9-2024

Territorialising the cloud or clouding the territory? Volumetric vulnerabilities and the militarised conjunctures of Singapore's smart city-state

Orlando WOODS
Singapore Management University, orlandowoods@smu.edu.sg

Tim BUNNELL
National University of Singapore

Lily KONG
Singapore Management University, lilykong@smu.edu.sg

Territorialising the cloud or clouding the territory? Volumetric vulnerabilities and the militarised conjunctures of Singapore's smart city-state

Orlando Woods [a,*] , Tim Bunnell [b] , Lily Kong [c]

a College of Integrative Studies, Singapore Management University, Singapore

b Department of Geography, National University of Singapore, Singapore

c School of Social Sciences, Singapore Management University, Singapore

Published in Political Geography (2024) 115, 103211. DOI: 10.1016/j.polgeo.2024.103211

Abstract

This article explores how the volumetric characteristics of cloud computing can create new expressions of territoriality, which in turn can reveal new axes of vulnerability and threat. Whilst recent work in political geography has sought to "locate" the cloud through analyses of data centre geographies and data-driven processes of smart urbanism, we look beyond the material plane and consider the amorphous territorialities of voluminous data instead. As much as these data are acted on by the legal-regulatory mechanics of the state in a bid to territorialise them, so too do these data volumes serve to cloud, and thus obscure, territory. Processes of territorialising and clouding exist in a state of dialectical tension with each other, and reveal the volumetric vulnerabilities of cloud computing. We validate these theoretical claims through an analysis of in-depth interviews with senior stakeholders in Singapore's Smart Nation initiative. In Singapore, defending the city is equivalent to defending the nation, which causes the military to play an outsized role in securing the city-state. We consider how the attack surface of the city becomes a more voluminous construct with cloud computing, how strategies of geofencing attempt to secure the cloud, and how these processes reveal the increasingly militarised conjunctures of everyday life. Overall, these insights reveal a need for political geography to continually evolve its theoretical premises in line with the rapid digitalisation of the world.

Keywords

Cloud computing, Territory, Data volumes, Attack surfaces, Datastructures, Military, Singapore

1. Introduction

In a data saturated world – one in which a growing number of decisions and processes are automated and delivered virtually – debates concerning the role, power and influence of the state have been brought to the forefront of scholarly concern. For example, a recent special issue of the journal *Geopolitics* explored the challenges posed by trans-territorial digital services – notably clouds and digital platforms – the aim being to reveal how 'the traditional coupling of concepts of sovereignty, territoriality and the state, of jurisdiction and borders, must be rethought' (Glasze et al., 2023, p. 919). The resolutely ungrounded nature of digital innovations in general, and of data ecosystems specifically, poses both challenges and opportunities for political geography to evolve and expand in new directions. Echoing this sentiment, Baur (2023: 1) has called for scholars to 'tak[e] technology in the making and its role in (geo)politics seriously', suggesting a relatively slow integration of technology with political geography's theoretical constructs. Going further, Atkins (2021: 2, original emphasis; also Fard, 2020) is specific in his assertion that 'geographers should engage more fully with the question of *where* the 'cloud' is'. There is a deceptively simple answer to this question: the material form of the cloud is the data centre, and cities are often where the cloud is deployed in response to the data-driven demands of "smart" urbanism. We contend, however, that there is a prior step to locating the cloud that entails identifying *how* the cloud becomes locat*able*. Recognising that the cloud stretches to 'a horizon of 'infinite data' that 'act[s] on the threshold of perception itself' (Amoore, 2018, pp. 6, 4), we suggest that attention be paid to the ways in which states and other actors strive to territorialise a resolutely deterritorialised construct, and thus materialise the cloud by establishing and enforcing regimes of measurement, understanding and control.

We argue that the volumetric characteristics of cloud computing need to be foregrounded and understood if the theoretical underpinnings of political geography are to evolve alongside the digital infrastructures that increasingly mediate politico-urban life. We call these infrastructures "datastructures" in recognition of their voluminous nature, their embeddedness within (geo)political processes, and their outsized role in structuring politico-urban decisions and outcomes. Our notion of datastructure provides a generative way of reframing infrastructure in volumetric terms. Digital infrastructures often transcend territorial-political borders and reveal the complexities of territory as a trans-boundary, and increasingly volumetric – that is, three-dimensional, calculable and thus governable (Eiterjord, 2024) – construct.
Territory *becomes* volumetric through processes of datastructuring, with modalities like cloud computing, for example, both revealing and expanding the limits of territorialisation. Put differently, the datastructure causes territory to become implicated in new practices of volumetric calculation and control according to where data is located, who it pertains to, and how it is used. Whilst the "infra" prefix of infrastructure positions it – conceptually at least – *below* structure, the fact of voluminous digital data is that it already-everywhere, and thus works as an omni-directional form of structuring logic. We expose the new forms of politico-urban risk and vulnerability that emerge at the nexus of data and the voluminous geographies it reproduces. Our

aim is to reveal how the expansive "attack surface" of the cloud exposes the volumetric vulnerabilities of the city, which in turn necessitates various strategies of territorialisation. Whilst the volumetric turn within the social sciences is now well-established (Elden, 2013; Goldstein, 2019; Jackman and Squire, 2021), especially in relation to the city (Connor & McNeill, 2022; Graham, 2011, 2016; McNeill, 2019, 2020), the *vulnerabilities* that emerge from volumetricism remain unexplored, especially when understood in relation to *digital* volumes. Importantly, our focus on data volumes deliberately shifts attention away from the data centres that have hitherto been the focus of scholarship on digitally mediated territoriality (see Amoore's [2018] notion of "Cloud I" and "Cloud II" geographies). By decoupling the cloud from the data centre through which data is stored, novel understandings of territorial formation and tension that go beyond the material can be forged.

Our analysis begins with the premise that the datastructure of the cloud and the political structuring of territory exist in a state of dialectical tension with each other. This tension causes each construct to continually try and assert itself over the other, in turn exposing the fundamental incompatibility of each. Whilst the cloud is inherently voluminous, unruly, amorphous, distant, and the preserve of the machine, territory is relatively less voluminous (or rather it can be *imbued* with volume), ruled over, calculable, proximate, and the preserve of statecraft. These distinctions create tension insofar as much as governments attempt to territorialise the cloud, so too does the datastructure of the cloud work to "cloud" the territory. Territorialising the cloud is an attempt to render something that is volumetric, flat. It is an attempt to control the automated, and to rationalise the nebulous. These efforts reveal the problematic and unruly nature of data as a voluminous construct, and how the aspiration to forge a 'technical territory' (Munn, 2023a) is often elusive. On the other hand, clouding the territory occurs when the technological tools – and the data they leverage – used to manage territorial formations causes them to expand in volumetric ways. Territorial expansion along digital lines creates new axes of vulnerability and securitisation, and causes the assumptions of knowability, calculability, and rationalisation associated with the geometric plane to be challenged anew. With the expansion of territory into the realm of the cloud, the attack surface of the city expands, but so too does it become vaguer and less well-defined. No longer is territorial defence associated with the establishment and policing of borders; rather, it is about trying to *create* borders and governability in a constantly changing, and resolutely border*less* context.

We illustrate these theoretical claims through an analysis of the smart city-state of Singapore, where the overlapping of the "city" and the "state" causes matters of national security to be urban as much as they are national concerns. The defensive role of the military has caused Singapore to become a 'key theoretical site for applying a governmentality optic, given the contiguous relationship with sovereign nation-state-power' (McNeill, 2019, p. 851) and the fact that, despite its small size, it 'retains one of the best military forces in the Indo-Pacific' (Laksmana, 2017, p. 347). Increasingly, the remit of the military has expanded into the digital domain, with cyber defence becoming a key part of Singapore's military strategy, and a point of

crossover into the civilian domain. The paradox of state territoriality stems from concerted efforts to draw on 'technical expertise and various forms of calculative governance to expand the *volume* of Singaporean territory' (McNeill, 2019, p. 850, original emphasis; after Bunnell et al., 2006; Shatkin, 2014), with the widespread embrace of digital technologies under the rubric of the Smart Nation providing one of the clearest ideological moves to expand the idea of volume along new axes of understanding. However, this expansion into the digital realm creates new vulnerabilities, thus foregrounding the need for new strategies of territorialisation. These strategies, we argue, exist at the military-civilian nexus, a "military conjuncture" that emerges from the 'stacking and moving of more and more people and things above, across and below tightly defined, interlocking sites within increasingly dense spaces' (McNeill, 2020, p. 815). The embedding of military capabilities throughout the city reveals the extent to which cloud computing has a role to play in making cities increasingly vulnerable, insecure, and thus militarised constructs (after Kitchin & Dodge, 2019).

Three sections follow. The first reviews the literatures on cloud computing and data centre geographies. The second introduces the politico-territorial context of Singapore. The third is empirical and considers how the voluminous attack surface that cloud computing gives rise to foregrounds the ongoing militarisation of everyday life in Singapore.

2. Territorialising the cloud or clouding the territory?

Political geography has a long lineage of identifying and demarcating the limits of power and control. These attempts to 'bring the abstract world into vision' (Amoore, 2018, p. 10) clearly manifest through the map, and its attempts to rationalise space by flattening it in cartographic form. Whilst there have since been concerted attempts to recognise the multi-dimensionality of political worlds, advances in technology tend to outpace political thinking. The cloud is a paradigmatic example of this trend, as it 'cannot be brought into human vision … algorithms are communicating with other algorithms at speeds beyond human observational capacity' (Amoore, 2018, p. 10). Throughout the world, states wrestle with the fact that clouds are ungrounded, ephemeral and leaky datastructures, even if the actual data centres through which they manifest are 'geographically grounded, materially built up, and capital-intensive' (Fard, 2020, p. 7). Scholarship to date has focussed on the materialisations of the cloud through data centres, but the cloud gives rise to other geographies that pose less clearly defined problems for state and non-state actors. By foregrounding the volumetric capacities of cloud computing, we can appreciate the radical transformation of state territoriality in response to the datastructures that underpin new regimes of governance and control (Elden, 2013; Glasze et al., 2023; Zurita & Munro, 2019). These transformations have recently been embraced through Baur's (2023: 2) questioning of how 'ideas of innovation and progress contrast with ideas of control; how these imaginaries are entangled with the material and technological developments of cloud systems; and ultimately, how these systems are enmeshed with traditional political concepts of sovereignty and territoriality'. Below we explore the tussle between the desire to flatten something volumetric

(territorialising the cloud), and to mitigate against the vulnerabilities that volumes create (clouding the territory).

2.1. Volumetric geographies of cloud (in)security

The volumetric turn in geography has gained considerable traction over the past decade or so, and has caused urban space in particular to be understood as a more pluri-dimensional construct. Yet, as much as there have been concerted efforts to explore how 'horizontal and vertical extensions, imaginaries, materialities and lived practices intersect and mutually construct each other within and between subterranean, surficial and suprasurface domains' (Graham and Hewitt, 2013: 75), understandings of volume have often proceeded through the analytical vectors of either the built environment, or the policy or financial frameworks through which political power is asserted. In this vein, volumetric urban space is typically seen as an 'envelope through which state accumulation strategies are materialized through both the technical manipulation of territory and the metrics that accompany it' (McNeill, 2019, p. 849). Absent from these analyses, but nonetheless a vital driver of the ongoing "metricisation" of territory, is the role of data in creating new modalities of "volume". These modalities coalesce in the cloud as a volumetric metaphor for the datastructures that are driving many (smart) urban developments. Just as 'the production of digital data has accelerated tremendously over recent years' causing 'more and more processes [to be] datafied' (Glasze et al., 2023, p. 920), so too does the cloud offer a new interpretation of the volumetric. The paradox of the cloud, however, is that as much as its volumetric characteristics contain the potential for new forms of urban knowledge- and decision-making, these characteristics can also create new forms of urban insecurity. This paradox is well-captured in Baur's (2023: 2) assertion that the cloud has become an inextricable part of 'political initiatives and powerful imaginaries – imaginaries that show struggles for data security, (digital) sovereignty, economic profits, and innovative futures'.

Effective cloud computing is therefore predicated on cloud security, and cloud security is predicated on "securing the volume" (after Elden, 2013). Munn (2022: 979; see also Starosielski, 2015; Furlong, 2021) echoes this sentiment, but also reveals some of the biases that underpin existing scholarship on cloud (in)security:

> The cloud model is one predicated on security and stability. Indeed, much of the rhetoric around data centers is based around maintaining an unwavering vigilance against attacks of all kind, whether stemming from natural disaster, mechanical failure, or human sabotage … Cloud computing represents a model of power that is highly secure yet highly situated. Bunkered down and hedged in, the data centers of cloud computing form a hermetically sealed environment that cannot be penetrated by attack.

The vulnerabilities of the cloud are indexed here to its material – or data centre – form and must therefore be secured through the surface plane. By recognising and embracing the cloud's volumetric characteristics, however, we seek to extend the attack "surface" of the cloud beyond the data centre. In doing so, we also extend it beyond the traditional mapping of territory, thus

recasting territory as more of a three-dimensional network than a surficial plane. We intentionally problematise the idea of the "surface" here, as the cloud's pluri-dimensional qualities make it simultaneously surface-*less* and *omni*-surficial. This problematisation explodes the idea of a "new military urbanism" (after Graham, 2011) out into new directions; directions that are invisible, omnipresent, and often involve a deterritorialised sense of threat that comes from everywhere. These complexities means that cities' defence apparatuses must continually evolve into the digital domain, as 'smart city systems are typically large, complex and diverse, with many interdependencies and large and complex attack surfaces … [which] are multiplied due to a system's many interlocking parts, which are owned and managed by a diverse set of stakeholders' (Kitchin & Dodge, 2019, pp. 50, 48; see also Amoore, 2018). Indeed, whilst Kitchin and Dodge (2019) provide a comprehensive overview of the cybersecurity challenges that all smart cities face – and highlight various mitigation and prevention strategies – they do not engage with the theoretical questions of how territoriality is being recalibrated through the volumetric geographies of the cloud. Recently, Linneman and Turner (2022: 23) extended these ideas to the realm of policing, and in doing so advance an understanding of the political geography of police power that 'pay[s] close attention to both height and depth in the fabrication and colonization of three-dimensional or volumetric political space'. We extend this trajectory further by considering how the volumetric vulnerabilities of the cloud lead to the 'creeping and insidious diffusion of militarised debates about 'security' in every walk of life' (Graham, 2011: XIV).

These are debates that are at once felt at the level of international geopolitics, but also through the everyday navigations of the city. They are mediated through the layering of the datastructures of the cloud throughout the urban environment and beyond, creating a truly global geography of cloud volumes. Writing of Chinese technology company Huawei, for example, Munn (2023b: 80) observes how it has 'steadily assembled layers of informational architecture' that have now come to 'constitute the front lines of a new battle, where control over the production, transmission and mediation of information confers a certain geopolitical advantage'. This "advantage" is premised on the creation and extension of what Munn (2023b: 80) calls a 'Chinese-centred technical territory' that works through the interstices of the public and private sectors, between data and the informational architectures that support them, between the cloud and the data centre, and, perhaps most tellingly, between the countries that are solution-providers and solution-buyers. These dynamics foreground a new geopolitical reality in which the state is caught between the competing processes of territorialising the cloud whilst also clouding the territory. As Bratton (2016: 33) puts it, the freedom spaces associated planetary-level computation consist of 'land, sea, and air all at once, equally tangible and ephemeral. It can be both inside the line of the Westphalian state and its internal legal optics but outside its borders and sovereignty'. The volumetric nature of cloud space renders it inherently leaky space that continually seeps through the cracks of the borders, boundaries and legal-regulatory frameworks that strive to contain it. It is in this vein that it creates possibilities for new understandings of cloud territorialities and the infrastructures that underpin them to emerge.

2.2. Geopolitics of territoriality and infrastructure beyond the data centre

To date, the territoriality of cloud computing has been explored primarily through the lens of the data centre. Data centres have been interpreted as the material counterpart to the amorphous cloud – something visible, tangible, and thus easy to study. Their extension outwards into the volumetric space of the cloud causes them to become multi-layered infrastructures – or what Furlong (2021: 191) calls "cloudfrastructures" – that have been 'billed as simultaneously everywhere and nowhere … with a seemingly endless potential for expansion'. Our notion of the datastructure imbues the cloudfrastructure with political potential; it is something that causes new political assertions, contestations and vulnerabilities to emerge. Whilst the cloud is a resolutely deterritorialised phenomenon, data centres are unique in that their territories can be spatially disconnected from the end-user. This sets them apart as infrastructural formations, as they 'do not necessarily need to be close to their users' (Atkins, 2021, p. 1) and has led to the development of "hyperscale" data centres that maximise economies of scale. An important point to note here is how closely data centres can be tied to the assertion or undermining of state power. Patterns of "infrastructural territorialisation" (Lesutis, 2021) have been observed, for example, in Guizhou, China, where the expansion of the data centre industry has been linked to 'broader process[es] of state-building' and the 'co-production of further state legitimation' (Pan, 2022, p. 2412). Whilst data centres have a geopolitics unto themselves – of location, positioning, and serviceable markets – there is a need to look beyond the specific geopolitics of the data centre. To look beyond is to recognise the important reality of the cloud's uniquely volumetric geography, its frustratingly amorphous nature, and above all its capacity to *obscure* and *obstruct* the workings of territory according to the logics of the state. When these factors coalesce, they foreground new geopolitics of the cloud; geopolitics that are decoupled from territorial borders, are omnipresent, and lead to the ongoing securitisation of urban life.

To be clear, this geopolitics goes beyond issues of data sovereignty and the regulation of cross-border data flows. Numerous studies have considered how the state seeks to assert 'more national autonomy in the digital sphere' (Glasze et al., 2023, p. 929). Often, they reveal the state's efforts – to varying degrees of success – to territorialise the cloud by rendering the data contained therein to be "bounded" by legal or regulatory frameworks, and thus controllable as distinct "technical territories" in which 'activities and identities are mediated through software, platforms and services' (Munn, 2023b, p. 81; also Rossiter, 2017; Rasmussen & Lund, 2018). In Europe, for example, Baur (2023: 11) considers how a "technical border" was established 'between Microsoft's globally interconnected data centres and Microsoft Cloud Germany, denying US officials access to the latter'. In the US, the relatively recent adoption of the *Clarifying Overseas Use of Data Act* (also known as the Cloud Act, 2017–2018) has seen service providers that are subject to U.S. jurisdiction being forced to submit data controlled by it or any subsidiary to the U.S. authorities. The novelty of the Act is that it allows the U.S. government to

circumvent the territorialisation of data by using a basis other than territoriality to establish its jurisdiction and collect data overseas. It invokes the nationality of the third parties that host data, and because nationality is a valid criterion for invoking and exercising jurisdiction, the law is consistent with international law. It should, however, be noted that the way that the United States interprets the criterion of nationality is very extensive, making its lawfulness under international law questionable (Glasze et al., 2023: 943).

What we see here is the U.S. government extending its reach outwards, laying claim to the data stored by data centres beyond its putative territorial borders in a bid to claw data back within its borders. To the north of the U.S., the government of Canada has passed legislation to try and enact a form of "data sovereignty" in which 'domestic public data traffic must not leave Canadian territory' the ramifications for the cloud being that 'the abstract deterritorialised cloud is … reterritorialized as an intelligible and governable entity' (Amoore, 2018, p. 8). Whilst studies like these show various attempts to territorialise the cloud, which in turn gives rise to a geopolitics of data sovereignty that is indexed to the location and control of data (centres), underemphasised is an appreciation of an oppositional, but also complementary, dynamic; that is, the "clouding" of territory along volumetric axes of vulnerability and threat. Recognising and embracing the mutually constitutive nature of "clouding" and "territorialising" will enable us to appreciate more fully the 'tension between a predominantly territorially defined form of sovereignty and the inherently global pretensions of an increasingly deterritorialised security apparatus' (Potzsch, 2021, p. 71). These tensions find meaning and value in Singapore, where the country's small size and wholesale embrace of digital governance strategies renders it both vulnerable to global forces – technological and otherwise – but also uniquely able to control its data cloud through the militarised conjunctures of the city-state.

3. Surface, security and "smartness" in Singapore

Singapore is an island city-state that has long been successful in projecting an image and impact that is bigger than its geographical landmass might suggest. These projections extend along three dimensions that might be summarised as the expansion of surface, the expansion of securitisation throughout many walks of life, and the longstanding embrace of technology, and, in recent language, "smartness", as an enabler of urban efficiency. Binding together these three dimensions is a survivalist mentality that stems from the country's location in heart of the Malay Archipelago, its lack of natural resources, and its unrelenting focus on economic development, political control and social cohesion. For the first dimension, Singapore's small size and aquatic border separating it from neighbouring Malaysia and Indonesia has caused the government to become 'highly effective in politicizing the governance and planning of space, as a means of shaping the national body politic' (McNeill, 2019, p. 854). The state has long sought to both 'maximiz[e] its territorial resources' but also to 'expand its extraterritorial presence' through processes of land reclamation (expanding the surface), and also through the 'active production and integration of high-rise and subterranean planes of economic activity (expanding the volume)' (McNeill, 2019, pp. 854, 855). These (extra)territorial expansions have seen Singapore

extend itself in three dimensions – outwards, upwards and downwards – creating a volumetric urban landscape that is plugged into 'highly competitive and standardized airspaces, and maritime geographies of global connection' (McNeill, 2019, p. 854). That said, mirroring the broader trend in the literature outlined earlier, whilst Singapore's volumetric urban landscape has been studied from the perspective of the engineering and design of the built environment, lacking is an understanding of alternative volumes that are more nebulous and harder to identify and control. These are covered in the third dimension, below.

The second dimension builds on the first, as the country's small size, coupled with its geopolitical circumstances, enforce the narrative of vulnerability whilst simultaneously validating the need for the military to play an outsized role in everyday life. As Laksmana (2017: 355; see also Tan, 2011) puts it, a 'common narrative in Singapore's strategic community is the historical experience of vulnerability – nearly an existential "angst" narrative' which originates from the fall of colonial Singapore to the Japanese in 1942 and continues to the present day. Importantly, since Singapore's separation from Malaysia in 1965, a priority was to develop the defensive capacity of the Singapore Armed Forces (SAF) from scratch. These origins are important, as 'SAF's formative leaders were not full-time military officers; they were seconded civil servants' (Laksmana, 2017, p. 355) which signals the provenance of the fact that Singapore's military is not apart from everyday civilian life, but constitutive of its very fabric (Sayin et al., 2022). As Laksmana (2017: 356) goes on to explain:

These conditions not only created an officer corps initially characterized by "civil servants in uniform", but over time, they eventually gave rise to a civil-military "fusion" where there is hardly any fundamental disagreements between the political and the military leadership regarding the SAF's basic mission, structure, posture, doctrine, and role … Conceptually, the unified civil-military relation is encapsulated in Singapore's "Total Defense" national security strategy aimed at strengthening and mobilizing resources in five mutually supportive domains: military, civil, economic, social and psychological. This framework allows Singapore to offset an array of security predicaments through integrated civil-military strategic interactions at various levels, linking the various players in Singapore's "defense ecosystem", between the users (SAF), developers (e.g. MINDEF, Defense, Science and Technology Agency or DSTA), and producers (i.e. local defense industries).

Importantly, this "fusion" between the military and civilian domains permeates all aspects of national ideology and planning. Perhaps the best example of this is the fact that National Service is mandatory for all male Singaporeans and second-generation Permanent Residents once they reach the age of 18 (with some deferments being granted for the purpose of study), and regular Reservist training thereafter to ensure that a significant proportion of the male civilian population remains "operationally ready". The fusion of the military and civilian domains also mirrors the fusion of the second and third dimensions. Specifically, the SAF is known globally for its technologically advanced military capabilities (Walsh, 2007), with advancement referring to both its military hardware and software. In 1971 the Ministry of Defence – MINDEF – established an

Electronic Warfare Study Group which in turn laid the foundations for establishing the integral role of technology in Singapore's defence ecosystem and foregrounded the formation of the Defence Science and Technology Agency (DSTA) in 2000 (Laksmana, 2017). Since then, the military-civilian fusion has become more pronounced, and more necessary, through the formulation of the Smart Nation in 2014.

In terms of the third dimension, the embedding of "smartness" in Singapore's urban fabric – by which we mean the embedding of technology within socio-spatial processes and decision-making – has a long history that predates the launch of the Smart Nation (see Kong & Woods, 2018). Notwithstanding, the digital nature of the Smart Nation, and the scalability and interoperability that comes with Big Data and cloud computing, causes the Smart Nation to be distinct from previous waves of technologisation. Specifically, the development of the Smart Nation Platform, and the Smart Nation Operating System (SN-OS) that underpins it, presents an 'ambitious example of a comprehensive and massive cloud computing platform that sets the foundation for whole-of-government policy-making and practices' (Ng, 2018, p. 43). Whilst a private cloud – known as the "Central G-Cloud" – is used for many government agencies, there has since been an embrace of "hyperscale" cloud solutions, which in turn has created a growing degree of dependence on private sector cloud service providers like Amazon Web Services (AWS). Important is the fact that having a private cloud is one of the most effective ways of "securing the volume" and thus mitigating against cyber-security threats, meaning that any reliance on private sector providers increases the attack surface considerably and thus raises the vulnerability of the city-state. This is important because, as Ng (2018) observes, the Cloud Readiness Index 2016 (compiled by the ACCA) places Singapore behind Australia, South Korea, and India in cyber-security prowess. Whilst the government has adopted a 'co-ordinated approach to deal[ing] with cyber-enabled threats' (Ng, 2018, p. 45), the fact remains that the securitisation of the Singapore city-state now transcends the geopolitics of size and location, and is implicated in the more amorphous and trans-boundary domain of cybersecurity as well. It is in this vein that the embrace of cloud computing as a key enabler of the Smart Nation can be seen to "cloud" the territory of Singapore, creating militarised conjunctures to become further embedded throughout daily life.

4. Volumetric vulnerabilities and the militarised conjunctures of Singapore's smart city-state

The empirical subsections that follow draw on qualitative research conducted amongst the architects of Singapore's Smart Nation initiative. In total, interviews were conducted between mid-2021 and mid-2022 with 32 individuals representing the public and private sectors. Notable is the seniority of our interviewees, with many of them being in leadership (i.e., Permanent Secretary, CXO, or Director-level). Also notable are the seven interviews we conducted with representatives of Singapore's defence ecosystem, including the Ministry of Defence (MINDEF); the Defence, Science and Technology Agency (DSTA); and the Home Team Science and Technology Agency (HTX). The interviews form part of a wider project on the globalising and provincialising characteristics of smart city development in Singapore in relation to other urban

contexts around the world (see Woods et al., 2023, 2024a; 2024b). All interviews were conducted by at least two of the authors, and most were conducted by all three. All interviews were also recorded, fully transcribed, and coded for themes. Given the seniority of many of our interviewees, all were given the option – and most consented – to be named in the empirical analysis that follows. Divided into three subsections, we now consider the emergence of voluminous attack surfaces and the resultant geopoliticisation of the smart city-state, geofencing and the territorial dialectics of the cloud, and the ensuing expansion of the militarised conjunctures of everyday life.

4.1. Voluminous attack surfaces and the geopoliticisation of the smart city-state

Singapore's size and location have, for decades now, been used to signal the city-state's vulnerability, and the associated need to develop outsized defensive capabilities. These characteristics also position it as an infrastructural nexus for global telecommunications providers, and increasingly for digital solutions providers as well. Simultaneously, these characteristics reveal Singapore's territorial vulnerabilities *and* strengths, and thus illustrate the fact that territory is often 'best understood as a process rather than an outcome, as an assemblage that is continually being made and remade volumetrically' (Zurita & Munro, 2019, p. 39). Nikhil Eapen, the CEO of one of Singapore's largest telcos, StarHub, explained the geopolitical uniqueness of Singapore in that it is "a bit of a focal point in Asia because all the subsea cable systems pump into Singapore, and then we've got corporations from all sides, different sides of the geopolitical spectrum [converging in Singapore]". As much as these characteristics reveal the advantages of Singapore as an infrastructural hub for industry, so too do they hint at the voluminous nature of these infrastructural assemblages and the complexities they give rise to. Nikhil went on to observe how, as a hub, "there's going to be a disproportionate amount of cyber threat acts, state-sponsored cyber threat activity, and quasi-state sponsored". These threats are voluminous in nature – they extend down into the subsea domain of pipes and cables, outwards along the bordered surface of Singapore's territorial limits, and geographically everywhere through the territorial indistinctions of the cloud. Vicky Wang, a Commander in MINDEF's Cyber Defence Group, explained how, as a result of these volumes, "the attack surface has increased because it's not just about defending our physical borders, but there are also all these networks that we depend on that others disrupt. So, there are different dimensions to defend".

Looking beyond the infrastructural assemblage that has come to define Singapore's contemporary geopolitical position, the volumes of the cloud create several unique challenges for mitigating the risks of vulnerability. Arguably the most pronounced of these is the dominance of the Smart Nation as a vision of Singapore's urban futurity. Another, however, is indexed to the complex interplay between core and edge networks that comprise contemporary cloud datastructures. As Munn (2020: 271) explains, 'rather than the closed ecosystem of the centralized data center, where a company can control access to servers, edge networks are a far more open, unrestricted architecture' that is 'more susceptible to rogue gateway attacks' because

of the ‘lack of a global perimeter’. Nikhil went on to articulate the difficulties of identifying vulnerabilities within the public datastructure of Singapore, as

if you just look at the capacity on the public clouds' workload running everywhere – core, edge, and very distributed – I think that makes the problem around threat detection and threat remediation very much more acute, because your attack surface is therefore much, much, much wider. And what that means is you can’t protect every attack surface. You need to have sort of a data lake, algorithmic, AI-based approach where you’re doing a constant, high compute, anomaly identification, and that has to be an emphasis.

What Nikhil gestures towards here is the clouding *effects* of Singapore's datastructure – its datastructuring – on its territorial (in)securities. Volumetric attack surfaces cannot be monitored and defended by humans; they require volumetric solutions that leverage the data lake in ways that create a territorialised sense of advantage over potential security threats. These observations have important ramifications for the political geography of territory, which has long been understood through the lens of extraction. Evident is the emergence of an alternative understanding that reveals ‘the arrangement of more than just surface land plots’ meaning that, with volume, the ‘repertoire of state technologies that work to measure the qualities of land in a multidimensional way has grown’ (McNeill, 2019, p. 849; after Elden, 2013; Amoore, 2018). Vicky explained the ramifications of this new territorial dynamic from a military perspective, sharing how “when you think about cyber-attacks, cyber-defence, there are really no geographical boundaries … it can come from anywhere, it doesn't need to be closest to you … [so] your defence lines have changed, your boundaries have changed”. Vicky went on to articulate an understanding of volume that goes beyond the size or quantity of data that is being produced and processed by the Smart Nation, but includes the “network and the logs in the network and what you need to process to defend the networks, it's also becoming voluminous”, in total contributing to the emergence of a “bottomless amount of data” that foregrounds the need to “automate by, for example, using data analytics to make predictions about whether an attacker has come into the network”. Automated defence is becoming a necessary response to the volumetric vulnerabilities of the smart city-state, contributing to a dialectical interplay between territorialising and clouding, and constant efforts by the state to assert the former process over the latter.

4.2. Geofencing and the territorial dialectics of the cloud

One of the biggest disruptions triggered by the shift to cloud computing has been the need to embed private sector owned and operated datastructures within public sector entities. This is especially true in the context of the smart city, where the provision of municipal services is becoming increasingly dependent on private sector players. Put differently, public decision-making becomes privately *mediated* public decision-making. Notwithstanding this shift, ‘very little attention, if any, has been paid to the infrastructural geographies that enable this shift of power from public to private entities’ (Fard, 2020, p. 4). Whilst our articulation of

“datastructures” might help to fill the lacuna, there remains a geographical problem that stems from the private-public interplay. This is a problem that is deeply territorial in nature. As Fard (2020: 4) explains, the fact that most of this infrastructural space is located ‘outside of the bounds of cities has established a conceptual blind spot which has undermined the scope of influence and the significance of these spaces in the creation of ideologies and … power dynamics’. Managing this shift has presented various problems to the Singapore government; problems not just related to technological sovereignty and control, but also those related to policy, organisational development, and instigating a cultural shift. Kok Ping Soon, the former CEO of GovTech – the branch of government responsible for implementing the Smart Nation – recalled how, initially,

the policy said that everything must be on-premise and so forth, and, of course, there are all these different dynamics and paradigms for how our systems are secured on the cloud, so we have got to go through a whole policy review and what comes out of it, essentially, is that we put in place … a commercial-first policy … We work with Amazon Web Services, Google, as well as Microsoft to set up a technical environment which we call the Government on Commercial Cloud that kind of provides a bit more protection, so to speak. We geofence with some data localisation to allow agencies to say, OK, this is safe to move our applications onto the cloud.

Whilst Ping Soon gestures here towards a symbiotic relationship with the private sector, the fact remains that private sector collaboration invariably clouds the territory, as evinced by the security concerns expressed by other government agencies. In response, the territorialising strategies of “geofencing” and “localising” data are deployed to appease concerns and strike a balance between territorialising and clouding. Territorialising is, in Ping Soon's words, a way to “internalise the risks involved” in partnering with private sector solutions providers. The territorialisation of data through geofencing and localisation can be seen as an attempt to centralise data management and security within the government, even if it remains inherently voluminous. Debates about data locality and data residence are not new, but they are implicitly more complicated in a context like that of Singapore. In the U.S., for example, the jurisdictional parameters of cloud computing are relatively easier to enforce because they have the size and critical mass needed to scale solutions. Hunter Neald, a Distinguished Engineer with GovTech, explained how, for smaller countries like Singapore, “we can't necessarily have dedicated environments for these things, we need to be able to work as a corporate would inside of these cloud service providers” and in doing so manage the challenges that come from “digital identity, sensors, and IoTs … which interact across all these platforms”. Increasingly, then, we can begin to see not just how ‘territorial power is enacted and contested through technical infrastructures’ (Munn, 2023b, p. 80; also Atkins, 2021; Glasze et al., 2023), but also that infrastructural – or datastructural – power is enacted through territory (Woods, 2022a, 2022b). Vicky explained the territorial dialectic that this gives rise to:

For big organisations, especially governments or even militaries, it’s attractive to move onto the cloud … But there comes with it some downsides that militaries and governments have to worry

about, especially if the cloud is not owned by you, or not located within your national territorial boundaries – if the cloud belongs to some other country … You worry if you will always have access to the cloud if you need it, especially when we're talking about the business of war. It's national security.

Compounding these risks is the fact that when it comes to cyber security products, "a lot of it is off-the-shelf, and actually a lot of the high-end things don't necessarily come from, don't always come from the military or the defence sector" (Vicky). As much as we can see the private domain impinging on the public domain, so too are security products designed for the civilian domain becoming viable solutions for military buyers. Arguably, these products are better designed to mitigate the risks associated with voluminous attack surfaces than their military counterparts. In response to this dynamic, Hoo Soo Pin, the Director of Digital and Corporate Transformation for MINDEF, shared how not only is Singapore developing its own commercial cloud, but so too is it investing in a digital factory. Whilst still in the pilot stages, the digital factory is designed to instil the "rapid product development methodology" within MINDEF, which will give it the capacity to "quickly develop products that meet needs" (Hoo Soo Pin). Koh Jin Hou, the Director of Digital Factory for DSTA, explained how the digital factory reveals how the military domain is driving technological innovation for the rest of the government. In his words:

We can perceive the whole MINDEF, SAF as an ecosystem making up various business domains such as our own logistics, HR, employee, etc., akin to a mini government. So, while the Smart Nation drives digitalisation through various industry transformation maps for the different sectors, it is similar in our situation to develop digital transformation roadmaps for our internal business domains.

These transformation roadmaps are integral to the development of the Smart Nation, as they enable the government – and the military in particular – to innovate quickly and independently of any private sector entity. As Soo Pin put it, "if MINDEF/SAF can leverage our digital factory rapidly to meet operational needs, I think that is something we can offer the smart city conversation on how to develop products that meet changing needs in a very rapid way". The need for rapid response is a priority for defence and military systems, and thus is incubated in the military domain before being extended out to the civilian domain. Soo Pin provided a tangible example of what is meant by this by recalling how, during the COVID-19 circuit breaker period, the development and use of data visualisation dashboards and digital tracking tools for the purposes of contact tracing reflect the fact that the "same kind of technological flexibility that we adopt for our warfighting systems can be applied to such digital products". It is through these applications from the military to the civilian domain that we can begin to appreciate how the volumetric vulnerabilities associated with cloud computing are leading to an expansion of the militarised conjunctures of everyday life in Singapore.

4.3. Expanding the militarised conjunctures of everyday life

The security challenges posed by the volumetric vulnerabilities of the cloud foreground the need to understand the expansion of the military domain into more walks of life. This need is pronounced in Singapore, as it being a city-*state* means that national-level and city-level security are often one and the same thing. Letchumanan Narayanan, a Commander in MINDEF's Imagery Support Group, shared how "we don't have anyone to compare with" before claiming that "if I look at the United States, the security layer is not there, the military does not operate there [in the city] often, it is just the police". Accordingly, MINDEF plays a bridging or *conjunctural* role that serves to "translate technologies and competencies that are used in traditional military domains for opportunities in the non-military domains" (Hoo Soo Pin). In the realm of cybersecurity, the military can be seen as a defensive platform that serves not only Singapore's military needs, but its domestic civilian needs as well. These 'conjunctural geographies' cause the military to become 'simultaneously embedded and disembedded from the space-times they mediate' (Graham, 2020, p. 453). Mah Chia Hui, an Associate Cybersecurity Specialist in GovTech, shared how many of MINDEF's projects are "national interest projects", whilst Vicky shared how her role in the Cyber Defence Group is to "provide 24/7 cyber defence of the Singapore Armed Forces networks, the war fighting networks" before going on to assert that "my unit is like an enabler for the Smart Nation, [which is] about improving the lives of Singaporeans by harnessing technology … The downside of being more reliant and intertwined with technology is that our lives become disrupted when the network becomes disrupted". Technological dependencies create militarised dependencies that lead to a degree of conceptual overlap, and indeed slipperiness, between the military and civilian domains.

These dependencies span both the human and technological realms. In terms of the human realm, Vicky shared how MINDEF's Incidence Response Teams would support the National Response Teams to manage cyber-attacks, but also to offer things like "cyber-threat intelligence, threat hunting capabilities for early warnings of potential cyber-attacks". In terms of the technological realm, the need to customise products to suit the Singapore context further exacerbates the sense of dependency. Soo Pin shared how MINDEF's digital products are "not so easily found off the shelf" and because of Singapore's relatively small size, "we can't develop everything on our own, we work with global partners to bring in technologies … we work with Amazon to have a commercial cloud, but we influence quite heavily the security aspects of that commercial cloud". Operating through the public and private sectors, and the military and civilian realms, both enhances the defensive capacity of the Smart Nation, but also, paradoxically, renders the city-state more vulnerable to attack. Letchumanan explained the situation clearly in his admission that "I protect the city like it is the nation" before going on to explain the interoperability of the defence and technology industries, and, specifically, how:

> we are also concerned about the security of our smart city systems. Our own infrastructure networks reside in Singapore, often running on the same fibre optic, physical or logistical infrastructure … Unlike other militaries [around the world] if the city goes down, I presume most

of their military service and data centres will probably be in some mountains somewhere. I'm afraid Singapore doesn't have that privilege.

The militarised conjunctures of Singapore are rooted in the shared infrastructure that supports the cloud. This shared infrastructure serves to territorialise the cloud, but at the same time it also serves to cloud the territory by increasing the attack surface of the city. Whilst scholarship has considered the extensive militarisation of urban environments around the world, it has not considered the infrastructural conjunctures that gives rise to militarisation, nor the paradox that increasing security capacity also serves to increase *in*security. Graham (2011: XI-XII) calls this the 'startling militarisation of civil society – the extension of military ideas of tracking, identification and targeting into the quotidian spaces and circulations of everyday life' which in turn 'represent dramatic attempts to translate longstanding military dreams of high-tech omniscience and rationality into the governance of urban civil society'. The spectre of threat is now omnipresent and remote. And, just as the emergence of the smart city has galvanised the "extensions" and "translations" that Graham (2011) evokes, so too does the militarised city-state of Singapore cause them to become acutely felt throughout civilian life. In this vein, Soo Pin referred to MINDEF as a "sleeping giant" that is needed to "awaken the people" as "MINDEF, when we want to put our mind to something, and when the entire ecosystem aligns, it goes all the way". The main challenge, according to him, is to recalibrate mindsets so that MINDEF is seen as a *peacetime* defensive organisation: "if you ask any average MINDEF/SAF employee today, they will tell you their raison d'être is in defence, but how do we then shift the person's motivation and recognition that what we do for defence is equally applicable to peacetime applications". Military defence is becoming interspersed with peacetime defence, creating seamless alignments and continuities between the two constructs.

Of course, this close relationship between the military and civilian domains has a long provenance in Singapore, and remains enshrined in the policy of National Service. What the Smart Nation and the datastructures of the cloud have done, however, is to further collapse the distinction between the two. Soo Pin shared how in his "dream world" when MINDEF employees and National Servicemen "move from a civilian space into a military infrastructure, a military camp, a military environment, their overall experience is seamless" to the point that "MINDEF/SAF wants to be levelled up and be in pace with the smart city, to the level at which we think we reduce the gap between our citizen army with their experience when they are with army". The "citizen army" that Soo Pin evokes extends to everyone – military employees and civilians alike – and reveals an exchangeability of people, ideas, constructs, and terms. Soo Pin referred to this as a "domain level transformation for National Service" into something that is not apart from civilian life, but even more tightly integrated with it. As he put it, "the uniqueness of a citizen armed forces would also imply what we do or do not do with our NS men impacts the people around, that work and live around them, their employers, their family … How do we use digitalisation to reach out to their family?" The everywhereness of the cloud can be seen to drive the everywhereness of the military. It encompasses new capabilities and opportunities for more

seamless urban life. But, in the same breath, it also creates new vulnerabilities and necessitates new forms of defensive oversight. The dialectic of territorialising the cloud and clouding the territory sits at the heart of these dynamics and determines the shape and extent of the militarised conjunctures of everyday life in Singapore.

5. Conclusions

As much as the cloud transcends the territorial demarcations of political power, so too does it serve to reproduce and thus complicate them in new, and often obfuscatory ways. The volumetric nature of cloud computing, and the datastructures it gives rise to, foreshadows the volumetric vulnerabilities that emerge because of cloud-based dependencies, as the language and praxis of volumes sit uneasily with the calculative logics of state rationality, surveillance and control. These dynamics find meaning and relevance in the contemporary smart city, where the intermeshing of private supply and public demand in and through the datastructure creates new co-dependencies, and with them, new forms of vulnerability, risk and resilience. With these assertions in mind, the contributions of this paper are twofold. One, it brings the study of infrastructure into productive conversation with the study of volumes, with data providing a connective interface between the infrastructural and the volumetric. Our notion of "datastructure" provides a conceptual framing through which the complexities of this interface can be advanced. Two, it has brought ideas and understandings of the smart city into conversation with militarised understandings of territory and territoriality, and has considered how the enveloping nature of cloud storage yields new axes of vulnerability and threat. By moving discourses concerning the securitisation of smart cities beyond the domain of surveillance and policing, we consider instead the existential threats that voluminous data can evoke. Accordingly, we have advanced an understanding of the smart city as a volumetric construct insofar as the datastructure that underpins it transcends the built environment, the material plane, and the bordering processes that attempt to demarcate politico-regulatory control. Doing so causes the logic of securitisation to stretch across new, digitally defined trajectories of political praxis, opportunity and risk.

Expanding some of the ideas raised in this paper, we contend that just as political geography has been slow to integrate the novelties afforded by new media technologies, computer and data science, and digital infrastructures into its theoretical constructs, so too can these domains reveal generative areas of theoretical expansion. There is a need for political geography to better align itself with the restructuring of the world along digital lines, to ask how attendant questions of data management, automation and prediction might be reshaping the (geo)political terrain of contemporary power structures, and to consider how these structures might be reconfigured along the territorial interstices of the material and more-than-material planes (see Woods, 2021). We have explored these reconfigurations through the heuristic of cloud storage and the data centres to which it is indexed, but so too do the domains of large language models, generative AI and augmented/virtual reality provide novel ways to advance the political imagination. Further, as much as these applications provide analytical subjects, so might they be usefully deployed as

methodological orientations that see us looking with, through and beyond the algorithm, for example, or the process of machine learning, or the production and deployment of synthetic data. Our point is that technological innovation often begets political innovation. Just as politico-regulatory stakeholders often scramble to keep pace with technological advancement, the same can be said for politically oriented theory-building. Whilst political geography has always had the interrogation of political technologies – whether of statecraft, territory and territoriality, or bordering – at its core, there is value in taking the idea and potential of technology more seriously if it is to keep pace with the ongoing digitalisation of the world.

Funding information

This work was supported by a Partnership Development Grant from the Social Sciences and Humanities Research Council of Canada ["Smart Cities in Global Comparative Perspective: Worlding and Provincializing Relationships"].

CRediT authorship contribution statement

Orlando Woods: Conceptualization, Formal analysis, Writing – original draft, Writing – review & editing. **Tim Bunnell:** Formal analysis, Funding acquisition, Investigation. **Lily Kong:** Formal analysis, Funding acquisition, Investigation.

Declaration of competing interest

The authors declare there are no competing interests to declare.

Acknowledgements

Thanks to Ivin Yeo for research support.

Data availability

Data will be made available on request.

References

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. Progress in Human Geography, 42(1), 4–24.

Atkins, E. (2021). Tracing the 'cloud': Emergent political geographies of global data centres. Political Geography, 86, 1–3.

Baur, A. (2023). European dreams of the cloud: Imagining innovation and political control. Geopolitics. https://doi.org/10.1080/14650045.2022.2151902

Bratton, B. (2016). The stack: On software and sovereignty. Cambridge, MA: MIT Press.

Bunnell, T., Muzaini, H., & Sidaway, J. (2006). Global city frontiers: Singapore's hinterland and the contested socio-political geographies of bintan, Indonesia. International Journal of Urban and Regional Research, 30(1), 3–22.

Connor, A., & McNeill, D. (2022). Geographies of the urban underground. Geography Compass. https://doi.org/10.1111/gec3.12601

Eiterjord, T. (2024). Securitise the volume: Epistemic territorialisation and the geopolitics of China's Arctic research. Territory, Politics, Governance, 12(1), 93–111.

Elden, S. (2013). Secure the volume: Vertical geopolitics and the depth of power. Political Geography, 34(34), 35–51.

Fard, A. (2020). Cloudy landscapes: On the extended geography of smart urbanism. Telematics and Informatics, 55, 1–11.

Furlong, K. (2021). Geographies of infrastructure II: Concrete, cloud and layered (in)visibilities. Progress in Human Geography, 45(1), 190–198.

Glasze, G., et al. (2023). Contested Spatialities of digital sovereignty. Geopolitics. https://doi.org/10.1080/14650045.2022.2050070

Goldstein, J. (2019). The volumetric political forest: Territory, Satellite fire mapping, and Indonesia's Burning Peatland. Antipode, 52(4), 1060–1082.

Graham, S. (2011). Cities under siege: The new military urbanism. London and New York: Verso.

Graham, S. (2016). Vertical: The city from satellites to Bunkers. London and New York: Verso.

Graham, M. (2020). Regulate, replicate, and resist – the conjunctural geographies of platform urbanism. Urban Geography, 41(3), 453–457.

Graham, S., & Hewitt, L. (2013). Getting off the ground: On the politics of urban verticality. Progress in Human Geography, 37(1), 72–92.

Jackman, A., & Squire, R. (2021). Forging volumetric methods. Area, 53, 492–500.

Kitchin, R., & Dodge, M. (2019). The (In)Security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of Urban Technology, 26(2), 47–65.

Kong, L., & Woods, O. (2018). The ideological alignment of smart urbanism in Singapore: Critical reflections on a political paradox. Urban Studies, 55(4), 679–701.

Laksmana, E. (2017). Threats and civil-military relations: Explaining Singapore's "trickle-down" military innovation. Defence & Security Analysis, 33(4), 347–365.

Lesutis, G. (2021). Infrastructural territorialisations: Mega-infrastructures and the (re) making of Kenya. Political Geography, 90, 1–11.

Linneman, T., & Turner, J. (2022). Three-dimensional policeman: Security, sovereignty and volumetric police power. Theoretical Criminology, 26(1), 23–39.

McNeill, D. (2019). Volumetric urbanism: The production and extraction of Singaporean territory. Environment and Planning A: Economy and Space, 51(4), 849–868.

McNeill, D. (2020). The volumetric city. Progress in Human Geography, 44(5), 815–831.

Munn, L. (2020). Staying at the edge of privacy: Edge computing and impersonal extraction. Media and Communication, 8(2), 270–279.

Munn, L. (2022). Twinned power: Formations of cloud-edge control. Information, Communication & Society, 25(7), 975–991.

Munn, L. (2023a). Technical territories: Data, subjects, and spaces in infrastructural Asia. Michigan: University of Michigan Press.

Munn, L. (2023b). Red territory: Forging infrastructural power. Territory, Politics, Governance, 11(1), 80–99.

Ng, R. (2018). Cloud computing in Singapore: key drivers and recommendations for a smart nation. Politics and Governance, 6(4), 39–47.

Pan, D. (2022). Storing data on the margins: Making state and infrastructure in southwest China. Information, Communication & Society, 25(16), 2412–2426.

Potzsch, H. (2021). Capturing clouds: imagin(in)g the materiality of digital networks. In J. Schimanski, & J. Nyman (Eds.), Border images, border narratives: The political Aesthetics of boundaries and crossings (pp. 65–82). Manchester: Manchester University Press.

Rasmussen, M., & Lund, C. (2018). Reconfiguring Frontier Spaces: The territorialization of resource control. World Development, 101, 388–399.

Rossiter, N. (2017). Imperial infrastructures and Asia beyond Asia: Data centres, state formation and the territoriality of logistical media. Fibreculture Journal, 29, 152–171.

Sayin, O., Hoyler, M., & Harrison, J. (2022). Doing comparative urbanism differently: Conjunctural cities and the stress-testing of urban theory. Urban Studies, 59(2), 263–280.

Shatkin, G. (2014). Reinterpreting the meaning of the ‘Singapore model’: State capitalism and urban planning. International Journal of Urban and Regional Research, 38(1), 116–137.

Starosielski, N. (2015). The undersea network. Durham, NC: Duke University Press.

Tan, A. (2011). Punching above its weight: Singapore's armed forces and its contribution to foreign policy. Defence Studies, 11(4), 672–697.

Walsh, S. (2007). The roar of the lion city: Ethnicity, gender, and culture in the Singapore armed forces. Armed Forces & Society, 33(2), 265–285.

Woods, O. (2021). Clashing cyphers, contagious content: The digital geopolitics of grime. Transactions of the Institute of British Geographers, 46(2), 464–477.

Woods, O. (2022a). A harbour in the country, a city in the sea: Infrastructural conduits, territorial inversions and the slippages of sovereignty in Sino-Sri Lankan development narratives. Political Geography, 92, 1–9.

Woods, O. (2022b). Infrastructure's (Supra)Sacralizing effects: Contesting littoral spaces of fishing, faith, and futurity along Sri Lanka's Western Coastline. Annals of the Association of American Geographers, 112(8), 2344–2359.

Woods, O., Bunnell, T., & Kong, L. (2023). The state-led platformisation of financial services: Frictionless ecosystems and an expansive logic of "smartness" in Singapore. Geoforum, 146, 1–9.

Woods, O., Bunnell, T., & Kong, L. (2024a). Insourcing the smart city: Assembling an ideo-technical ecosystem of talent, skills, and civic-mindedness in Singapore. Urban Geography, 45(5), 735–754.

Woods, O., Bunnell, T., & Kong, L. (2024b). Island platforms and the hyper- terrestrialisation of Singapore's smart city-state. Territory, Politics, Governance. https://doi.org/10.1080/21622671.2024.2317211

Zurita, M., & Munro, P. (2019). Voluminous territorialisation: Historical contestations over the Yucatan Peninsula's subterranean waterscape. Geoforum, 102, 38–47.