network on the grounds of national security risks (Zhao, 2010, p. 266). A decade later, as the "Chinese Internet" leapfrogged toward domestication alongside the development of its censorship apparatus, China started being referred to as one of the "black holes" of the Internet, where freedom of speech was swallowed by authoritarianism. The gradual articulation of a Chinese concept of cybersovereignty, up to Xi Jinping's calls for a "community of shared future for mankind," have contributed to China's proposal of a multilateral alternative for the governance of the emerging stack (McKune & Ahmed, 2018). This reshuffling of global Internet governance has been accompanied by accusations of the "balkanization" of the Internet, or warnings against the threat of China's influence on communication networks. The successes of China's tech industry on global markets (specifically in the domains of manufacturing, artificial intelligence, and 5G infrastructure) have triggered a resurgence of Cold War rhetoric that either reduce these adjustments to a bipolar "tech war" between superpowers (Lee, 2018) or conflate agencies across layers, identifying a Chinese effort in digital empire building (Keane & Yu, 2019).

One of the blind spots of the stack model is that, in describing an emergent totality through familiar examples of platform companies and Anglo-American contexts, it might appear to replicate ethnocentric topographies of computation. Pressed by the need to account for how states absorb computational infrastructure and integrate informational flows to secure territories, Bratton (2018) has updated his model by introducing the concept of "hemispherical stacks." Hemispherical stacks are versions of the Stack "for which the steerage of the state, even if unbound by Westphalian borders, is paramount" (p. 80); they partition the vertical topology of computation over existing territorial jurisdictions, national imaginations, and cultural histories, and confront each other with competing models of governance while also negotiating a necessary degree of integration. For Bratton, three hemispherical stacks are currently staking their claims to planetary computation: the American stack, the Chinese stack, and the European stack (p. 80). Their different approaches to sovereignty—epitomized by neoliberal market economy, techno-nationalist developmentalism, and regulatory protectionism—extend beyond the national or regional borders of the territories they are grounded in and push against each other at the Interface layer, revealing how hemispherical stacks are both "projects and projections" (p. 82).

While the concept of hemispheric stacks succeeds in situating different models of governance, a hemisphere is a specific type of dome resulting from the halving of a sphere, and this could still suggest an intrinsic bipolar split of planetary computation. The plurality of stacks as projects and projections can instead be understood in terms of domes jostling and occasionally intersecting at different layers. In this sense, the Chinese stack is rendered visible as a dome, the self-representational enclosure of a national computational project that is sustained, as a projection, from both the inside and the outside (see Figure 5). From the inside, the Chinese stack is enveloped by a dome sustained by the struggle to develop indigenous computing, the proud adoption of *guochan* (national manufacture) devices, and a broad spectrum of patriotic support of homegrown technologies. From the outside, this dome projects soft power campaigns and diplomatic outreach on social media, an alternative model for infrastructural development, and an attractive tech industry landscape for venture capital investment. The dome is how sovereign states imagine themselves as in control of the stack: As illustrated by current articulations of cybersovereignty, China strives to rein in the challenges brought by planetary computation under its national jurisdiction through the vertical force of state governance and law (Hao, 2018).

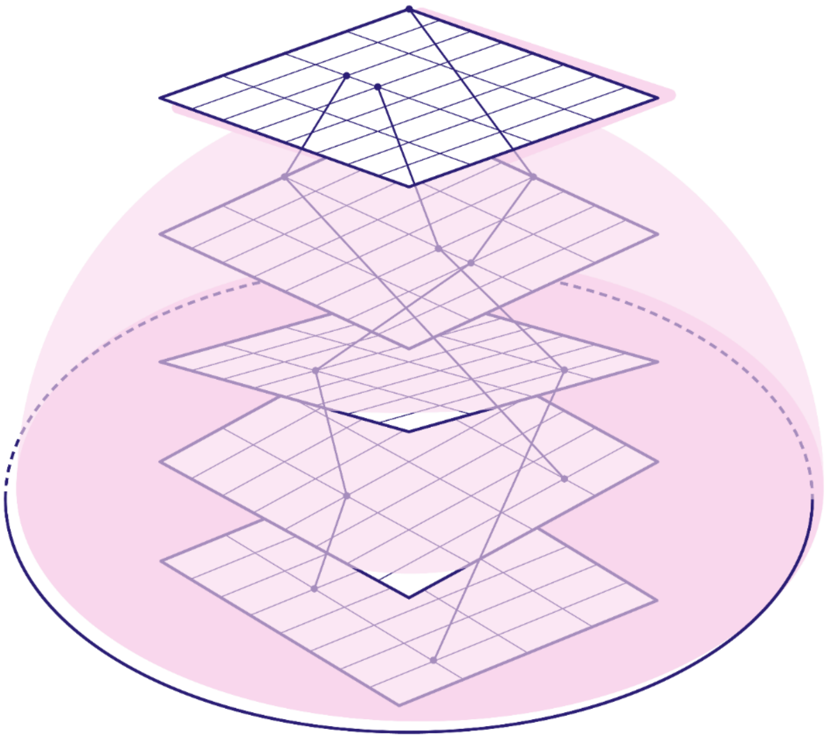

Figure 5. Domes segment the stack in self-representational enclosures that function as both project and projection.

Understanding the Chinese stack as a dome allows to reproach project and projection, and more generally to emphasize how, in a generalized undoing of sovereignty across the globe, states incorporate features of the stack as much as the stack incorporates features of a state. Topologically speaking, a dome is not an element mediating between layers nor a point of contact between them, but an extension of the Interface layer that coalesces into a representation that a stack gives to itself: an "interfacial regime" (Bratton, 2018, p. 80) negotiating the redefinition of sovereignty as it confronts other domes doing the same thing. The Chinese stack is not even subsumed into a singular, coherent dome, as its scope depends on the actors and positions doing the projecting: the securitized enclosure promised by the Chinese state is slightly offset from (and occasionally conflicting with) the enticing interior marketed by cloud platforms to international clients, and so on. Being the result of the stack incorporating features of the state such as verticality and encompassment (Ferguson & Gupta, 2002), domes help making sense of the paradoxical coexistence of infrastructural trade wars and supply chain dependencies, for the intersection of interfacial regimes and the resulting enclosures does not neatly overlap with connections and linkages at the Cloud, City or Address layers.

Conclusion: Infrastructural Topologies to Come

The goal of this article is to conceptualize a topological model capable of accounting for the scale and complexity of China's digital infrastructure. In the first half of the article, I have identified a series of heterogeneous and contrasting topographical imaginations that have been used to describe Chinese ICT development, arguing that they lack the depth and nuance to capture shifts in planetary computation that increasingly transcend established frames of analysis. At the beginning of the 2020s, as China takes a leading position in the development of digital technologies, it is necessary to move beyond topographical representations and conceptualize the layering and overlap of computational structures at multiple scales through the use of topology. For this purpose, I have introduced Benjamin Bratton's theorization of the Stack: Analyzing communication infrastructure through the stack model allows one to trace how different actors restructure across multiple sociotechnical layers. Because many discussions of the stack conflate its planetary scale with familiar Euro-American case studies, I have argued that China—with its techno-nationalist policies, expansive tech industry, and burgeoning platform companies—needs to be urgently situated within this model.

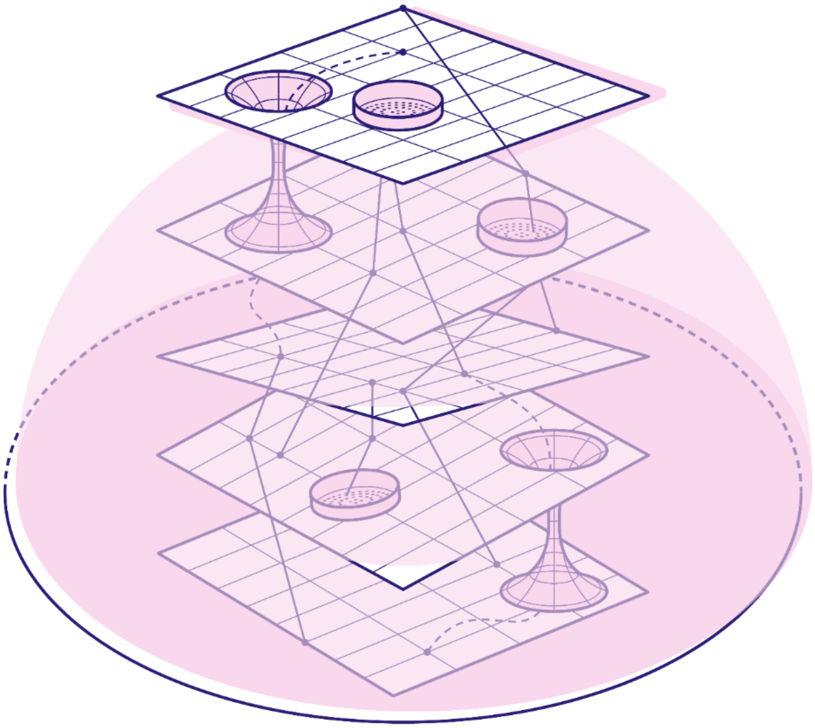

Figure 6. Gateways, sieves, and domes expand the topology of the stack.

In the second half of this article, I have expanded the conceptual vocabulary of the stack through three topological configurations: the gateway, the sieve, and the dome (see Figure 6). Drawing on case studies at different scales—QR codes as gateways, censorship, and filtering as sieves, cybersovereignty projections as domes—I have explained how these topological configurations complicate the model of the stack with much needed nuance. More specifically, I have illustrated how gateways consolidate contingent and flexible contact points between stack layers into standardized infrastructures; how sieves complicate the functioning of censorship through their unpredictable and counterproductive interactions; and how domes visibilize the interface between stack and state sovereignties, as projects that double as projections. These three topological configurations are identified through case studies of Chinese digital infrastructures, and some of their features are clearly connected to the history of China ICT development; at the same time, their situated emergence does not necessarily imply national boundedness. Gateways, sieves, and domes are not a complete repertoire of stack topology, and might combine or split up, forming other configurations: as situated convergences of *topos* and *nomos*, they offer useful analytical tools in other Asian contexts and beyond, particularly when the interaction between stack and nation-states demands new theoretical models.

The advantages of modeling digital infrastructure topologically can be exemplified by revisiting the fraught development of the PLCN cable described in the introduction. The 12,971-km submarine cable, deployed by a transnational consortium including a Chinese broadband provider and American platform companies, was promoted to its investors as a convenient and reliable gateway to the Asia-Pacific and, hopefully, to the Chinese market. Its projected operations have been profoundly shaped by the sieves operating on both of its ends, including the restrictions of the Chinese operations of Google and Facebook and the halt imposed by U.S. regulators. Its geopolitical destiny, caught in the frictions between the Chinese and American domes, deforms the topology of this infrastructural linkage and has cascading impacts on planetary computation: Taiwan and the Philippines—the cable's functional landings as of July 2020—gain prominence as East Asian network hubs, while Hong Kong loses some of its shine as a regional access to the Chinese market. In this specific case, the surface tension between two domes is ruptured by sieves that determine the outcome of a specific infrastructural gateway; in other instances, these configurations might interact in substantially different ways, deforming the stack and reorienting its layers while preserving its emergent purchase on computation and its challenges to national sovereignty.

References

Austin, G. (2014). *Cyber policy in China*. Cambridge, UK: Polity.

Barme, G. R., & Sang, Y. (1997, June 1). The Great Firewall of China. *Wired*. Retrieved from http://archive.wired.com/wired/archive/5.06/china_pr.html

Bratton, B. H. (2014, March). The Black Stack. *E-Flux Journal*, *53*. Retrieved from http://www.e-flux.com/journal/the-black-stack/

Bratton, B. H. (2015). *The Stack: On software and sovereignty*. Cambridge, MA: MIT Press.

Bratton, B. H. (2018). On hemispherical stacks: Notes on multipolar geopolitics and planetary-scale computation. In S. Wang (Ed.), *As we may think: Feedforward: The 6th Guangzhou Triennial* (pp. 77–85). Guangzhou, China: Guangdong Museum of Art.

Chang, C. (2020, April 9). Google set to use U.S.–Taiwan undersea cable. *Taiwan News.* Retrieved from https://www.taiwannews.com.tw/en/news/3913150

Chen, G. (1988, September 20). Xinxi · jiezou · weilai—Fang Meiguo zhuming weilaixuejia Tuofulei fufu [Information, rhythm, future: Interviewing the Tofflers, famous couple of American futurologists]. *People's Daily*, p. 7.

Chen, J. Y., & Qiu, J. L. (2019). Digital utility: Datafication, regulation, labor, and DiDi's platformization of urban transport in China. *Chinese Journal of Communication*, *12*(3), 274–289. doi:10.1080/17544750.2019.1614964

Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, *26*(103), 85–100. doi:10.1080/10670564.2016.1206281

Dai, X. (2002). Towards a digital economy with Chinese characteristics? *New Media & Society*, *4*(2), 141–162. doi:10.1177/14614440222226316

de Kloet, J., Poell, T., Guohua, Z., & Yiu Fai, C. (2019). The platformization of Chinese society: Infrastructure, governance, and practice. *Chinese Journal of Communication*, *12*(3), 249–256. doi:10.1080/17544750.2019.1644008

de Seta, G. (2018, April 17). *Into the Red Stack*. https://hkrbooks.com/2018/04/17/into-the-red-stack/

Dr. Peng Group. (2019, July 5). *Dr. Peng Cloud is actively engaged in writing of the White Paper, to promote development of cloud network convergence.* Retrieved from https://www.drpeng.com.cn/en/news/35/242.html

Dyer-Witheford, N. (2013). Red plenty platforms. *Culture Machine*, *14*, 1–27.

Edwards, P. N., Bowker, G. C., Jackson, S. J., & Williams, R. (2009). Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems*, *10*(5), 364–374. doi:10.17705/1jais.00200

Egyedi, T. (2001). Infrastructure flexibility created by standardized gateways: The cases of XML and the ISO container. *Knowledge, Technology & Policy*, *14*(3), 41–54. doi:10.1007/s12130-001-1015-4

Endeshaw, A. (2004). Internet regulation in China: The never-ending cat and mouse game. *Information & Communications Technology Law*, *13*(1), 41–57. doi:10.1080/1360083042000190634

Fang, B. (2011, November 15). Weilai wangluo de anquan wenti [Future network security issues]. *Sina Tech.* Retrieved from http://tech.sina.com.cn/t/2011-11-15/11396321935.shtml

Ferguson, J., & Gupta, A. (2002). Spatializing states: Toward an ethnography of neoliberal governmentality. *American Ethnologist*, *29*(4), 981–1002. doi:10.1525/ae.2002.29.4.981

FitzGerald, D., & O'Keeffe, K. (2020, February 7). Tech giants seek Hong Kong alternative after U.S. blocks data cable. *The Wall Street Journal*. https://www.wsj.com/articles/tech-giants-seek-hong-kong-alternative-after-u-s-blocks-data-cable-11581100520

Hao, Y. (2018, January 29). *Wangluo shijie de yuanzexing yu linghuoxing—San shijiao xia wangluo zhuquan de duili tongyi* [The principledness and flexibility of the cyber world—The unity of opposites in cyber sovereignty from three perspectives]. Retrieved from http://www.dgcs-research.net/a/xueshuguandian/2018/0103/70.html

Hartford, K. (2000). Cyberspace with Chinese characteristics. *Current History*, *99*(638), 255–262.

Hecht, J. (2018, January 5). Submarine cable goes for record: 144,000 gigabits from Hong Kong to L.A. in 1 second. *ITU News.* Retrieved from https://news.itu.int/submarine-cable-hk-la/

Hong, Y. (2016). Zhongguo yu guoji hulianwang: Boyi shi de guoji ronghe [China and the global Internet: A contested convergence]. *Xinwen Yu Chuanbo Yanjiu*, *B12*, 108–113.

Hong, Y., & Goodnight, G. T. (2019). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication*, 1–19. doi:10.1080/17544750.2019.1687536

Hong, Y., & Xu, J. (2019). Toward fragmented platform governance in China: Through the lens of Alibaba and the legal-judicial system. *International Journal of Communication*, *13*, 4642–4662.

Jia, L., & Winseck, D. (2018). The political economy of Chinese Internet companies: Financialization, concentration, and capitalization. *International Communication Gazette*, *80*(1), 30–59. doi:10.1177/1748048517742783

Keane, M., & Yu, H. (2019). A digital empire in the making: China's outbound digital platforms. *International Journal of Communication*, *13*, 4624–4641.

Kjellberg, H., Hagberg, J., & Cochoy, F. (2019). Enacting a digital market infrastructure in the U.S. grocery retail sector, 1967–2010. In M. Kornberger, G. C. Bowker, J. Elyachar, A. Mennicken, P. Miller, J. R. Nucho, & N. Pollock (Eds.), *Thinking infrastructures* (pp. 207–232). Bingley, UK: Emerald Publishing Limited.

Kockelman, P. (2013). The anthropology of an equation: Sieves, spam filters, agentive algorithms, and ontologies of transformation. *HAU: Journal of Ethnographic Theory*, *3*(3), 33–61. doi:10.14318/hau3.3.003

Latour, B. (2009). Spheres and networks: Two ways to reinterpret globalization. *Harvard Design Magazine*, *30*, 138–144.

Law, J. [John], & Mol, A. (2001). Situating technoscience: An inquiry into spatialities. *Environment and Planning D: Society and Space*, *19*(5), 609–621. doi:10.1068/d243t

Law, J. [Julienna]. (2020, January 20). Jumping the Great Firewall: How Google continues to operate in China. *RADII*. Retrieved from https://radiichina.com/great-firewall-google-china/

Lee, K. (2018). *AI superpowers: China, Silicon Valley, and the new world order*. New York, NY: Houghton Mifflin Harcourt.

Liu, X. (2019). *Information fantasies: Precarious mediation in postsocialist China*. Minneapolis: University of Minnesota Press.

Liu, Y. (2019, August 29). Erweima: Ruyingsuixing saoxingtianxia [QR codes: Inseparable, go scan the world]. *People's Daily Overseas Edition*, p. 9.

Lury, C., Parisi, L., & Terranova, T. (2012). Introduction: The becoming topological of culture. *Theory, Culture & Society*, *29*(4/5), 3–35. doi:10.1177/0263276412454552

Malecki, E. J., & Wei, H. (2009). A wired world: The evolving geography of submarine cables and the shift to Asia. *Annals of the Association of American Geographers*, *99*(2), 360–382. doi:10.1080/00045600802686216

Marvin, S. (2015). Volumetric urbanism: Artificial "outsides" reassembled "inside." In O. Coutard & J. Rutherford (Eds.), *Beyond the networked city: Infrastructure reconfigurations and urban change in the North and South* (pp. 227–241). London, UK: Routledge.

Mattern, S. (2014). Interfacing urban intelligence. *Places Journal*. doi:10.22269/140428

McKune, S., & Ahmed, S. (2018). The contestation and shaping of cyber norms through China's Internet sovereignty agenda. *International Journal of Communication*, *12*, 3835–3855.

Möllers, N. (2020). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology, & Human Values*, 1–27. doi:10.1177/0162243920904436

Moss, S. (2016, October 13). Google, Facebook invest in U.S.–Hong Kong submarine cable. *Data Centre Dynamics.* Retrieved from https://www.datacenterdynamics.com/en/news/google-facebook-invest-in-us-hong-kong-submarine-cable/

Mozur, P., & Lin, Q. (2019, February 7). How Facebook's tiny China sales floor helps generate big ad money. *The New York Times*. Retrieved from https://www.nytimes.com/2019/02/07/technology/facebook-china-internet.html

Plantin, J.-C., & de Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273. doi:10.1080/17544750.2019.1572633

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. doi:10.1177/1461444816661553

Qiu, J. L. (2010). Chinese techno-nationalism and global WIFI policy. In M. Curtin & H. Shah (Eds.), *Reorienting global communication: Indian and Chinese media beyond borders* (pp. 284–304). Champaign: University of Illinois Press.

Reed, P. (2019). Platform cosmologies: Enabling resituation. *Angelaki*, *24*(1), 26–36. doi:10.1080/0969725X.2019.1568731

Ren, D. (2017, July 16). QR code takes a step toward world conquest as group adopts standard. *South China Morning Post.* https://www.scmp.com/business/banking-finance/article/2102855/qr-code-takes-baby-step-world-conquest-group-adopts-global

Schiller, D. (2008). An update on China in the political economy of information and communications. *Chinese Journal of Communication*, *1*(1), 109–116. doi:10.1080/17544750701861970

Shapiro, A. (2017). The urban stack: A topology for urban data infrastructures. *TECNOSCIENZA: Italian Journal of Science & Technology Studies*, *8*(2), 61–80.

Solomon, R. (2013). Last in, first out: Network archaeology of/as the stack. *Amodern*, *2*, 1–23.

Straube, T. (2016). Stacked spaces: Mapping digital infrastructures. *Big Data & Society*, *3*(2), 1–12. doi:10.1177/2053951716642456

Suttmeier, R. P., & Yao, X. (2004). *China's post-WTO technology policy: Standards, software, and the changing nature of techno-nationalism* (No. 7; NRB Special Report, p. 47). Seattle, WA: National Bureau of Asian Research.

Terranova, T. (2014). Red Stack attack! Algorithms, capital and the automation of the common. In R. MacKay & A. Avanessian (Eds.), *#Accelerate#: The accelerationist reader* (pp. 379–399). Falmouth, UK: Urbanomic.

Tsui, L. (2007). An inadequate metaphor: The Great Firewall and Chinese Internet censorship. *Global Dialogue*, *9*(1/2), 60–68.

Webster, G., Sacks, S., & Triolo, P. (2019, April 2). *Three Chinese digital economy policies at stake in the U.S.–China talks*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/

Xiang, N. (2019). *Red AI: Victories and warnings from China's rise in artificial intelligence*. Independently published.

Zhang, L. (2020). When platform capitalism meets petty capitalism in China: Alibaba and an integrated approach to platformization. *International Journal of Communication*, *14*, 114–134.

Zhang, Y., Yuan, R., Qu, Y., Liu, Y., & Han, W. (2019, September 23). In depth: The fight for dominance in China's mobile payment market. *Caixin*. https://www.caixinglobal.com/2019-09-23/in-depth-the-fight-for-dominance-in-chinas-mobile-payment-market-101464880.html

Zhao, Y. (2007). After mobile phones, what? Re-embedding the social in China's "digital revolution." *International Journal of Communication*, *1*, 92–120.

Zhao, Y. (2010). China's pursuits of indigenous innovations in information technology developments: Hopes, follies and uncertainties. *Chinese Journal of Communication*, *3*(3), 266–289. doi:10.1080/17544750.2010.499628