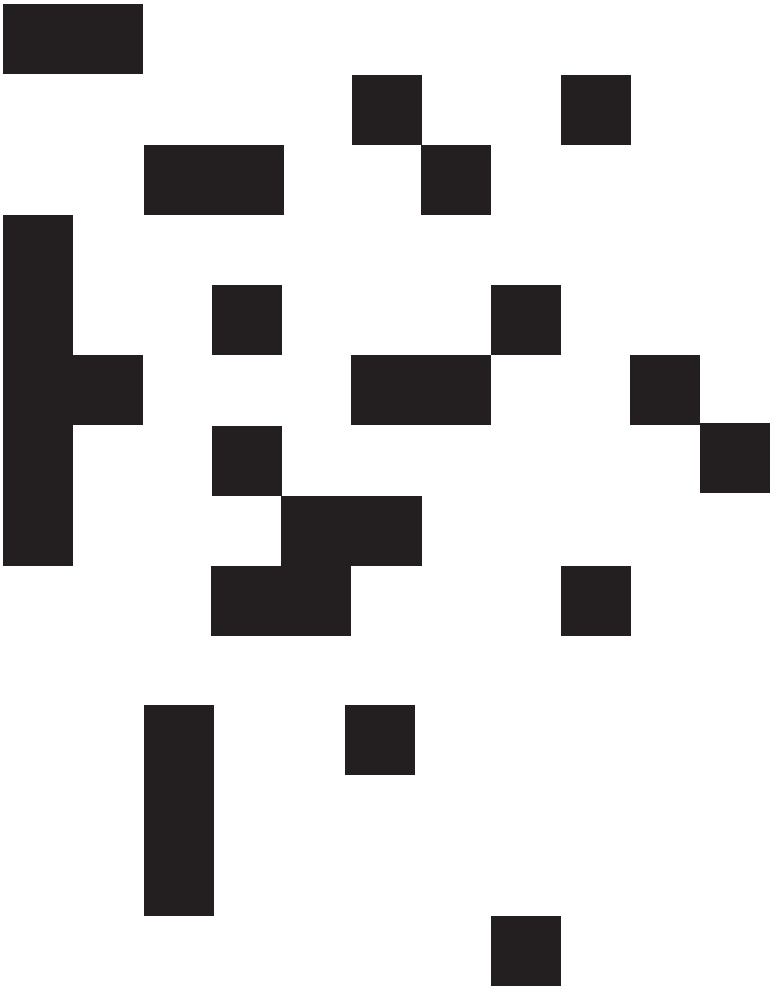
Data Farms
Circuits, Labour, Territory



Data Farms
Circuits, Labour, Territory

Low Latencies, Open Humanities Press

Contents

What is at stake in naming data centres as data farms? These installations are essentially hangars packed with computers. They congregate servers, switches and wires that facilitate the storage, processing and transmission of data in high volumes and at fast speeds. Data centres present a scale of operations, potentially planetary in scope, that intensifies and multiplies the productive and extractive capacities of digital technologies. They also trouble modern notions of national sovereignty as politico-juridical authority coextensive with geographical borders. Data sovereignty may be of the state or beyond its regulatory purview. Either way, there's a territorial logic of data transmission and communications infrastructure that frequently does not duplicate or overlap with national borders. Such variances are motivated in part by the business model of data centres. The economic advantages that accrue to parties with servers in these installations derive not only from opportunities for peering and networking within data centres but also from inputs to client machines that may be situated at vast distance. Yet data centres have precise locations, often clustering in sites where there is access to energy, skills, land concessions, tax exemptions or undersea cables. There are no data centres without land and water. Like the 'dark satanic mills' that William Blake associated with the factories of the industrial revolution, data centres also burn fossil fuels. Yet, despite these continuities with agrarian and industrial activity, the data economy generates stark figurations of territory, power and circulation.

The Data Farms research continues a trajectory begun with the Transit Labour and Logistical Worlds projects. Examining sites such as shipping ports, transport corridors, chokepoints and mineral extraction facilities, these prior projects highlighted the software dimensions of logistical systems that coordinate the passage of people and things around the world. Our concerns were with the implications of logistics for labour forces and the politics of infrastructure. An interest in data centres emerged directly from this research. Logistical techniques of tracking, tracing, coordination and calibration cannot proceed without the accumulation and analysis of data.

Not only do data centres provide the 'intelligence' that enables logistical operations, but they also tend to collocate with logistical facilities such as warehouses, container parks and transport terminals in urban fringes and peripheries. These continuities and connections propelled our decision to approach data centres as a primary research object.

Data Farms concerns itself with data centre clusters in Hong Kong, Singapore and Sydney. There are three sites of investigation. First is Tseung Kwan O in Hong Kong's Southeast New Territories. Built on reclaimed land in proximity to high-rise estates and a waste landfill, Tseung Kwan O's data centre cluster is one of the world's largest. The installations in this site act as switches between the mainland Chinese and global data environments. In Singapore, our focus is the Tanjong Kling Data Centre Park in the island's industrial Jurong district. Earmarked for data centre development with water and power on site, Tanjong Kling hosts facilities built by companies such as Facebook, Equinix and Telin (Telkom Indonesia). Finally, in Sydney, we concentrate on the inner-city suburb of Alexandria, where California-based company Equinix maintains a 'campus' of five data centres with direct fibre cross connect, point-to-point cable capabilities that ensure maximum low latency, indexing the optimization of speed in the struggle against time elapsed.

These sites of investigation are points of departure only. The Data Farms research quickly expanded to encompass not only other data centres in Hong Kong, Singapore and Sydney, but also installations in India and China. Our intention in choosing the three initial sites was to provide orbits of entry for a wider study of data centres in Asia, a region where the presence of these facilities is rapidly expanding. The compulsion was not merely to contrast the preponderance of data centre studies focusing on North America and Europe. By examining the intersection of the data economy with territorial and political relations and technical systems, we sought to track how data centre operations actively reshape the dynamics of regionalism. As such, we approached these installations not only as critical

infrastructures but also as political institutions through which relations of power are asserted and redefined. In this sense, the study was less about data centres in Asia than about how these facilities generate forms of territoriality and novel arrangements of power that call the locational specificity of Asia into question.

Data centres command a power to connect agencies and their economic interests across the territory of cities, nation-states and continents. As a region hosting an ever-growing number of data centres, Asia is positioning itself within a geopolitical and economic constellation endowed with a capacity to govern and control data economies and financial transactions beyond traditionally defined geographical and cultural limits. The interoperability between data transmissions and transactions occurs in tandem with technical specifications and information architectures related to Internet protocols, storage media, cable infrastructure, database systems and hardware design. Also relevant are commercial trade agreements and juridical frameworks specific to the regulatory regimes of nation-states.

When speaking of the territoriality of data centres, it is insufficient to invoke the idea of Asia as a discrete region or even as a complex geocultural formation that differs as much from itself as its others. The borders that comprise a regional space contained by cultural and political imaginaries along with various political-economic organisations and trade-driven agreements (e.g. ASEAN, SAPTA, FTAAP) do not map neatly on to the infrastructural space of data centres whose locations happen to be within Asia. Depending on operational requirements, contractual conditions and commercial interests, the provenance of data may be territorially distinct at sovereign, geopolitical levels from the location of its storage. More specifically, the Asia of data storage, transmission and processing consists in part of a string of facilities within cities and countries that, while geopolitically belonging to the Asian region, are spatially tied through political economy and protocological interoperability to similar installations distributed across the world.

If technological properties are ontologically prior to the state and corporation, questions of state formation and global economy can be approached from the perspective of infrastructural installations and their operations. But facilities such as data centres do not sit in isolation from the environments with which they are enmeshed. The territory of data centres includes not just the geography of cables, servers and clients that spans their operations; it might also be understood in a more diagrammatic sense as consisting of institutional and commercial elements or entities and their capacities brought into relation. Such a notion of territory suggests a more flexible comprehension of time and space that can be termed territoriality. The Data Farms research thus proceeds with the following hypothesis: territoriality consists of operational practices specific to infrastructural systems and technical devices, the effects of which produce territory as spatial arrangements and temporal dynamics that may parallel or conflict with state-based claims to control over the bounded space of the nation and its sovereign extensions.

The territory and territoriality of data centres are both enabled and defined by multiple spatial layers in conjunction with variable circuits of time. Part of the scalar dimension of data centres is not territorial in the geographic sense but is rather derived from amassing colossal amounts of data that enable the centralization of analytic and economic power. While there is design variation in how data centres are constructed from one site to the next, this doesn't mean that power doesn't concentrate. If climatic considerations linked to energy consumption were the only determining factor in deciding where to locate data centres, then countries like Iceland and Norway and not Hong Kong and Singapore would index the geopolitics of data. But data centres do not only distil power geopolitically. Data exchange coupled with standardization creates power through economies of scale and comparative advantage, leading firms to collocate within particular facilities. The best data centre to be in is the one where everyone else has decided to go.

The data centre as communications infrastructure extends from bricks-and-mortar of the building, the specific cabling, monitoring, security and fire safety mechanisms of its internal operations, the training regimes (e.g. Cisco networking certification) required of its human operators, the kinds of specific computing devices engineered to optimize rack space and save costs (e.g. 1RU servers), the 'hardened' software, operating systems (usually Linux or other UNIX variants), the software utilities used to monitor, route, load balance and optimize bandwidth and network traffic, the algorithms that ensure security, redundancy and optimization in the writing of data to disc – the list could go on. To enter one of these installations is to encounter a sterile and securitized environment. Server stacks sit in alternate hot and cold aisles to facilitate efficient heat expulsion. Although data centres are largely devoid of human bodies, flashing lights and humming fans register activity at the client end of network architectures that connect them to the outside world. Sure, some of this traffic is generated by remote sensing or other automated routines. But server load also indexes distant labour. Whenever a firm locates servers in a data centre or hires services from a cloud provider, its workforce begins to interact with machines whose location may be unknown to them. These arrangements create infrastructural, economic and relations between otherwise disconnected labour forces.

Patterns of territory and territoriality generated by data centres affect not only the extension of sovereign and governmental and logistical powers. They also create intersections between the circulation of data and the circulation of capital. The production of data as a commodity involves a massive reduction of turnover time with respect to earlier forms of commodity production and circulation. Data centres may become the ruins of the future, a probable outcome as the relentless push to centralize hardware holdings and dish out software 'as a service' begins to meet decentralizing tendencies such as edge computing. However, as installations of fixed capital, these facilities enjoy a relatively long lifespan with respect to the turnovers they support. The industrial

factory circulated capital through a protracted process of extracting value from labour, distributing commodities and closing the cycle by converting money into capital after sale. In the data centre, these transactions happen at lightning speed.

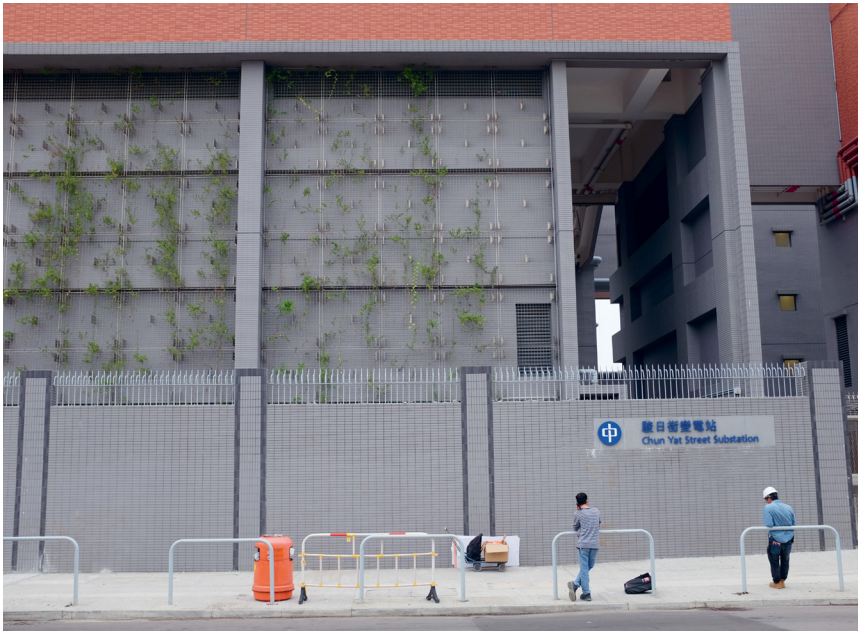
The static mass of data centres is lodged in dirt and concrete and seemingly without an object of acceleration required to meet Newton's second law of motion. There would seem, therefore, to be no obvious material force generated from their situation. Yet the speed with which data moves along cables extending from data centres across oceanic and continental territories relies, by contrast, on post-Newtonian and non-mechanical physics. Herein lies the paradoxical force of the situation of data centres: they are static in terms of infrastructural location, but at the operational level they are mobile in terms of the acceleration and transmission of data.

Bringing critical attention to the coupling of algorithmic capitalism with data centres instantiates a materiality that helps demystify the abstraction often associated with processes of capital accumulation. Such an approach pushes us beyond the concepts of chain, flow and network that have dominated recent studies of the global political economy. The chain metaphor does not register how relations of peering between firms in data centres create new forms of comparative advantage. The flow metaphor cannot account for packet switching technologies that transmit data in bursts rather than in constant streams. And the network metaphor cannot explain how the physical wiring of data centres generates distinct topologies that determine how different clients, users and labour forces interact (or don't) in digitalized environments.

There remains a series of questions about what sort of data traffics through different data centres distributed in strategic locations throughout the world. Are there juridical regimes specific to different types of data? How is the provenance of data complicated in legal ways by the location of its storage? What sort of protocols of hardware and storage are required for, say, financial data as distinct from the data collected by the state or

military apparatus, or produced in social media worlds? And to what extent do the technical operations, geography of location and political economy specific to different data centres determine the types of businesses and organizational practices dependent on hosting services?

The Data Farms research embraces these questions with a critical focus on Asia as the site of expanding data centre operations. Our curiosity is not simply with how data storage, processing and transmission extend the bounds of Asia beyond Asia or the dynamics of globality and mutations of capital that accompany this extension and its inevitable contraction back into particular geographically located facilities. We mine the capacities of data centres for concepts that index how their potentially planetary reach crosses their miring in material conditions of land degradation, thermodynamic excess and hydrological cycle disruption. The question concerning infrastructure thus becomes not simply how it works. More pointedly, it emerges as a question about how life – certainly nonhuman life but also even the most privileged human life – becomes secondary to making things work.



Images (above and opposite) Ned Rossiter

Historically the warehouse functioned to contain habit. Be it routines of work associated with the packing of goods or the use of ledger books to keep track of inventory, the warehouse operated as a storage and processing technology making habit accountable. More recently, the architectural form of the warehouse has been repurposed within digital economies as data centres. Otherwise known as server farms, and often referred to as 'the cloud', these facilities extend the warehousing functions of storage and processing to include the transmission of data. These two primary typologies – of the warehouse as storage and processing facility, and the warehouse as digital infrastructure for the circulation of data – are respectively marked by habits of labour and habits of data. The operational systems in contemporary warehousing cannot be made actionable in the absence of technical topologies that decide how habit is known and governed according to strictly calibrated routines of nesting, stacking and distribution. These technical and computational operations increasingly take place within data centres, which offer software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and, more recently, AI-as-a-service (AIaaS) to business, government and cultural sectors. While the technical destabilizes the sovereign authority of human actors, it nonetheless submits to the operational requirements specific to institutional agendas, geopolitical struggles and political economic interests.

How does the ubiquity of computational regimes, the calibration of subjectivity and routines of organizational culture standardize habit within warehouse settings? What is the traffic in data between warehouses and data centres, and what sort of tensions prevail between systems of management, operational routines and labour practices in these two separate but intersecting settings? What political, economic and social implications arise in the historical shift from what Stefano Harney terms 'statistical populations to logistical populations', and how does this bear upon the habits of labour and the computational processes of data? These background questions orient and motivate the inquiry set out in this essay.

Our focus is on how the *habits of data* – that is the routine and repeatable processes through which digital data circulates within and across logistical operations – connect with and shape the habits of labour in warehouse settings. Habits understood in this way mediate the movement of goods from warehouse to supermarket, calibrating the rhythms of working lives in cities integrated with computational systems. The habits of labour and the externality of contingency also bear upon the habits of data, with disruption to supply chains and deviation within workplace settings prompting a reconfiguration of software architectures to maintain the functionality of databases and enterprise resource planning (ERP) systems. Finally, computational processes and procedures internal to the functioning of data centres act upon data in ways that lend them a habitual propensity that loops back into how labour becomes increasingly indistinguishable from the operation of machines, giving rise to a politics of parameters.

Techniques of Measure

Within warehouses, the classification and retrieval of goods produce a spatialization of practice that constitutes a typology of knowledge predicated on logics of collecting, ordering and governing that is shared with the anthropological and social setting of the museum. The warehouse parts company with the museum insofar as the collection and ordering of objects is motivated not by an impulse to acquire knowledge of the habits, practices and beliefs of cultures and societies, but rather to dispense with the commodity object in a targeted, just-in-time fashion in order to replenish catalogues and remake inventories that scale with consumer markets. At the same time, knowledge practices become inseparable from routines of circulation and turn-over motivated by the demand for increased economic efficiencies. Voice directed order picking technologies have been incorporated, for example, within warehouses such as Walmart in the US, Asda in the UK and Woolworths in Australia 'to maximize speed and minimize error in production and distribution' (Kanngieser). The real-time governance of labour regimes

in these facilities are distinct from Taylorist practices of the assembly line in factory settings. The logistical technique of tracking and tracing the movement of bodies and commodities within warehouses is designed to extract maximum value from habits of work and classificatory knowledge that determines the location of things. The data centre provides the computational architecture that manages inventory and work practices of the warehouse. Encompassing logging, billing, visualization, data authentication, predictive analytics, business intelligence, search, conversion, publication and backup, the software services of the data centre establish the parameters of habit within the warehouse.

Time-and-motion studies forecast the organization of work habits beyond sites of manual labour in late capitalism. Referencing the growing disparity in incomes between executives and managers and all other roles since the mid-twentieth century, Gérard Duménil and Dominique Lévy's coinage and analysis of 'managerial capitalism' suggests that the precision management techniques of Taylorism never disappeared but were rather subsumed in later eras into cognitive capitalism, immaterial labour, contract manufacturing and the sharing economy of platform capitalism. Rather than through direct oversight, cameras, sensors, inventories, computer logins, trackable RFIDs and wearable devices produce the disciplining regime that ensures, within ever decreasing margins of error, compliance within a virtualized warehouse that has externalized its own functions of containerization and securitization across entire supply chains. Moreover, the machinic vision of the state is amplified and outsourced within and complicated by the optics of digital facilities such as data centres that capture, store, process and analyse the routine activities of citizens and non-citizens alike as they traverse differential zones and spaces of inclusion and exclusion. The platform governance of this form of sovereign power both of and beyond the state registers simultaneously 'the maximal state and the minimal state [which] convene and even converge' (Bratton).

State-centred concepts of sovereign power are less suited as analytical devices to explain the force

of capital as sovereign. Moreover, a notion of sovereign power derived from technical operations, media of communication and infrastructural facilities such as data centres imbues authority and decision-making with significantly different characteristics and tendencies. Notions such as sovereign media or infrastructural imperialism register the power of technical systems to command authority and make decisions in ways that produce new spatialities and temporalities external to how space and time are typically understood in disciplines such as international relations and area studies, which weld geopolitics to civilizational cultures in Cold War imaginaries of inter-state contests. When sovereign power is decoupled from the state, the conceptualization of habit is similarly liberated from the everyday routines of human subjects. Instead, the habits of machines and data can be identified as asserting a sovereign command of how the everyday is experienced. Needless to say, the everyday shares with contingency a disruptive potential that unsettles totalizing systems of power. Recasting concepts of power in ways alive to contingency also broadens the sort of typologies we can attribute to habit.

Platform Operations

The architecture of platform firms like Amazon illustrates how habit re-forms into a modular warehousing arrangement, operating both vertically and horizontally. Its warehouses are models of efficient labour extraction and exploitation. Less recognized in critical studies of labour, its data centres, operating under the brand of Amazon Web Services (AWS), are the largest and most successful cloud computing operation in the world. They generate twice the revenue of its nearest competitor (Microsoft) and most of the company's gross profit, responsible for Amazon's explosive capital growth over the past decade. Amazon's Prime account model is subscribed to by more than 100 million US customers. Amazon Mechanical Turk (AMT) – an Amazon cloud computing service that contributes little to its bottom line – has nonetheless been widely studied as an exemplar of micro-work. AMT's stratified selling plans are offered

as fee-for-service, with the 'professional' plan a virtual prerequisite for selling any meaningful volume.

Amazon's world of e-commerce expanded in the 2000s to other commodities, with similar consumer virtues. The release of Amazon Prime in the US market in 2005, which was later extended to other countries, removed all shipping costs, guaranteed delivery within two days and included subscriptions to Amazon's growing catalogue of music, video, book and gaming content. Coordinating its own warehouse operations from inventory picking to household delivery, since 2006 AWS has also operated as a centre for many of the world's most intensive data services. After its own data centre was burned down in a fire in 2010, video streaming service Netflix began to outsource its data hosting to AWS. Alone, it is responsible for 15 per cent of global Internet traffic. Other customers include Fortune 500 companies (Kellogg's, Siemens), leading tech companies (Dropbox, Spotify) and more than 1 million additional paying customers. With the launch of facilities in Cape Town in April 2020 to compete with Microsoft's Azure and Huawei's cloud services, the physical locations of AWS data centres now cover every continent outside of Antarctica. In hindsight, Amazon's rise appears with all the inevitability of every technology success story.

AWS's injunction to 'just sign up and start working' acknowledges the commoditization of the data centre, and a corresponding shift in the habits of IT storage procurement. Since then, the term 'elastic computing' has become a principle of flexibilized computing resources as well as an Amazon brand. Less feted are Amazon's exploitative labour practices that subjugate workplace performance through calibration machines. Compared with other Silicon Valley leaders, even for its white-collar engineering workforce conditions are described in a 2015 *The New York Times* expose by Jodi Kantor and David Steitfeld as 'tough', 'punishing' and committed to 'purposeful Darwinism' typified by practices of 'stack ranking' – routine evaluations that score employees into categories, and eliminate those in the lowest quartile or decile. The same report attributed much of these cultural

conditions to CEO Jeff Bezos's 'data-driven management', and more recent reports suggest that conditions have not improved since, with stack ranking still common.

Metrics extend from its data centres and knowledge workers throughout the web of connectivity and influence managed by Amazon. High volume inventory items are prioritized in the online store; high velocity and quality Mechanical Turk workers ('Turkers') are rewarded with reputational scores that lead to future work; high volume sellers are guaranteed lower monthly fees and greater functionality; and, until recently, high productivity warehouse workers received incentive targets designed to maximize outputs. In the latter case, Amazon's response to a Bernie Sanders'-led campaign for a minimum hourly wage of US$15 has been largely seen as a success for workers' rights, but, as US Amazon workers themselves noted, for many wages will actually decrease as a result of these changes.

What distinguishes the platform corporation from earlier modes of mass capitalism – symbolized at various times by the East India Company, Ford, General Electric, IBM or Walmart – is precisely the cultivation of a multiplicity of disjointed but rigorously coordinated global habit regimes that stretch from the home office (the site of consumer data generation and Mechanical Turk labour) to the warehouse and data centre. 'Amazon', 'Facebook' and 'Google' become, under our schematization, platform-fields, equivalent in their social determining force to education, military, culture, family and so on. This prompts further conceptual rethinking with regard to how institutional forms are understood within digital, networked media and associated organizational practices. Such rethinking becomes only more critical as these platforms rival the authority of knowledge hitherto experienced by the social sciences. Facebook's continuous archiving of the varied likes, tastes and habits of half the planet's population make the academic survey, compiled through expensive grant applications, ethics procedures and beseeching requests made of a hopefully representative sample, appeared to be an exercise in epistemological wishful thinking. The 'royal road' of any social data science

career is increasingly from academia to the heart of platform analytics, assuming that a working life is not first catapulted into the ditch of obsolescent skill sets. This arrangement is not, as would be case for the statistical sociologist, a description but becomes instead, in the hands of the platform engineer, a blueprint and design.

Robots Dream of Nothing

Within a computational paradigm the managerial predilection to authorize change is usurped by media of decision. Robotic process automation (RPA) functions as a curious new intervention in the habitual relationship between machine and human in the warehouse and office. Despite what the name implies, RPA projects appear to be less motivated by the transfer of control from human to machine than an institutional accommodation of existing technical situations. In many cases, RPA is used to automate routine human actions with other, often legacy machines, when an upgrade or replacement of those machines is too costly or complex. We could think here of the intractable place occupied by mainframes in the finance sector, still resident within banking data centres and yet whose design and operation inspired the HAL, the antagonist of *2001: A Space Odyssey* more than half a century ago. Institutionally, even or especially in IT, old habits die hard. Within these situations, RPA involves software 'bots' filling in electronic forms, using scripted versions of operating procedures that a human workforce would otherwise follow. These new bots must contend, without complaint, with the awkwardness of bygone usability paradigms, just as humans would. Their behaviour is gestural, habitual and seemingly distinct, inasmuch as their attributes of presence and performance constitute their status as an proprietary object. These bots are designed to move a mouse across windows, tab between fields, respond to strange error codes, and wait for the resident system to respond after hitting the 'Enter' key. Here, machinic organizational decisionism is inscribed less through executive order, and rather by the further reduction of mundane bureaucratic operations to the logic of fault-tolerant probabilistic decision trees.

Yet the status of RPA bots as property is ambiguous. At the level of gesture, the machine replicates the on-screen routines of how a human might interface with software. Similarly, as the human worker or consumer orients their gestural activity in ways bound to the coordinates of the machine, the concept of property is rendered problematic. The human, which for Vilém Flusser encompasses both capitalist and proletarian, becomes 'the property of machine'. The functioning machine allocates a function for the human. This cybernetic redistribution of decision-making shifts leadership roles in ways that reach beyond the executive layer of organizations. The proliferation of decisions in banking and logistics registers how leadership and labour mutually enmesh with 'time-critical media' (Ernst). Able to measure, format and calculate the temporal axis of decision-making, time-critical media of decision such as RPA produce a mode of power specific to automated technologies enlisted in the governance of workplaces and provision of services. A central consequence of time-critical media involves the reorganization of space, which includes facilities such as warehouses.

Once the site of a specific function of capital – storage of goods that awaited maximum realization of profit – the warehouse now extends its logic throughout supply chains and into the lives of all those who, wittingly or otherwise, contribute their labour to the rise of the platform. So too, as the example of RPA shows, for the office. For consumers and labourers, there remains some minimal selectivity as to one's platform or rather poison of choice. Yet regardless of specific configuration, with the maturation of platform capitalism the containerization of habit is well underway. Resistance is less a case of subverting or avoiding platform co-optation, and more one of acknowledging its effects and organizing alternative arrangements. Habits do indeed often need to be broken.

A longer version of this text was published in Tony Bennett, Gay Hawkins and Greg Noble (eds), *Assembling and Governing Habits* (Routledge, 2021).

Image (opposite) Ned Rossiter

Images (above and opposite) Ned Rossiter

What happens when researchers experimenting with custom networking software in the digital medium have no choice but to conform to the existing laws and regulations applicable within the national jurisdiction of each of their cultural partners?

As one would expect this works against the singular, global, monolingual Internet that acts as a homogenizing technology, persistently eradicating difference. Effective digital literacy practices depend more on bottom-up processes than on top-down policy initiatives. These issues play a major role in the progression of the humanities in the Singaporean context and beyond. Meanwhile techno-capitalist-dominions have default standards that relentlessly control, define and control how Internet users connect and thus influence social imaginaries of what the Internet is, was and could be.

The bio-socio-cultural implications for Internet and online communities in the Asia Pacific are complex. Infrastructure is intimately tied to the data centres which host the platforms of networked activity. Singapore hosts over fifty percent of the servers in South East Asia. Participation, power, agonism, agency and social issues aside, the total amount of digital data several years ago surpassed the total amount of printed data, and it has been accumulating since then at an exponential rate. This confronts society with a new problem – the long-term storage not to mention archiving of important digital materials with their mutual ecological footprints.

Server stacks assemble in sealed off cryogenic cooling chambers. Data centres are currently locked down realms, menacing high security authoritarian compounds. Data centres tend to cluster in particular territorial environments, often based on the presence of infrastructural conduits that date back to previous episodes of imperial expansion – for example, the cable connections established by the British in the late nineteenth century. These reticent facts are mirrored by use limitations prescribed by governmental requirements for content that engages with the public sphere. A regulatory framework introduced in 2014 states that online content providers must apply for a license (renewed

on a yearly basis) if they 'report an average of at least one article per week on Singapore news and current affairs over a period of two months, and are visited by at least 50,000 unique IP addresses from Singapore each month over the same period of two months' (Infocomm and Media Development Authority).

Some people make the case that 'Singapore has one of the freest internets in Southeast Asia and is liberal compared to China, with a score of 87/100' (Freedom House). But this fact cannot be perceived in isolation from the experience of living on the ground. Adding to the convolution of the vernacular and the institutional, and the local and global, it is necessary to consider the challenge put by the omnipotence of Singapore's black boxed data centres and the government's Smart Nation initiative.

An open data sharing site was created where anyone can access datasets made available by the Singaporean government. Launched in 2011, Data.gov.sg creates a free and open data portal that makes relevant and understandable government data public. The datasets presented in this website are limited and can hardly be utilized in a particularly useful way by average citizens. The heterogeneity of this open data hinders meaningful analysis and search, which leads to a limitation on the transparency level. Unlike for instance, Wikipedia's open history, the so-called open data sharing site only provides datasets summarized into visual graphs rather than the raw data that the name offers forth.

Considering the democratization of knowledge together with infrastructure is a task for those who want to break out of the black box, customize artisanal code and mod their computer away from inbuilt consumer control paradigms. On the ground in Singapore, the presentation of radical experimental art or even just the materialist informatics of postdigital cultural projects that deploy the Internet (not even remotely critically) is often fraught. When it comes to potential deployments of the postcolonial archive in postdigital culture, legal frameworks remain local.

Now the postcolonial archive has been expanded, its tendrils reach into the cauldrons of the

feminist Internet – a quintessence that intends to corrupt monolithic server stacks in data centres where they physically reside and contain the processors that emit noxious vapours and steam heat.

An antidote to this is the feminist server – it is engaged, autonomous, it supports and enables the community it was created by and for. It is a site of possibility where ethical, political and intersectional agonism manifests. In the bedlam of poetic computation, a need for consistency arises. This tension between thinking and doing, between reflecting and acting, brings together the concept of the feminist server stack. The consciousness raising inherent in these questions is the beginning of their answering: the Internet must claim a new autonomy, notwithstanding access and even self-determined management of the web server where data is stored.

When attempting to deploy projects that implement the Internet in a critical, poetic and fictional way, problematic issues invariably surface for transdisciplinary research and knowledge production. A feminist server is 'feminist' because, first, it acknowledges imperialist sovereignty issues around technological power relations. Second, its intention is to provide services for its community by countering the current system administration habitus. The feminist server stack supports actants by foregrounding the deeply intertwined relationship between twenty-first century artistic methodologies and feminist server technology. It reflects upon the evanescent condition of networks and our embodied processes that administer and act in relation to cultural processes of computation. Bonds of trust and reciprocal efforts are needed to maintain the server, remain engaged and inspired, and to contribute to the necessity for continual maintenance.

In broad terms, this undertaking addresses the need for an expanded digital practice that reaches beyond the problem of how to preserve ephemeral cultural heritage. The modes of performance computational media enable, through which living beings participate and interact, make necessary the implementation of

frameworks for bottom up digital culture that shapes *in situ* digital literacy. This approach to knowledge encourages the user to be a content producer instead of content consumer. It involves a reflexive ethos that encourages continual questioning of established responses and behaviours to digital media production and reception. The feminist server stack fosters a radically subjective and experiential approach to the cultural production of software poetic code.

At stake is the circumvention of traditional top-down authoritarian methods of assigning value and organizing digital knowledge production. The feminist server stack also departs from rote learning skill acquisition that advocates home-brewed methods for collective gain (think of self-organized digital literacy circles, readings of computational poetry that can also write and run). An interdisciplinary approach to computer literacy acknowledges vaster insights into digital infrastructure that lead to radical innovations that are more holistic, cutting-edge and potentially meaningful to all whom participate in performing the Internet. By encouraging software literacy through modes of experiential pedagogy, an alternative body of empirical knowledge can contribute to rewrite Internet sovereignty out of its current totalitarian emergence. The cashless society advocated in Singapore's Smart Nation policy should 'move away from identity politics and moral policing, and formulate much more radical programs such as education, fair trade, and ultimately a global redistribution of wealth (which goes way further than the demand for compensation)' (Lovink).

The obstacles one encounters when attempting such a project – for instance, simply user testing the Internet infrastructure as an art medium in Singapore with the cooperation of all stakeholders and from the three tiers of government – hinder the ability for researchers to fully understand their apparatuses. Further, to experientially learn is to be able to understand how to technically posit possible revisions away from the current techno deterministic destiny, 'the spread of a social credit system and its associated sensors, QR codes, and other trace-reading tools can create new security concerns

separate from those it allegedly aims to reduce through near-ubiquitous monitoring of behavior' (Ahmed). The feminist server approach not only critically identifies these malefic conditions, but also envisions a more hopeful future trajectory of an alternative, conceivably more autonomous version of the Internet and a less utilitarian understanding of what it means to be a human or an intermediary (such as a webserver) for that matter.

Holistic development of a user-centred, participatory approach to the codesign of networking systems can be facilitated by having access to the inner workings of the devices that collaborate with infrastructures. These features mean that the expanded postcolonial archive has the potential to greatly advance our thinking about how we experience a repository of knowledge. The digital infrastructures supporting today's ubiquitous computing are inherently messy, heterogeneous and locally shaped by power relations. Overhauling the current role of the automated data centre means highlighting the need to look differently at how such repositories of knowledge and research may be shared, assessed, stored or archived. This underscores our ability to rethink the mechanism – to be able to partially control and rewrite (or at least understand how to *tune in*) the technology that runs the Internet.

The analytical term feminist server stack posits a locus for understanding how computational technologies not only reveal new insights about the materiality of postdigital culture but also transform propensities for embodied contemplation. Examining the reach of ubiquitous computing into our daily lives and the impact of networked computation has upon the planet, the visceral quality of computational media influences our very habitus – our desires and fears, concerns, and prejudices. By introducing experiential methods such as the feminist server stack to imagine new possibilities, it is possible to present models for promoting a discussion of software pedagogy and the postdigital cultures situated in the Asia Pacific region.

Examining how the themes of large-scale data aggregation are problematized, in and through performing

arts and twenty-first century art forms of the postdigital, reveals a need for a multiplicity of Internet cultures and of diverse Internets and communities. Beyond the elite language of computer subculture *1337/ leet sp33k* and the endless torrent of memes, a feminist server stack opens pathways to reconfigure these mechanisms, just as a choreographer exploits their ability to arrange ephemeral systems into a meaningful dance of composites. Advocating for feminist server stacks means highlighting the significance of subtlety, nuance, conflicting gestures, positions and paradox as frameworks and resources for a broad range of projects across critical analyses, postdigital performance and network cultures. This approach allows a reconsideration of the Internet as a potential place of vast autonomy and self-determination – and not a place of mercantile, malicious ubiquitous surveillance.

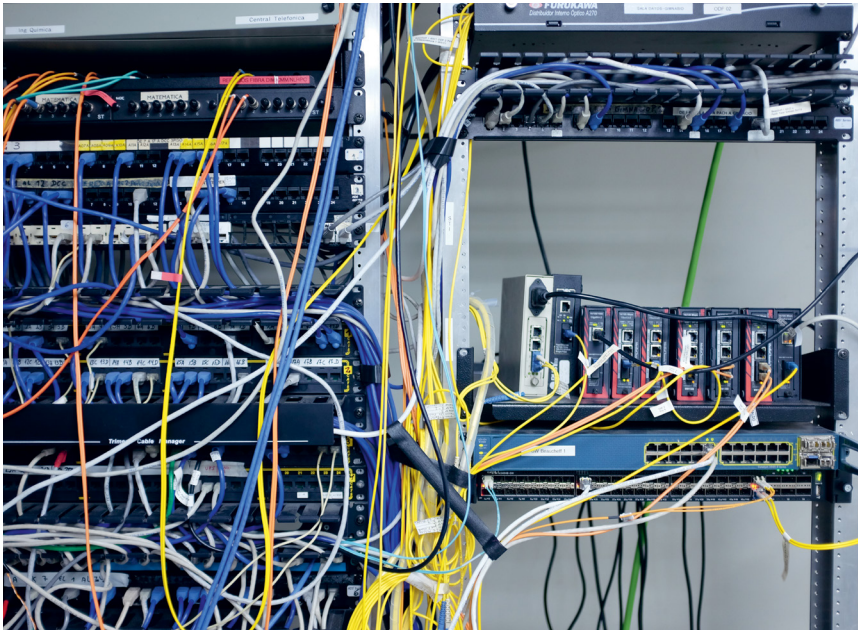
Censorship is one of the greatest challenges facing the Internet today. The feminist server stack challenges official modes of knowledge production and dissemination over the Internet sanctioned by state and commercial interests. Governed by the new 'merchant academic', digital media pedagogy is a field rife with cultural and social markers of exclusion (and belonging) dominated by techno capitalist hegemony. There is need for crucial didactic reforms in software literacy along with validation of the role of feminist server stacks that presently operate mainly under the radar of official culture. Through the formidable and eery nocturnal apparitions of *Penanggal* (Malay), *Ma lai* (Vietnamese), *Pontianak* (Singapore), and the *Kuntilanak* (Indonesia) – bio-political-techno-cultural devices – the postcolonial archive can be reimagined as postdigital and hosted on a feminist server.

The feminist server stack is inhabited by computers, cyphers and enigmas that both embody and resist the dynamics of dominant authoritarian structures in a deceptive dance of energetic elemental forces. In this crucible of equivocal visceral putrefaction, we can find all sorts of veracity. Banshees of the female spirit sisterhood may manifest: the *Krasue* (Thai), *Ahp* (Khmer), *Penanggal* (Malaysia), *Kasu* (Lao), *Kuyang* (Indonesia), *Manananggal*

(Philippines) with their entrails and alien viscera glowing for the community to read in order to predict and scry more promising and situated futures.

Coming into entrainment, being co-present with the materiality of the apparatuses is to be tacitly aware of the metal alloys and the energetic properties of the elements that comprise the computational networks of the Internet. To behold and even consider the distant possibility of a feminist-led data centre is to offer fresh insights into the prescriptive and top-down approaches of Internet Service Providers. It is also to rejuvenate more salutary relationships between meaning, politics and desire. No longer seeing the names of disciplines divided one from another as categories, projects become intertextual and fundamentally transdisciplinary, belonging to several categories at the same time. By encouraging alternative ways of performing with the materialities of the network beyond consumer-driven affordances and archival teleology, these efforts accentuate our ability to reconsider the mechanism – to be able to codesign, to read and rewrite (or at least tacitly understand) the signalling processes of software that runs the Internet. We live our lives and make meaning through building visceral networks of solidarity with intermediaries: minerals, lifeforms, humans and non-humans alike.

Images (above and opposite) Ned Rossiter


Central Telefonica
MATEMATICA
FURUKAWA

At the end of a two hour-long tour through the bowels of their brand new 'server hotel' near Basel, Switzerland, the CEO brought us back to the meeting room and signalled that he would now take questions. Our colleague raised his hand and asked, jokingly, if they were afraid that some of us would break in at night, now that we know everything about the myriad security mechanisms that the company had installed. 'We're actually not afraid that someone would break into the physical building', the CEO replied, 'the problem is that we are promiscuously connected'.

'Promiscuous connectivity' sits at the heart of the planetary-scale infrastructure that so many data centres now form part of – the cloud. Whether the servers in a data centre carry highly sensitive data of financial transactions or publicly accessible collections of holiday photos, they depend on promiscuous connectivity to guarantee continual and remote accessibility. A bit like a multinational corporation, the cloud 'offers a vision of globalization' – 'a coalition of geographic areas that move capital and resources through the most efficient path' (Hu). The cloud seemingly hovers in between or above its physical infrastructure – a pledge of ubiquity and infinity. As a global political operation, it emphasizes redundancy and infrastructural detachment, or the general expendability of its infrastructural elements.

In a piece titled 'Could We Blow Up the Internet', Tim Maughan comes to the conclusion that a cyber-attack is much more effective in terms of potential collateral and cost than any imaginable attack on the physical infrastructure of the cloud. If we believe the CEO of the aforementioned server hotel, this threat applies to any kind of data centre that provides remote access to data and computing capacities. However, a quick search reveals that cloud infrastructure facilities are typically replete with perimeter fences, security guards, surveillance technologies, biometric readers and reinforced steel cages designed to keep out any unauthorized personnel. In a video presentation about Google's data centres, a top executive describes the various levels of physical security that someone trying to get into the centre would have to

pass through. The rooms housing the actual server racks are akin to a sanctum sanctorum. Only those with the highest security clearance proceed all the way through.

Despite the fact that promiscuous connectivity is the most disquieting liability of data centres, their physical fortification proceeds unabatedly. As the only visible element of a system that 'buries or hides its physical location by design' (Maughan), the data centre as 'thing' provides singular opportunities to market the resilience of the system as a whole.

It is this moment of Gestalt thinking, when figure and ground simultaneously merge and separate, that it becomes difficult to know what exactly we are encountering – the whole, or something slightly more than the sum of its parts? How do we study and make sense of the apparent contradiction in that the data centre is an expendable infrastructural element, but that its significance ties to the infrastructural *promise* it exemplifies, a promise of resilience that applies to the system as a whole?

In this text, we assess the relationship between data centres and the cloud through the methodological device of the cosmogram: 'a text that results in a concrete practice and set of objects, which weave together a complete inventory or map of the world' (Tresch). Writing, art and investigations tell of pre-histories of data farms and cloud infrastructures through the lives of older media (Hu, Peters); by identifying their material components (Burrington, Starosielski); their ability to reshape notions of sovereignty (Amoore, Bridle); and through new figurations of knowledge in terms of spatiality (Bratton). In these accounts, the boundaries between the encompassing system – the cloud – and its constituting elements – i.e., the data centre – tend to blur in favour of systemic logics. Cosmograms present a vision of the relation between part and whole. They draw inspiration from ancient temple architecture, which strives to represent the cosmos by laying out and reinforcing the relations between humans and other beings. As such, they register how science and technology bring into the world not only facts and

artefacts but also narratives, structures and feelings. Cosmograms are as much performative and reflexive as they are representative and classificatory. In other words, they intervene in the world and provoke questions about their own status, limits and qualifications.

In thinking with and through cosmograms, we want to suggest a fork emerging from the study of the cloud in terms of the material components that operationalize it – undersea cables, servers, security, storage and so on. If this material assembly shows us how things are *actually* materially architected (and thus supports the infrastructural promise of the cloud), 'cosmogram thinking' allows us to appreciate the uncertain 'cultural choreographies' at play, the 'contestations, additions, deletions and replacements' (Tresch) that disturb the holism proposed by our internal maps of how the cosmos is architected.

The primary infrastructural promise of the data centre is that it will provide jobs to wherever data centres come to be housed. When Facebook opened its third data centre in Luleå, Sweden, its mayor was happy that the land and affordability of energy could allow the data centre to 'grow'. But he was most enthusiastic about the jobs that would come to the region, even if he was not very sure what they would be or what people would do.

Unfortunately, this rather classic infrastructural promise rarely materializes. Large-scale data centre facilities tend to remain' in-between spaces' (Johnson), built in accordance with the principles of global logistics, yet managed as an agglomeration of machines, including the now infamous human-exclusion zones. When viewed through the daily work of a data centre manager or technician – persons with little executive power, but with security clearance to inhabit the inner chambers of a data centre – an alternative microcosm of the cloud takes shape.

Advertisements for data centre jobs tend to emphasize the need not only for management skills and technical know-how but also physical endurance. An Amazon data centre technician role 'has a physical component requiring the ability to lift & rack equipment

up to 40lbs; it may require working in cramped spaces or elevated locations, dominated by an incessant, noisy hum that tend to ridicule the adhering to health & safety guidelines'. On a Quora thread about working at a data centre, 'George Henry' asks: 'Can you work in an environment where you have spoken to not one other person for 8 hours?' And he notes that while it is not as good as working 'at corporate', still, 'you are lucky to get a desk. As the team grows, your work environment improves (12 or so people usually warrants free food and video game consoles)'.

Salute Inc, an organization founded by a former US Army reservist, Lee Kirby, tries to employ veterans in data centre management. The most significant skill might be endurance: 'Kirby argues that the transition from infantryman to data centre technician is easy: working remotely, maintaining dangerous equipment, communicating with a team and acting fast in the face of unexpected situations are skills expected both in the army and in data centers'.

Taking a step back from seeing the cloud as a medium that virtualizes social relations, we take the technicalities, standards and certificates that guide data centre operations to compose an alternative cosmogram of the cloud. In so doing, we move away from the metaphorical elusiveness implied by the figure of the cloud to ask how data centre operations enable, challenge and, to some degree, replace traditional sociality through the organizational intricacies of 'post-human institutions': a 'new form of architecture for data and machines ... almost liberated from human intervention and entirely shaped by technological rationales'. Our cosmogram does not reveal a disguised materiality – it is neither another mapping of its very material infrastructure nor a visualization of its equally material carbon footprint. Instead, we concentrate on the co-location of objects and technical practices that determines the place of the human in the data centre. 'To understand how people inhabit this world ... we must shift our attention from the congealed substances of the world, and the solid surfaces they present, to the

media in which they take shape and in which they may also be dissolved' (Ingold).

Approached from this perspective, the cloud appears fragile, physical, precious, neurotic even, in that it is constantly in need of maintenance and care, always insecure, despite its physical fortification through tailor-made architectures. Orchestrated through data centre operations, the cloud is constantly evolving computational and logistical challenges that human operators must take on in highly personal and material ways. The data centre is a new kind of architectural interface, the post-human institution that organizes human/non-human cohabitation as the labour of relentless troubleshooting.

John Tresch writes about a specific cosmogram, the tabernacle, that 'the day they stop doing all the different kinds of work that built the temple, when the people enter it, when the priests have accomplished all the necessary rites in the proper order, God comes to the Hebrews: in the form of a cloud, he fills the tent'. Ultimately, however, the tabernacle is a design for a nomadic institution. 'What is fundamental', Tresch writes, 'is that the link with God is made possible by the mediation of a construction described in an extremely detailed and technical manner and this construction has a place for all of society and all of nature'.

The technicalities, standards and certificates that guide the labour of data centre managers and engineers provide an alternative cosmogram, embodying the relations between humans, nature and logistical machines. Architects are now rushing to design data centres as aestheticized machine landscapes or avant-garde leisure zones (see, for example, OMA's Museum in the Countryside), to appeal to those whose 'chronopolitics' (Sharma) are entangled with the promise of remote and relentless accessibility. If Tresch's invocation of the temple seems a stretch, consider Liam Young's description of data centres as 'typologies without history'. 'Should we visit them like churches?', he asks. 'Or should we wander through them like we wander through a forest? Maybe we go on picnics to the

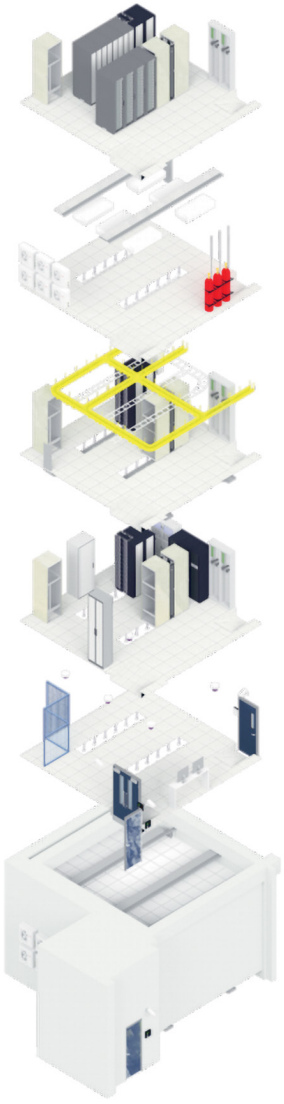
data centre like we once did to rolling hills. Maybe they become occupiable territories in ways that they're not allowed to be right now'.

The sacred geometries of the data centre materialize a certain 'infrastructural reason' (Carse), where human labour is defined through the operational politics of the cloud and an intimate relationship with the machine. In these spaces, the human must be adept at problem solving by trial and error, but is, at other times entirely alone with the cloud, or machine-like herself. As Tim Burke writes, my 'favorite data center was a building so hardened it was an accidental Faraday cage. When I went in, I knew that communication with the outside world was going to be severed like a cut ethernet cord. The data center was where I went to get away. It was where I went to think'.

Since the construction of early mainframe computers, shared computing facilities have provided models of how humans and computers might beneficially interact. Yet, in contrast to the emphasis on spatial co-habitation that high-flying architectural visions provide, we think of historical time-sharing systems as well as contemporary data centres as experiments in attuning the labour of humans to the rhythms of the machine. After all, a data centre 'is not a building full of computers but rather a computer with architectural qualities' (LeCavalier). The disorienting figure-ground relationship between the cloud and its data centres and other things that are part of our internet cosmology, disrupts and confuses our notion of what those alleged post-human institutions ultimately involve: more, and constant, human dedication to and intimacy with the machine. 'There is no room for a segregation mind-set', John Oyhagaray emphasizes. 'In the data center, everyone is responsible for system uptime'.

Cloud Cosmogram. To view the image in full size, visit http://cloudcosmogram.space/index.html. Or download the pdf: http://cloudcosmogram.space/index.html.

Image (opposite) Maya Indira Ganesh & Johannes Bruder



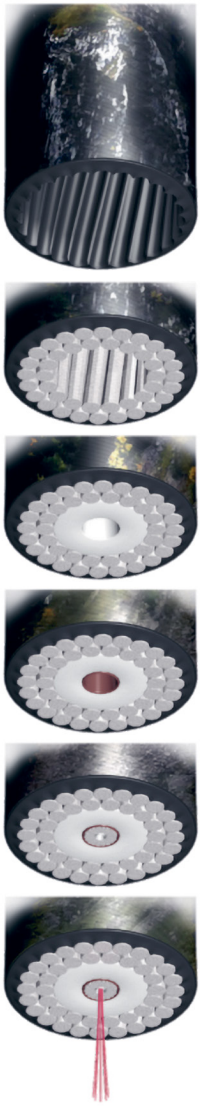


Image (above) Maya Indira Ganesh & Johannes Bruder
Image (opposite) Ned Rossiter

When nations speak of the internet today, they no longer use the language of the virtual but of soil. At the dawn of the internet, cyberspace was framed as a new realm decoupled from the state. This digital sphere stretched across the globe, making it essentially ungovernable. Yet over the last twenty years, this view has steadily been eroded, replaced instead by a vision of the internet as an extension of national territory. An array of technologies have arisen, both infrastructural and legal, that aim to align a nation's digital domain with its geopolitical domain, to marry its network with its physical boundaries and political interests – to create a domestic internet in the shape of the state. How do these forces impose territoriality on a system that is supposedly global and ungovernable? And how does the architecture of the internet enable or frustrate these efforts at bordering?

The internet was originally imagined to be a borderless realm. As the internet was adopted into more mainstream use in the mid-nineties, it was accompanied by the language of cyberspace. Cyberspace, it was argued, constituted a new realm in itself. On a technical level, the flexibility of network architectures seemed diametrically opposed to the nation-state and its hard-edged boundaries. Yet this architecture also led easily into a compelling political claim of being free from the legacies of state and soil. As David Wall remarks, the development of this 'exciting new domain' promised a global or international space that was 'potentially free of conventional politics, social order and social regulation'.

For many, this borderless world would not and could not be governed. 'Governments of the Industrial World', John Perry Barlow declared, 'Cyberspace does not lie within your borders ... Your legal concepts of property, expression, identity, movement, and context do not apply to us ... Ours is a world that is both everywhere and nowhere'. While Barlow's views emerged from a radical strain of politics, the ungovernable internet was taken up by far more mainstream politicians. In 2000, U.S. President Bill Clinton noted that Chinese authorities were already trying to crack down on the internet. 'Good luck', quipped Clinton, 'That's sort of like trying to nail Jello to

the wall'. The internet epitomized the free circulation of free speech. Any effort to impose a national set of values on this domain, to force it into a national mould, would only end in failure.

Along with cyberspace, terms like the information superhighway also posited a borderlessness, even if framed in different terms. As Tim May stated: 'National borders aren't even speed bumps on the information superhighway'. Through digitization, organization and connection, the internet would take the storehouse of the world's information, once the domain of exclusive libraries and elite countries, and make it available for all. This information superhighway would allow data to flow wherever it was needed, rendering the boundaries of the nation-state superfluous. The new borderless world was characterized by globalized flows of information, argued Kenichi Ohmae 'it is absurd to believe that lines drawn on maps can have any impact on its movements'.

Two decades later, those visions have been increasingly eroded to the point of seeming somewhat naive. Stepping into their place is a vision of cyber sovereignty, in the words of Yuan Wang: 'a natural extension of national sovereignty in the network environment'. In this vision, the singular Internet should gradually be transformed into 'our' internet, a national territory where norms should be defined, threats should be defended against and borders should be enforced. 'Behind the mists and magic of the Internet lies an older and stronger order', asserted Tim Wu and Jack Goldsmith, an order based on national laws and sovereign governance – a territorial order. Over twenty years, an array of techniques have been developed that assist states in imposing this order on the supposedly global and ungovernable internet.

The first of these techniques is data localization. For cloud companies, if data was certainly stored somewhere, that 'where' used to be 'wherever.' Such a view is increasingly at odds with the state-led push towards a territorial understanding of data. Cross-border laws seek to govern when and how data can be transferred into another jurisdiction. Information

according to these frameworks is not swirling in some nebulous realm 'out there' but is housed in data centres located inside the borders of the nation-state. As Pavan Duggal wrote, these cross-border laws challenge 'countries to adapt pre-digital modes of national sovereignty and economic competition to a digital industry that thrives on borderless and seamless exchange of information'. While the internet may be global, 'their' internet has clear boundaries. Indeed, one of the core aspects of cross-border laws examined by legal scholars are their 'territorial effect', the properties specifying what types of data are covered and under what conditions this data may be transferred outside the nation. Data itself has a geographical location, a place that lies inside or outside of the dotted line of the nation-state. From Malaysia to South Korea and Japan, many Asian countries have passed or are currently considering cross-border legislation.

As a result of this understanding, governments are placing companies under increased pressure to store and process this data in domestic data centres. In Anupam Chander and Uyên Lê's formulation, these localization strategies collectively construct a kind of 'data nationalism'. China's cybersecurity law, a rough analogue of the EU's GDPR, requires, as Alexander Koty writes, that 'all personal information and other key data produced and gathered ... must be stored in servers located in mainland China'. In the United States, GovCloud promises cybersecurity by offering a data centre infrastructure 'operated by employees who are U.S. citizens on U.S. soil'. Such language of soil and citizenry, dismissed as irrelevant two decades ago, points to the resurgence of territoriality within an internet context. Cross-border legislation frames data as a sovereign resource, information that is both inside the nation and linked to a national subject.

Alongside data localization, the increasing use of internet shutdowns represents a crude but powerful form of sovereignty. Berhan Taye argues that these intentional disruptions render the internet 'inaccessible or effectively unusable, for a specific population or

within a location, often to exert control over the flow of information'. Certainly, shutdowns have taken place in countries typically regarded as authoritarian: Chad, the Democratic Republic of Congo and Russia. However, the world leader in shutdowns is a democracy – India. India not only shuts down its internet more than all other countries combined, but is doing so more often, with the number of shutdowns ramping up over the last few years to become the 'new normal'.

For India, the internet is not a public good that must remain constantly available but a national infrastructure that can and should be switched off as necessary. Shutdowns in Kashmir, for instance, are justified by stating that they prevent the harmful spread of information, defuse tensions and maintain order. Regardless of its ability to quell civil unrest, the key point here is that the shutdown frames the internet as 'our' internet. Rather than a universal and global resource, this internet becomes a domestic infrastructure, a territory that follows the footprint of the nation-state and ends at the border. Along with this geographical link to the nation, there is also a link via power. Shutdowns flex a state's sovereign control, demonstrating a nation's ability to exert a crude but devastating force over their infrastructure by turning it off entirely.

Next to shutdowns, filtering or blocking presents a more sophisticated form of territorialization. Information on a domestic network can be filtered by hardware or software-based firewalls. Control at this 'digital border' allows packets to be modified, diverted or ignored altogether, aiming to construct an internet shaped in the image of the state. The prime example in any discussion of filtering is China and its so-called Great Firewall. Geremie Barme and Sang Ye argue that by filtering out polluting material 'aimed at undermining the unity and sovereignty of China', engineers sought to create their own distinct version of the internet, 'a Net that has Chinese characteristics'.

Filtering information seeks to remove or block media that are considered objectionable according to both governmental legislation and societal norms.

In this sense, filtering inherently frames the internet as an extension of national territory. To counter the dangerous and unfiltered information 'out there', technical mechanisms control the kind of information allowed into a country. The aim is to align the digital territory of China with its physical territory, to eliminate any kind of disparity when a subject moves between offline and online environments. For Xi Jinping 'there is no distinction between the virtual world and the real world: both should reflect the same political values, ideals and standards'.

What inspires this territorialization of the internet through shutdowns, localization and filtering? Certainly, one motivation is control. For states, these techniques aim to claw back a degree of authority over a domain seen as frustratingly slippery. When the internet becomes a tinder box that may ignite tensions – or more cynically, a site of counter-protest or embarrassment for the political establishment – then states want the ability to clamp down on these communications.

Yet perhaps more justifiably, these measures also kick back against a 'universal' vision of the internet long recognized as implicitly US-led. For some nations, the supposedly global internet appears more like American dominance enjoyed by a handful of technological giants: Google, Facebook, Apple, Amazon and others. These corporations, as Kalev Leetaru points out, are aligned with the technolibertarian ideologies of Silicon Valley and the broader Western values of consumerism and individualism. For states with more authoritarian leanings, a shift from the global Internet to a national internet allows them to strip out these unwanted values and begin embedding their own ideals.

For critics, such moves put the internet in danger of fragmentation, where the global internet becomes fragmented into dozens of nationalized and incompatible networks. Urgent calls to prevent fragmentation can increasingly be found in mainstream outlets, from technology blogs and civic organisations to political magazines. Yet, examining the literature, the world has stood on the edge of the fragmentation precipice for twenty years. Anxieties around fragmentation emerged

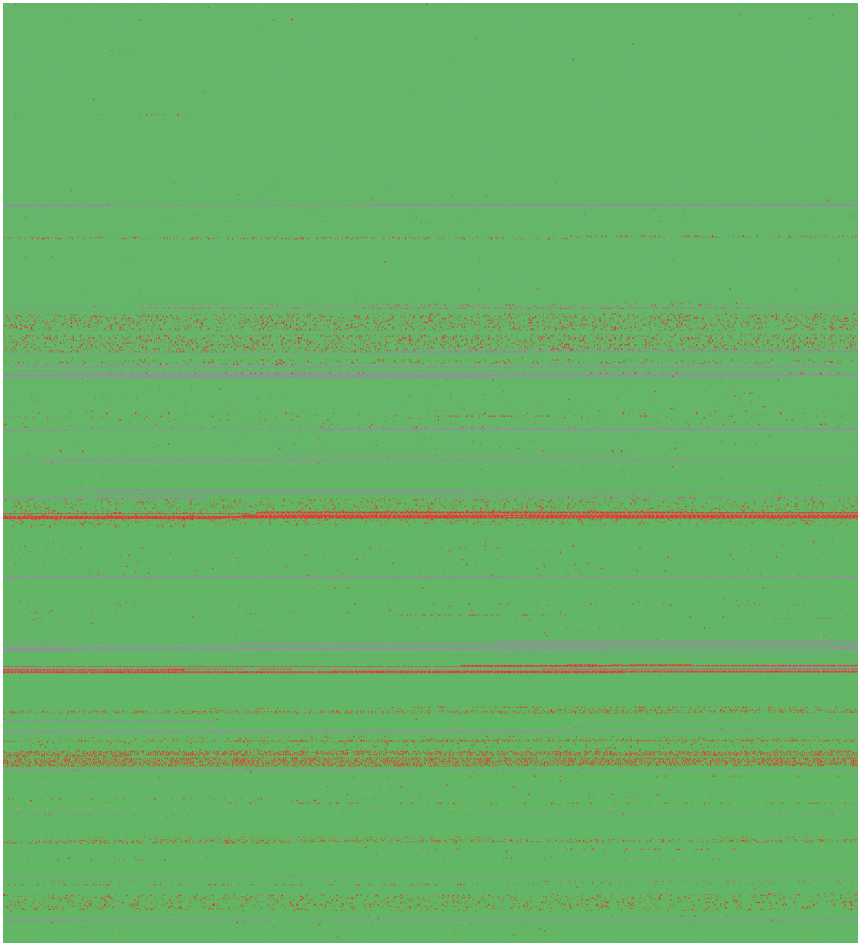
as early as 1997 and have continued uninterrupted since then, with each scholar proclaiming the end of the 'free and open' internet.

Despite the hand-wringing of these critics, the internet was always already fragmented. The singular 'Internet' implies a cohesive and overarching network that spans the globe. But the internet is better understood as a system of systems, a network of networks. And along with this technical fragmentation, each network also possesses a degree of autonomy emerging from its unique social, cultural and historical development. This is why scholars like Gianluigi Negro, James Griffiths, Johnny Harris and Benjamin Peters can chronicle the emergence of the Chinese internet, the Cuban internet, the attempt and failure to construct the Soviet internet and so on. These observations show how fragmentation has always been integral to the internet, both in technical architecture and historical development.

But perhaps the most damaging aspect of fragmentation as a spectre is that it replaces a myth of the borderless internet with another myth of the tightly bordered internet. Based on an (idealized) Westphalian model, the world is carved up into what James Caporaso calls 'spatially exclusive units' without overlapping jurisdictions. In this vision, each nation's internet conforms perfectly to the dotted lines of their national boundaries.

There is certainly a shift towards territorialization, with nations framing these networks as an extension of sovereign space. However, these territories are messy and their borders are permeable. The state dream of territorialization remains incomplete, and this is not due merely to technical inability, but because the nation derives its identity from entities outside itself. As a brief example to close, we can point to the 'troll army' of Diba. China's Great Firewall can be crossed using virtual private networks, or VPNs. Using these technologies, Diba's thousands of online activists jump the firewall in order to attack individuals and institutions that they declare have offended the nation. In venturing outside the domestic internet and onto platforms like Facebook and Twitter, their campaigns

overtly disobey the sociotechnical borders established by the state. And yet these 'extraterritorial' activities seek primarily to reinforce the authority of the Party and bolster the concept of the nation for its inhabitants. Their actions show how the territory is shaped by activities outside it; the identity and stability of the nation is derived from its surroundings. This 'porous' territory presents a counter-image to the simplistic dichotomy of borderless versus fragmented, offering a more nuanced view of state attempts at internet nationalization.



Images (above and opposite) Luke Munn

The cultural history of the data centre in today's Singapore begins with cyberpunk. But let's be clear: it's not that this marginal, paraliterary genre, pioneered by a handful of North American authors, succeeded in predicting the future – that is, our present. Instead, the cyberpunk writing of the late 1980s and 1990s gave literary form to the uneven historical unfolding of *its own present*, registering, with techno-Orientalist bewilderment, the contradictions between what was (even then) a novel application of state power and what were (not quite yet) the exigencies of a globalizing, data-driven capitalism.

Neil Stephenson's 1996 essay, 'Mother Earth Mother Board', is one of the first great meditations on internet infrastructures. It is framed as a travelogue in which the author, a 'hacker tourist', documents and historicizes the laying of a hybrid undersea-overland cable of then-unprecedented length, the Fibre-Optic Link Around the Globe (FLAG). Singapore appears as a hazy semi-presence that refuses to connect to this ambitious cable lay. Four years after Stephenson's piece appeared in *Wired* magazine, the less evocatively named Southeast Asia-Middle East-Western Europe 3 cable, a project behind which Singapore threw its considerable island weight, would exceed FLAG in length by some 10,000 kilometres. SEA-ME-WE3 is still the world's longest cable. Its administration lies with Singapore's premier telecommunications company, Singtel, which the country's government owns by way of its sovereign wealth fund Temasek Holdings.

To Stephenson's name, we can add that of William Gibson and his notorious essay on Singapore, 'Disneyland with the Death Penalty'. There, Gibson reflects upon the possible futures awaiting Singapore in the wake of the government's sweeping turn to information technology. It is 1993, and Singapore wants to bring itself online. Singtel's manoeuvres in the international submarine cable industry are part of a wider set of state-directed shifts, collectively branded the 'Intelligent Island' initiative: computers in the home and the workplace; partial automation of air and maritime transportation

infrastructure; recalibration of the workforce towards cognitive and service labour. For Gibson, Intelligent Island heralds an imminent collision. How will such a fastidiously administered society with its eminently functional infrastructures and its uncontested juridical punitivity, he asks, handle the pornographic weirdness, the anarchic 'wilds' of the same 'X-rated cyberspace' with which it now seems so desperate to interface?

By the early 1990s, the economic hegemony of Japan was on the wane and cyberpunk had yet to register the immense productive forces of a burgeoning Chinese capitalism. Singapore, then, served as a new or transitional repository for techno-Orientalist figurations. Consider a sequence from Bruce Sterling's 1988 novel *Islands in the Net*, where the transcript of a parliamentary hearing on Singapore's information governance interrupts the cyberpunk moment par excellence – plugging into the Net:

She sat, and turned the deck on, and loaded data. Pop-topped a jug of mineral water and poured it in a dragon-girdled teacup. She sipped, and studied her screen, and was absorbed. The world around her faded. Into black glass, green lettering. The inner world of the Net. PARLIAMENT OF THE REPUBLIC OF SINGAPORE Select Committee on Information Policy Public hearings, October 9, 2023

In *Islands in the Net*, cyberspace is not a representational abstraction, but a literary configuration of infrastructure space. On the novel's first page, the protagonist trips on an electrical cable and falls hard on her face. Sterling describes the Net not as a matrix of information but as a world-historical integration of old-new communications infrastructure. Meanwhile, the eponymous 'islands' are 'data havens' that feed upon the global economy of information, 'abstracting, condensing, indexing and verifying' the data that the Net economy requires for its operations. These 'islands' circumvent commercial protocols and privacy laws in order to store data indiscriminately and limitlessly. We could say, using twenty-first century terminology, that Sterling's data havens blend the technical functions of the data centre with the murky juridical status of the special economic zone.

As an island haven of this sort, an 'arrogant and technologically reckless' Singapore is home to 'radical technical capitalists', complete with their own space programme, who stand stubbornly opposed to the 'globalists', the 'post-industrialists', the 'economic democrats', the partisans of the harmonious global order promised by the Net. Suffice it to say that Sterling shares Gibson's deep misgivings with the heavy hand of the country's technocratic rule. The novel's Singapore segment begins with airtight socio-political control but spirals into chaos and breathlessly concludes with riot, martial law, barricades in the streets and a bloodbath in the Straits of Malacca. The encounter between Singaporean governance and global data flows must end in catastrophe. Otherwise, as Gibson frets, Singapore 'will have proven it possible to flourish through the active repression of free expression. They will have proven that information does not necessarily want to be free'.

It's an anxiety of the 1990s indeed, almost a quaint one to our ears; one cannot argue any longer, under conditions of today's data-driven capitalism, that the Singapore government exercises a monopoly on the unfreedom of information. But the point is not to valorize cyberpunk for its predictive qualities. It is instead to reach for a more salutary insistence, namely that taking Singapore-oriented cyberpunk seriously will make it difficult to think Singapore's encounter with global data technologies in isolation from cycles of accumulation and crisis at the level of the capitalist world-system. The data centre can and should be historicized – this principle is what we keep in mind as we close the novels and walk among the buildings.

Within Singapore's short post-independence economic history, the origin of the government management of wired connectivity lies in the wired connectivity of government management. While Gibson and Sterling were publishing their cyberpunk opuses, the Singapore government was already several years deep into the first phase of its National Computerization Plan: the Civil Service Computerization Programme. The very first 'data centre' in Singapore would shortly

appear, growing out of a move to centralize the National Computer Board's (NCB) servers into three 'hubs' – one each for land, people and enterprises. Singtel's late 1990s purchase of National Computer Systems, the private-sector arm of the NCB, indicated a sharp convergence of government computerization initiatives with government-linked expansion into regional and global telecommunications. More recently, the Smart Nation masterplan initiative, rolled out in 2014, promises to shape policy around the state's accumulated hordes of population, environment, infrastructure and surveillance data. 'The government', as the chief executive of the newly minted Government Technology Agency (GovTech) puts it bluntly, 'has a lot of data'. When we examine Singapore's data centres from the perspective of land zoning, electrical grid allocation, environmental policy and the promotion of investment by multinational corporations, we also brush up against the place of data storage within the technological innovations of the state apparatus. State plans for Singapore's data centres run in parallel track to the centrality of data to Singapore's state planning.

The Singaporean data haven in Sterling's novel had 'the dignified cover of an address in Bencoolen Street, while the machinery hummed merrily in Nauru'. No such stark sundering of front-end commerce and back-end hardware is to be found in Singapore's data centres. More often, the humming machinery *is* the dignified address. The practical desire for server co-location and proximity to cable landings sometimes appears indistinguishable from the wish-fulfillment of seamless connectivity. A technical specifications pamphlet for Global Switch's data centre in Tai Seng outlines the structure's cooling, connectivity and security features, but also emphasizes its location: 9 km from the Central Business District, 15 km from Changi Airport, a Mass Rapid Transit station within 10 minutes walking distance. Data centre clients, it would seem, want to feel linked not only to the cable networks of the wider Asia Pacific region from the Singaporean switch point, but also to the financial strongholds and transportation infrastructures of the island itself.

The production of urban space in Singapore, wherein space is subject to homogenization, allotment, measurement, sorting and categorization, begs the question of the *preconditions* for such logistical ordering or, in other words, the prior conditions of enclosure and dispossession that could have made such a formal spatial order operative in the first place. We know from historians like Loh Kah Seng that present patterns of residential and industrial zoning in Singapore could not have happened without large-scale evictions and resettlements of so-called 'squatters' in the wake of the devastating *kampong* fires of the 1950s and 1960s. Up to a third of Singapore's data centres are located in what was once the Lorong Tai Seng *kampong*, where extant residents were all resettled into state-subsidized public housing in the three decades following a landmark August 1961 fire. A daring 1986 land swap by the Jurong Town Corporation, the government-linked agency behind Singapore's post-independence industrialization, would go on to cement the transformation of the old Lorong Tai Seng into the Tai Seng Industrial Estate, which now hosts local and regional data centre players like Starhub, ST Telemedia, Global Switch, Keppel DC REIT and Equinix. Meanwhile, the social history of the Jurong Industrial Estate, home to many of Singapore's remaining data centres, has yet to be written. State and state-friendly narratives of Singapore's industrial explosion frequently emphasize the providential features of the invitingly vacant Jurong swampland, with its flat terrain and proximity to deep coastal waters, while glossing over the more stubbornly human subjectivities that had to be cleared out along with the trees. Land acquisition and squatter resettlement were the ineradicable undercurrents of the dizzying years of industrialization. In the age of deindustrialization and datafication, they remain critically unthought episodes in the data centre's prehistory.

The zoning discourse of the Urban Redevelopment Authority (URA) defines data centre operations as 'E-business activities regarded as industrial uses'. Once designated as industrial buildings, Singapore's data centres must be constructed according to state guidelines on fairly rigid 'use quantums', such that a

minimum of 60 percent of the building's gross floor area (GFA) must be used for 'industrial purposes' – in this case, server racks. Just as containerization in shipping forced a degree of abstraction by shifting the standard unit of measurement for commodities from weight to volume, so too do state agencies like the URA domesticate data centre functions by incorporating them into established spatial frames of calculation and measurement. Zoning and urban planning are the spatial techniques that attempt to render data centres knowable to the state. This is state logistics understood as 'a particular, abstract representation of space' (Toscano), a 'volumetric urbanism' (McNeill) of which Singapore is an avant-garde practitioner.

The Centre for Strategic Futures (CSF) is a think tank of the Singapore government, housed within the executive agency known as the Prime Minister's Office. In his foreword to the 2019 issue of the CSF's publication *Foresight*, Singapore Prime Minister Lee Hsien Loong describes the project of futures planning as an interminable 'work that will never be done', as an intellectual project anchored in 'developing contingency plans free from the day-to-day demands of operational responsibilities'. This is not speculative fiction, but speculative governance. The nation-state must prioritize flexibility and resilience and must account and design for what Lee calls 'black swan events' and inevitable system failures; the nation-state must be run, in short, like a data centre.

If, as the CSF's Senior Advisor goes on to write, 'it is in our DNA as a country' to respond to 'complexity, uncertainty and accelerating change', then the state governance of data centres finds a shining prefigurative authorization in Singapore's colonial past, so that the colonial vision of entrepot trade and the contemporary vision of data circulation partake in the same genius of foresight: 'Just as Raffles made Singapore a free port in 1819, welcoming traders from any country, Singapore today could be a free data port'.

Does accelerating data centre construction on the island call back to imperial trade strategy in the same manner that fibre-optic cables retrace the

undersea pathways of colonial telegraph lines? In either case, it's plain that this historical repetition is neither natural nor guaranteed. The state intelligentsia knows that physical geography alone cannot, or cannot any longer, secure Singapore's position as a hub in a network. Like the move to reassert Singapore's transshipment dominance with the decades-long Tuas Mega Port project, the government's support for the data centre industry expresses a commitment to built form. It is these plans for construction, and not happy accidents of latitude, that will allow Singapore to continue understanding itself as a polestar orienting oceanic and digital channels of circulation. The recapitulation of logics of colonial economy is not an evolutionary spasm, but a state-directed project.

A 2017 renaming of the new data centre hub in the Jurong Industrial Estate, from the bland 'Singapore Data Centre Park' to 'Tanjong Kling', raises even more baleful colonial spectres. Ostensibly, the change associates data centre land nominally with existing industrial land also called Tanjong Kling. Urban planners seem to have forgotten the history of this word *kling* or *keeling*: its use in the colonial period is a racial slur. A once neutral Malay-language designation for the South Asian Kalinga kingdom had, by the early twentieth century, become a derogatory term for any person of South Asian descent, after *kling* was also generally understood to reference the jangling restraints of South Asian indentured labourers set to work in chain gangs throughout British Malaya. Indeed, what is now Chulia Street in Singapore's downtown core was 'Kling Street' until the 1920s, when the Indian Association of Singapore objected to the name and successfully lobbied for a change.

Today, one can walk around the Tanjong Kling park and see not towering data centres but empty allotments and glacial construction activities. Here and elsewhere, labourers from the Indian subcontinent constitute a visible majority among Singapore's construction workers. Their working conditions are framed by a backdrop of debt-financed migration and are sited at the conjunction of poverty wages, weak

labour laws and rampant intimidation tactics on the part of construction bosses. To set South Asian labourers to work building data centres in Tanjong Kling is to then mark their workplaces with the stamp of an earlier (but perhaps not, after all, so different) regime of labour migration and uneven development.

In 'Mother Earth Mother Board', Stephenson offers the following adage: 'Everything that has occurred in Silicon Valley in the last couple of decades also occurred in the 1850s'. This axiom remains instructive as a polemical corrective rather than an analytical truth. Its suspicion of analytical presentism is welcome, but it does not mean that the answer to the mysteries of the data centre is to be found in the innermost logics of 'copper cable colonialism' (Starosielski). In that spirit, it would also be mistaken to claim that everything that has occurred in the Singaporean governance of data centres has already occurred in cyberpunk. The final call, towards which this essay is an assemblage of preliminary attempts, will instead be to *multiply the genealogies of the data centre* in service of an attentiveness to the equally multiple political possibilities adequate to an era for which the data centre is the unassuming symbol.

Image (opposite) Ned Rossiter


COSCO

007 HOW DATA CENTRES PRODUCE TOPOLOGIES OF TERRITORY AND LABOUR

Brett Neilson & Tanya Notley

When people hear the term *data centre architectures*, they are likely to conjure images of large non-descript box buildings or perhaps of converted manufacturing warehouses. Far less likely will they consider the more opaque and hidden interior network architectures that connect machines inside data centres, even though these topologies are, operationally, much more influential.

The great allure of data centres is that their network architectures allow actors that operate within them to extend their activities territorially by establishing links with distant client machines. In doing so, data centres change the relationship these actors have with labour forces. To understand the client footprint produced by data centres as a form of territory is to treat these facilities not only as digital infrastructures but also as political institutions that influence the wielding of power across wide geographical vistas.

By paying analytical attention to the forms of power produced and sustained by data centre operations, we seek to extend the debate concerning the rising importance of these facilities in order to consider their implications for labour forces, workers and political struggle.

Server–Client Territories

The server–client relationship underlies the network architectures that data centres establish and implement with machines that operate outside their big box structures. In a server–client architecture, all computers connected to a network are either servers or clients. The former run programs or applications that share their resources with clients. The latter do not share resources but request content or service functions from servers. Clients distribute themselves around data centres, although not necessarily in spatial proximity.

However, this relation between servers and clients, also known as a north-south network relation, is not the only one that data centres enact. Because data centres concentrate servers under one roof and allow the establishment of peering connections – where servers can exchange data 'east to west' quickly

with cables plugged in to connect one server with another – they become powerful sites of data storage and service delivery.

To enter a data centre is to encounter a space devoted to the efficient operation of technical systems and largely devoid of human bodies and labour. Yet the humming fans and flashing lights on servers register the presence of distant labour forces that connect to the facility, knowingly or otherwise, at the client end. These may be traditional labour forces, however hired or located. Alternatively, they might be users, such as those who offer up data on social media platforms in return for the use of 'free' services.

Data centres store, process and transmit data from clients spread across diverse spaces and scales. This enables those actors who hire or place servers in these facilities to engage in economies of extraction that process, aggregate, analyze, use and sell data generated by these same clients.

For example, organizations with servers in data centres quartered in Singapore are predominantly interested in this location as an efficient and secure gateway to data sources and digital services operating within the Southeast Asian region. Singapore has advanced data infrastructure, attractive tax rates, flexible labour laws (for skilled migrants) and start-up and lucrative R&D incentives that have allowed the data industries to flourish. Singapore is also geographically sheltered from natural data disrupters: it is not prone to earthquakes, cyclones and tsunamis like many of its neighbouring nations. There are 70 to 75 very large data centres in the country, which constitute about half of Southeast Asia's total data centre capacity.

The presence of a company like Telin (Telkom Indonesia), which runs three data centres in Singapore under a local subsidiary, means that much of the data generated by this firm's clients is stored and routed through facilities in Singapore. Not only do Telin's Singapore data centres offer a launch pad for companies seeking to market digital products and services to the expanding ranks of Internet users in

Indonesia but they also provide service capacities for Indonesian companies and institutions that connect to Telin's national ICT networks.

Data centres generate a client footprint, or territory, which follows patterns of networked distribution and cuts across the exclusivity and contiguity of state territories. Yet because data centres obscure relations between clients and can only pass information through the mediation of servers, such patterns of territorial networking remain invisible to almost everyone, at least to those actors that are not organizations operating within such facilities. Data centres market their territorial reach to enterprises interested in hiring server space, giving territory a fungible quality. By this, we mean that the conceptualization of territory by data centre operators and users is characterized as much by openness and receptivity to patterns of economic exchange as it is to the political sovereignty of any particular state.

Telin Singapore, for instance, seeks to attract international business by highlighting its extensive network across the Indonesian archipelago. Yet, given the centrality of digital networking to contemporary forms of governance and rule, the commercial imperative of providing territorial reach to organizations operating in data centres also has wider legal and political implications.

Saskia Sassen notes that networked digital structures integrate 'only parts of national spaces' and 'cross multiple interstate borders with great ease'. Remarking that such networked structures cannot 'survive without some very material infrastructures, and, often massive conglomerations of buildings', she describes them as '*situated* territorial spaces' or 'new cross-border geographies of centrality'. Although Sassen does not deal directly with data centres, her understanding of these 'extractive and infrastructural spaces' registers the way in which data centres produce 'bordering dynamics' that are 'partly formalized, partly emergent, and partly not necessarily meant to be formalized nor to be particularly visible'.

Traffic: North–South and East–West

The capacity of data centres to generate operational spaces that function within but also partly beyond existing law and jurisdictional relations is an important territorial feature of their client footprints. These complex territorial dynamics do not mean that data centres are generic spaces whose geographical location is inconsequential. Although they may have weak social, as opposed to infrastructural, ties to the urban or national contexts in which they exist, these facilities tend to cluster in formally constituted territories that offer a safe harbour for data storage and favourable business environments because of their connectivity to electricity, undersea and overland cables.

Not all data centres (or indeed digital networks) are alike. The first and most obvious difference is between data centres run by single firms for their own operations and those that are multi-user ('co-location') data centres that bring servers utilized by different firms under a single roof. Data centres also have different network configurations that effectively form complex and distinct architectures. With names such as closed-tree, Clos, fat-tree, Dcell, BCube, c-Through, Helois, PortLand and Hedera, these network topologies determine how physical machines connect materially to each other (directly or via switches) in data centres. Different topologies imply different trade-offs between network qualities such as speed, redundancy, path diversity, energy conservation and scalability.

A data centre that attracts business from high-frequency financial traders, for instance, is likely to have a Clos topology, since this architecture reduces buffering and favours low latency transmission that provides information from stock markets with minimal delay. By contrast, a large commercial multi-user centre might prefer a fat-tree topology that modularizes the servers used by different firms and connects them to each other via electronic switches that lead to a 'meet-me' (peering) room. When such a centre supplies software, platforms or infrastructure as a service, however, a more flexible

architecture that utilizes optical switches to reconfigure during runtime is an attractive option.

The design of network topologies extends outside data centres into cabling systems, while the various architectures available have their own infrastructural histories; for instance, the widely used Clos topology has its origins in 1950s telephone exchanges. Different topologies can combine in a single data centre, for instance, creating hybrid networked architectures that seek to balance and optimize operations.

On top of the physical infrastructure of network topology, a software layer controls the virtualization process by distributing load and virtual machines across physical machines. With names like Sunbird, Nlyte and Tuangru, data centre infrastructure management software packages bridge information across organizational domains to configure workflows, power use and the like. Technically, this means the interaction with any single client stretches across different physical machines or even across physical machines in different data centres. It also means that data centre operations – including different types of interactions with workforces – become 'virtualized' or, put another way, opaque, dispersed, fragmented and hard to pinpoint as situated in any particular place or time.

Because of developments associated with virtualization, east–west traffic (between servers in the same facility) increasingly outweighs north–south traffic (between servers and clients located outside of data centres). Typically, a client interacts with a server in the access layer of a data centre, which then refers the query to other servers in the facility to assemble a response and send it back to the client. A search query, for instance, generates only a small amount of traffic between a client and the data centre. However, the response to this simple query generates a massive amount of traffic within the data centre.

Much of this east-west traffic relates to internal queries on user demographics, browsing history, interests, recent purchases, and so forth, and thus supports the extractive business models behind many social media

and mobile apps. Yet, because this arrangement means that signals generated by different clients often traffic across the same physical machines, it also generates infrastructural connections among users, firms and labour forces that might otherwise not be obvious.

Current accounts of global production tend to rely on metaphors of chains, flows or networks to trace and explain changing relations among economic actors. However, if we are to account for how the infrastructural conditions specific to digital economies shape relations between users, firms and workforces, we need to supplement political economic analyses that rest on these metaphors with an understanding of the new data architectures that determine the nature of operations inside data centres.

We are aware that the physical production of material commodities continues to expand at the global scale and that we cannot understand digital labour in separation from a wider analysis of changing divisions of labour. However, information networks have been crucial to the social expansion of labour beyond the walls of the factory and the office. Informatization also reorients other modes of production, from peasant economies altered by the introduction of genetically modified crops to manufacturing industries challenged by new fronts of automation based in artificial intelligence and machine learning.

Artificial intelligence and machine learning also contribute to service economies that are beginning to eclipse the advertising-based business models of large tech firms. Significantly, these technologies require the storage and processing of large amounts of data in data centres, confirming the centrality of these facilities to contemporary operations of capital. If we understand data supply as labour, however, what this situation confirms is that the real engine of these developments is living knowledge, intelligence and subjectivity.

Unpicking Networked Production Topologies

To speak of production topologies is to augment the discussion of the global economy based in metaphors of chains, networks and flows with knowledge of the

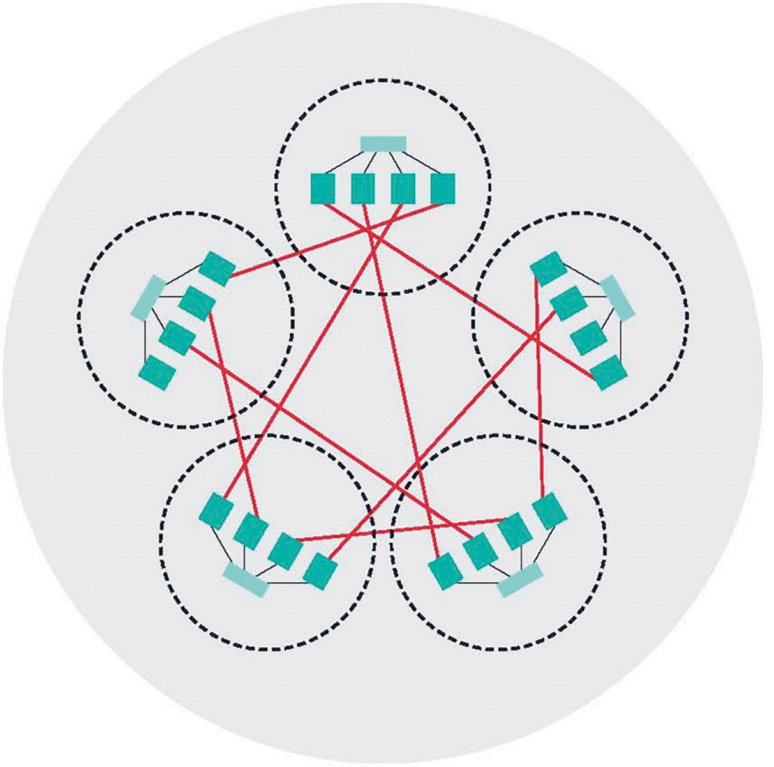
network architectures that structure operations within and between data centres. Celia Lury, Luciana Parisi and Tiziana Terranova suggest that topology provides a way of describing how 'a distributed, dynamic configuration of practices is organising the forms of social life'. In their conception, topology is 'emergent in the practices of ordering, modelling, networking, and mapping that co-constitute culture, technology and science'.

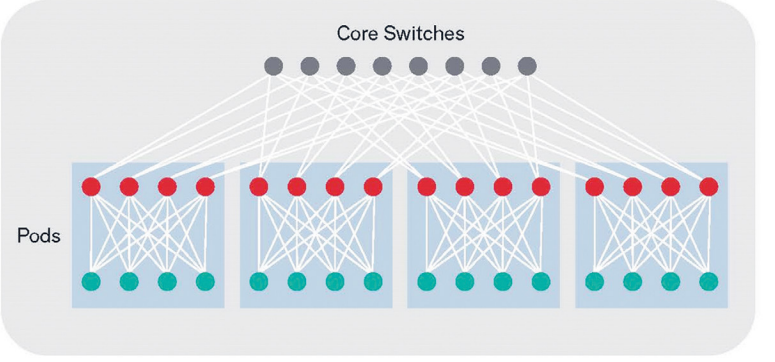
We seek to extend this perspective by bringing a discussion of how data centre networks open to a high degree of variability contribute to relations between firms, users and workforces in the contemporary digital economy. Knowledge of data centre topologies and processes of virtualization places the relations involved in producing goods and services and reproducing knowledge, capital and labour power in a more dynamic context.

Doubtless, production still sometimes occurs through linear chains and fixed networks; but without an appreciation of the more complex and distributed production relations introduced by data centre topologies, it will be difficult to identify critical points in production processes where workers might effectively apply their agency. This is because data centres provide an infrastructural fix for capitalist actors to skirt traditional labour actions, by designing logistical routes around which to redirect production processes, for instance, or by furnishing technologies of fault tolerance and mirroring that absorb such disturbances in ways that minimize their effects.

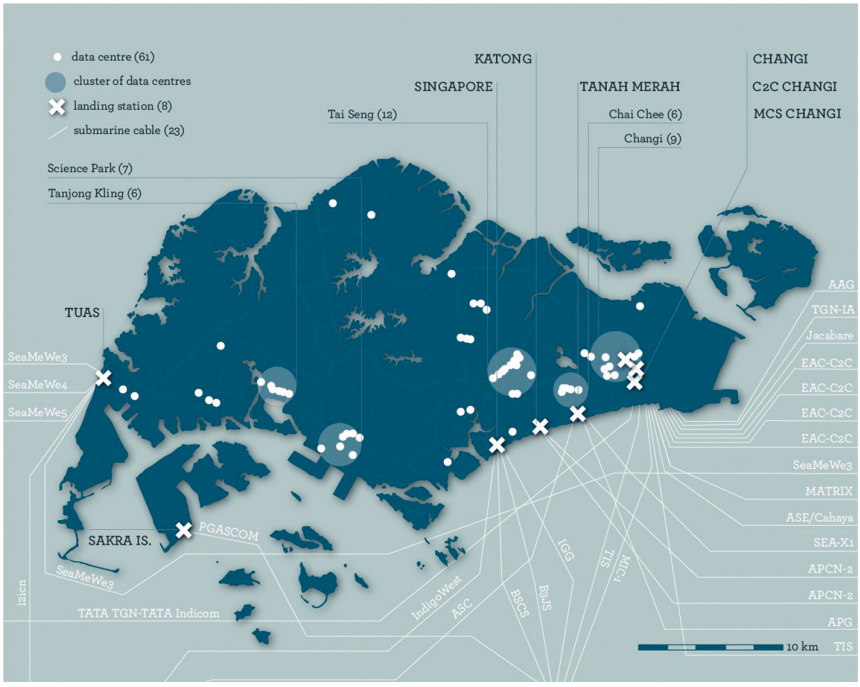
Assisting workers to see and understand how data centre production topologies connect them across different countries (or prevent them from being connected) and how they affect their employment statuses and social identities is a first step to imagining new forms of organization and solidarity adequate to challenge the extractive operations of contemporary digital capitalism.

A longer version of this text was published in the journal *Work Organisation, Labour and Globalisation*.





Images (above) makework (opposite) Andrea Pollio


data centre (61)
cluster of data centres
landing station (8)
submarine cable (23)
KATONG
SINGAPORE
TANAH MERAH
CHANGI
C2C CHANGI
MCS CHANGI
Tai Seng (12)
Chai Chee (6)
Changi (9)
Science Park (7)
Tanjong Kling (6)
TUAS
SeaMeWe3
SeaMeWe4
SeaMeWe5
SAKRA IS.
PGASCOM
SeaMeWe3
TATA TGN-TATA Indicom
i2icn
IndigoWest
ASC
BSCS
RJS
IGG
TIS
MCT
AAG
TGN-IA
Jacabare
EAC-C2C
EAC-C2C
EAC-C2C
EAC-C2C
SeaMeWe3
MATRIX
ASE/Cahaya
SEA-X1
APCN-2
APCN-2
APG
TIS
10 km

008 **DATA FARMS SONIFICATION: AN EXPERIMENT IN DATA MODELLING AND SPATIAL AUDIO**

Sarah Cashman, Michela Ledwidge & Brett Neilson

The world has been transformed by data. We rely on it. It's an essential part of contemporary life. Yet we rarely give thought to where it comes from, how it moves around the globe, or the environmental costs of its storage, transmission and processing. What if you could hear information flowing from one data centre to the next? What if each data transaction came with its own unique audio signature? From the gentle resonance of mundane data operations to the eerie sound of hijacks and attacks, the Data Farms sonification was an experiment in giving voice to data and its movements in the Asia-Pacific region.

The Data Farms sonification took the form of an immersive spatial audio application intended for use on a mobile device with headphones. Four or five users would carry their devices into an installation setting defined by a central marker. As they moved around this space, their locations would generate sonic 'events' based on real data and the probabilities of these events occurring in actual data centres. By default, these events were not visually depicted so that users could take an exploratory approach, however they could choose to display on their devices a text transcript describing the triggered events.

As it happened, this sonification experiment was stalled by the Coronavirus pandemic. The outbreak hit just as the build was finished. Lockdowns closed galleries and other installation venues. Social distancing protocols disallowed the bringing together of users in a confined space. The experiment is a process prone to failure, but in this case, it was the human and social landscape in which the sonification was to take shape that crashed. Responding to this predicament, this article and the videos that accompany it give a sense of an experience that is yet to be.

Concept

The sonification was developed by Sydney studio Mod in collaboration with researchers from the Data Farms project. Named for 'modding' practices in game cultures, Mod is a studio specializing in real-time and virtual production across platforms. Drawing on experience in alternative reality (AR) development, Mod's creative and

technical lead Michela Ledwidge worked with the Data Farms team to conceptualise and execute the build. The application was developed on Unreal Engine and sought to break ground by correlating locationally-generated spatial audio to physical movement through a virtual soundscape.

The challenges of translating the Data Farms research into an amenable user experience were manifest. With research sites in Hong Kong, Singapore and Sydney, the project approached data centres not simply as digital infrastructures critical to contemporary life but also as political institutions that generate distinct forms of power. Central interests were how these facilities generate client footprints that extend beyond national borders and the relevance of these networked territories for data extraction and labour exploitation.

These concerns influenced key design features of the sonification. For instance, the virtual space was divided into three 'territories' that represented the project research sites. As users moved between these territories, they would hear an instrumental variation in the sound generated on one of the application's two tracks. Importantly, on the other track, they could still hear events spawned in the other territories. However, due to their position, they would hear these events with less intensity, volume and tonality than if they were proximate to them. These sonic qualities reflected the project's interests in data transactions and territory.

Deeply embedded in the application's design, these auditory variations were not meant to be immediately intelligible to users. Instead, the sonification was intended to provide an aesthetically memorable experience, to provoke a sense of wonder and play that would prompt users to develop greater awareness of the role of data centres in today's economy, culture and society. To this end, two features were important. First, the experience should be brief, no longer than two or three minutes. Second, the sonification should have musical and cultural integrity. For this latter reason, musician and composer Yunyu Ong was added to the team to craft the sonic elements representing Hong Kong, Singapore and Sydney.

The choice to build a sonification was sparked by a desire to contrast the mainstreaming of data visualization as a research method and means of knowledge dissemination. The intention was to engage and communicate with non-expert publics on an intuitive and emotional level. However, the expectation was that this experimentation would also allow researchers to stumble across new patterns and questions in exploring data centre operations. Given the high degree of security surrounding these facilities, there was also the hope to open paths of investigation that didn't require physical access or direct contact with industry, although these were methods pursued in other parts of the Data Farms project. The sonification drew on publicly accessible internet databases as well as an expressly constructed data model that generated plausible events based on a researched portfolio of use cases.

Data Model

Sonification is not merely composition. It requires data to sonify. In the case of a sonification about data centres, it would seem that such data is abundant. After all, these facilities are vast sheds for the storage, processing and transmission of data. Yet much data held in data centres is proprietary, meaning unavailable for public use. Those data that are accessible do not necessarily relate to data centre operations just because they are transacted in these infrastructures.

In conceptualizing the sonification, data sources such as the registry of Autonomous System Numbers maintained by the Internet Assigned Numbers Authority and the PeeringDB database of network interconnection data were referenced. However, these data relate primarily to the routing of data signals between data centres. Their use needed to be supplemented by a data model that could plausibly generate data centre events and consequence scenarios representing routine transactions made in these facilities.

This data model is built on the Neo4j Bloom graph database platform that supports both the public facing app and a stand-alone query tool. The intention of

the query tool is its use independently of the sonification to research the relationship between a web resource and associated organisations and territories. The model generates events based on a simple actor, verb, subject syntax; for example, 'writer posts blog post', 'soldier seizes server', 'bot deletes social media post'. Permutations of relationships between actors, verbs and subject are editorially managed in the data model. The data is managed according to a list of use cases derived from the Data Farms project research and categories published by Freedom House detailing scenarios of filtering, blocking, content removal, digital attack and so on.

Events are generated by impact rules and probabilities in the model. The generated events can be thought of as plausible story elements that are combined with data from PeeringDB to assign a legal personality and location to the facility where they putatively originate, for example, 'hacker removes web service at Telehouse, Singapore, Block 750D, Chai Chee Road'. These prose narrative events are then sent for sonification and to the text transcript interface that users can access while moving through the soundscape.

The sonification process works according to a system of rules that assign musical qualities to events according to the actors involved, impact and probability. For instance, a low probability event will play at a higher pitch. High and medium impact events are more percussive. Sonic qualities are assigned to actors based on the five elements in Chinese philosophy (metal, wood, water, fire, earth). For example, events involving governmental and civic actors are played with woodwinds under the classification of Wood equating to 'all actors, civil, legal'. Those involving military or activist actors ('anything metallic, weaponry, defence, boisterous, violent') are played on metal instruments such as gongs or xylophones. Those involving social media are associated with Water and played on string instruments.

To supplement these procedurally generated sonifications, other events were also triggered by real network activity. Mod built the Data Farms backend as a web service drawing on both the Neo4j data model

and a network security service monitoring Border Gateway Protocol (BGP) incidents. BGP messages are received by data centre hardware to clarify available network routes. Where network hijackings or outages occur, the system draws on incident reports to generate short synthesised sonifications with atonal rhythmic qualities. This feature was developed to spotlight network incidents at the specific facilities in the Data Farms data model but was later widened to consider incidents anywhere in the world so that the public user experience would always include some BGP sonification (of the most recent incidents anywhere in the world).

The Data Farms public experience (the sonification) plays on a timed loop and resets with a break after each session. Events play randomly according to probabilities programmed into the model. However, each session includes at least one low probability, high impact event to illustrate the range of sonification options and give a loose narrative structure to the user experience. Consider a rare event such as boat cuts internet cable, an incident with dire consequences for data centre operations. The sonification will play with metal and string instrumentation accompanied by a high pitch drone for low probability and percussion for high impact.

User Experience

In an installation setting, users would view a large screen displaying a brief curatorial message about the sonification before entering the soundscape. As they wait for other users to complete their experience, the same screen displays the textual event log generated by the data model. Data Farms is a real-time spatial audio multi-user installation designed for headphones. The sonified data used in each session is procedurally generated from the data model – no two sessions are the same. While a session's overall composition is the same for all active users, the sonification is different for each user, based on how they physically move in relation to the virtual 3D soundscape. Walking through the installation gives the sensation of moving through different virtual 'territories'

as passing between defined areas of the soundscape triggers changes in orchestration.

Users enter the installation with their device held comfortably in front of them and with headphones plugged in. Each user must scan a central marker (e.g. QR code) to initiate the experience. Physical movement in relation to this origin is translated into movement through the virtual soundscape. A challenge identified from user feedback is the tendency for visual outputs on the device screen to interfere with the sonification experience. Screen cues are thus kept to a minimum.

A tension exists between musical and compositional strategies of the sonification, on the one hand, and its information transfer goals, on the other. A design-centred approach configures the sonification less as an instrument of research inquiry and more as media art – a medium for an audience with expectations of a functional and aesthetically pleasing experience. The question of how the user experience leads audiences to reflect on infrastructural power and the social, cultural and economic relevance of data centres remains open.

Afterlife

It is a strange prospect to discuss the afterlife of an installation permanently stalled by the pandemic. In many ways, the sonification has yet to see the light of day. Yet there is the possibility to make the application available online as a downloadable AR experience. The Data Farms web service itself (including an application programming interface, the data model and network monitoring services) can also be made available. A more costly option is to migrate the mobile AR experience to one that can be experienced online as a multi-player equivalent to the location-based experience we intended. Built on the Unreal Engine, this could involve the use of Pixel Streaming (WebRTC) technology so that any desktop web browser could be used to access the same virtual soundscape and hear the interactions of multiple users. Extended Reality (AR, VR, MR) is a fast-evolving field and Covid constraints suggest new directions for supporting both location-based and online audiences.

The Data Farms sonification is an artefact of collaboration between critical academic researchers/theoreticians and creative programmers/producers. The application bears the marks of this relationship, particularly the difficulties of translating empirically driven conceptual research into technical and informational formats that require strong internal consistency and interoperability between platforms. The question of what data could or should be sonified also haunts the collaborative process. The breakthrough moments were surely earned through episodes of frustration. In the end, what matters is the sound.

Download the sonification videos at https://www.datafarms.org/documentation

Images (above and opposite) Ned Rossiter


Warning: This is NOT
a Safety Barrier

Data centres reside in the middle of nowhere but connect to everywhere. They are often positioned in rural or peripheral nowhere lands yet run global connections from these locations. In the densely packed city of Hong Kong, the data industry is one of the competitors for space. It has discovered that old warehouses in logistical districts can be repurposed to serve the needs of the so-called platform society. The blind walls of warehouses-turned-data centres leave us speculating about their operation. Here I discuss how *peripherality* turns into *centrality*, *storage* gives way to *flux* and *voice* becomes *data* at the site of the data centre.

Centrality/Peripherality

Nicole Starosielski notes that turbulent ecologies contain chaotic social and natural forces that can interfere with the infrastructural operations of data centres and datacentric industries. To counter this, strategies of insulation that control or eliminate such forces are in place. As regards the data centre, fail-proof connectivity first requires disconnecting the contiguous: immediate environments and elements that pose a threat to the stable operation of the data centre. Hence, the location of a data centre is carefully considered. For instance, it may be important that there is no operational factory in proximity, yet a nearby fire station may be an asset. Although there are examples of 'downtown' data centres, designated data-centre parks in Hong Kong and elsewhere are typically placed at the urban periphery, in older industrial and logistical districts, rather than in the central business district. And, as the data centre's steady hum must go on, a reputation for stability and public order is an asset. Of course, cities building data centres, including Hong Kong, do manifest social tensions. Ironically, it may be the case that during the Umbrella Movement of 2014, protesters were able to occupy Hong Kong's central business district for an extended period of time, partly because the data centres were located elsewhere and hence the operation of the city's critical infrastructure was not threatened.

Part and parcel of the strategies of insulation are aesthetics that disconnect our attention and direct our gaze away from data centres. The latter are often made to look inconspicuous and nondescript, blending in with the non-digital warehouses of logistical districts for instance. Their generic design – a simple block lacking windows – seems the most literal instantiation of a technological black box that does not allow us to explore its inner workings. If we happen to throw a glance (but who really would?), blank walls merely stare back at us. The data centre poses as a kind of warehouse that holds society's memory, which is increasingly externalized and mediated due to ubiquitous computing and the accompanying shift to the cloud. Yet the data centre's own architecture is often hardly memorable. Eye-catching logos are avoided, though subdued decoration may feature colour schemes that hint at the identity of the corporation running the centre. Through such means data centres seek a balance between advertising for the purpose of attracting customers and remaining inconspicuous for security purposes. Some data centres keep their locations secret, only revealing the broader area in which they are located; others have their addresses available online as part of their sales pitch and they are directly mapped, for instance by the aggregating site datacentremap.com. Moreover, tours are organized for potential customers. Yet data centres are not public institutions abiding by codes of transparency and whomever wants to have a peek will be screened first. The combination of endeavouring visibility/distinction and obscurity/genericness results in occasional paradoxes revolving around advertising secrecy and branding inconspicuousness. Perhaps one strategy to negotiate the double bind is to follow the example of Google and simulate the data centre online as a hypervisible spectacle, as Holt and Vonderau point out.

Next to insulation and disconnection, data centres also draw on certain occurrences of proximity and manufacture specific patterns of connectivity. The once rattling physical trading floor of the Hong Kong Stock Exchange in Central has been turned into a museum, as all trade takes place virtually nowadays. Consequently,

a data centre advertises its proximity not to Central but to Tseung Kwan O in the New Territories, where the data centre of the Stock Exchange is located. This suggests that while peripheral in urban terms, data centres can nonetheless hold a central spot in infrastructural networks. If represented in multiple countries, data service providers advocate their specific regional or global networks. For instance, in Hong Kong, one data centre advertises its presence in all major financial hubs in Asia, supposedly offering the shortest possible, direct route and a highly reliable connection via the Asia Submarine-cable Express. Another data centre emphasizes its 'premium network gateways of high connectivity' with Mainland China. Data centres differ from analogue libraries or archives in that the latter tend to concentrate resources in support of knowledge production at a particular site, historically the capital of a state or empire. Data centres, on the other hand, facilitate networked production of information through relations across the globe spanning cables, data racks and servers that both transform and elude social power.

Flux/Storage

According to Robert Gehl, the separate yet inter-operable functioning of 'archive' and 'processor' have informed the defining architectural features of computers since the 1940s. Key in John van Neumann's computer design was that data and programs were stored in a memory unit while the processing of the data and the execution of the programs became the work of the processor. This enabled the flexible adaptation of computers to new tasks: mass storage could be interfaced with different programs to process data. Data centres are a continuation of this history. Partaking in the modular character of the internet as stack, the data centre as an archive is separate from, yet inter-operable with, heterogeneous data processing techniques. Moreover, data centres are replacing in-house IT departments and such outsourcing allows for flexible expansion and contraction for corporations, while new services can be added. Hence, to draw from Rob Kitchin, there is *IaaS* (Infrastructure as a Service), which only

offers storage capacity for cloud computing, leaving the choice and operation of the software to the customer; *PaaS* (Platform as a Service), which in addition manages the operating system layer by offering an execution environment to develop custom applications, such as smart city portals; and *SaaS* (Software as a Service), which furthermore manages the application layer and comes with company software that users access through their browsers and use remotely.

These *PaaS* and *SaaS* solutions can connect employees, supply chain partners and Internet of Things cityscapes alike, enabling new techniques of control, surveillance and extraction. Data is often generated without any purpose being specified in advance. It becomes valuable and meaningful when massive volumes of heterogeneous data are interlinked across racks and centres. Geoffrey Bowker contends that such archiving techniques constitute 'potential memory' from which an (open-ended) series of facts and narratives emerges. Meanwhile, the energy required to uphold the potentiality of memory is huge and raises questions about its supply, even when renewable energy is at stake. In Hong Kong, fifty percent of the overall energy derives from coal and eleven percent from the Guangdong Nuclear Power Station at Daya Bay, which resides at merely fifty-kilometre distance from the densely populated areas of Hong Kong. In 2015, it was discovered that the plant's alarm system had remained turned off for a period of three months – by mistake. Whereas at the time of its construction in 1986, following the Chernobyl disaster, a million people reportedly protested the development of the plant, Hong Kong's data centres nowadays hum on quietly without discriminating the energy source.

Data/Voice

In the smart city, data-driven governance redistributes perception, memory and cognition across different actors including corporations such as IBM, local institutions such as urban governance actors and citizens and consumers. Traditional governance actors are provided with dashboards that model and represent urban processes in

particular ways. Next to that, users as citizen-consumers mostly relate to data infrastructure via apps. When users as citizens or consumers engage with the interfaces of data-driven governance, their agency is often channelled toward more or less prescribed data input and responses. In Hong Kong, the government has spent HKD$38 million on the development of 127 apps as part of its smart city initiative, but open data activists argued that rolling out such apps is decidedly different from releasing datasets in 'open' and machine-readable formats. While Hong Kong's open data efforts in some ways have been strengthened over the years, the access to datasets for critical and civic purposes has diminished in others. For instance, the journalist Bao Choy was convicted for making false statements when requesting license plate information for a documentary investing the violence committed against pro-democracy protestors in Yuen Long district in 2019. Whereas the government boasts about the quantity of data that it is offering in open format, such numbers do not reflect opportunity for civic voice, which may require data of a different nature than what is available.

As populations become managed as data, data centres are modern-day heterotopic spaces that are by and large insulated from society and public life. Here data bodies are stowed away; their lives in the racks remain simultaneously unseen and surveilled. Despite the global impact of EU's General Data Protection Regulation (GDPR), in many places the law still offers little protection for the data bodies of their citizens and the global scale of data flux seems rather incompatible with territorial legislation anyway. After all, data is routinely trafficked across borders and such movements are often hard to trace. In Hong Kong, datacentric industries are a key component of plans to integrate the Greater Bay Area, implemented by the Hong Kong government with support from Beijing and in collaboration with cities in Guangdong Province. But do data mobilities abide by the 'One Country, Two Systems' principle? Critics have found that despite legal incompatibility between the two 'systems', there is weakened control over cross-border

transfer of user data because provisions to protect personal data are not yet in force and its definition remains underdeveloped. But excessive traffic can also constitute a weapon targeting specific data bodies. In June 2014, the Hong Kong website popvote.hk experienced what was according to some the largest DDoS (Distributed Denial of Service) attack in history. The website was being prepared to host an opinion poll, or non-binding referendum, on electoral reform, which also was the key issue that triggered the 79-day occupations constituting the Umbrella Movement later that year. According to reporting by Global Voices, the service providers supporting the website, namely Amazon Web Services, UDomain and Cloudflare, were forced to suspend their services. Yet only Cloudflare resumed support for the website afterward. The DDoS attack was meant to silence voices-turned-data, yet who would be responsible for the safety and rights of such data bodies under these circumstances? *Homo sacer* data bodies are free to roam through global networks, yet they are also outcasts, by and large deprived of rights and protections.

Image (opposite) Ned Rossiter


SEC
錄錄監控現正進行
攝錄影像將依照
個人資料(私隱)條例處理
Video surveillance is in operation
Collected images will be handled in accordance with
the Personal Data (Privacy) Ordinance
FUEL TANK
ROOM F
油缸F房
D
G
BEWARE
OF
SUFFOCATION
小心窒息
H F P
(FM 200)
七氟丙烷氣
CAUTION
小 心
This area is protected
by a FM 200 fire
extinguishing system
此處設有 FM 200 滅火系統防護
When alarm sounds
or upon gas discharge
evacuate hazard area
immediately
當警鐘響動或氣體發放時,
應即撤離現場

Images (above and opposite) Ned Rossiter

CAPITAL OPERATIONS: DATA AND WASTE

Brett Neilson

Borders are indispensable to capital's formatting of the world. As social institutions, borders not only mediate relations of capital and state but also establish boundaries, limits, interfaces and zones that register the profound transformations effected by capital's operations across and beyond existing territorial demarcations. The town of Tseung Kwan O in the New Territories of the Hong Kong Special Autonomous Region (SAR) is a site that bundles and multiplies these changes and variations. This restless spatial reorganization is most evident in the borders that separate its data centre cluster, waste dump and the nearby LOHAS Park real estate development.

Tseung Kwan O hosts one of the largest commercial data centre clusters in the world. Located on reclaimed land close to undersea cable landings and linked to digital infrastructures that support financial trading on the opposite shores of Hong Kong Island, the site is a crucial gateway and switch-point between the mainland Chinese and global data environments. Tseung Kwan O is also the site of one of Hong Kong's main waste dumps, the South East New Territories (SENT) Landfill. Close to capacity and under pressure from population density and land prices, the dump abuts the data centre cluster in the Tseung Kwan O Industrial Estate. This complex of spatial and infrastructural relations creates a series of borders that both crisscross the area and extend beyond it. To conceive of Tseung Kwan O as a borderland is to probe divisions between East and West, liberalism and state capitalism, data and waste.

Tseung Kwan O is a borderland because it hosts facilities that draw in materials from wider geographical vistas, creating opportunities for aggregation, treatment and analysis. In the case of the SENT Landfill, these materials are designated as waste, and although their origins are encrypted in tangled webs of supply, they are most immediately sourced from across Hong Kong's dense urban fabric. By contrast, data centres assemble electronic information, which is stored, processed and transmitted in binary form through complexly arrayed networks of digital switches. Connected to the wider

world by undersea cables, Tseung Kwan O's data centres serve clients across a potentially global expanse but derive their locational advantage primarily from their proximity to China's mainland data industries and markets.

Insofar as their operations catalyze and unsettle the production of borders, data centres index the emergence of capital as a political actor. Due to the role of data in transforming economies and social relations, these facilities function not only as technical infrastructures but also as de facto political institutions that inscribe, challenge and defend established monopolies of jurisdiction and sovereignty. Their capacity to generate topologies of power that exceed state borders crosses their material location within existing political territories and subjection to patterns of regulation and oversight that abide by geopolitical relations of national division and regional competition. Nowhere is this clearer than in Hong Kong, which, as a Special Autonomous Region of China, enjoys proximity to the mainland while maintaining a distinct economic and administrative system.

The slogan 'one county, two internets' is popular among digital activists who seek to preserve a free and open internet in Hong Kong. However, the conditions described by this phrase also give rise to Hong Kong's emergence as a data centre hub. The figure of the gateway features widely in discussions of Hong Kong's relation to the mainland, particularly regarding operations of capital and finance. Even if many of the mainland's first-tier cities now eclipse Hong Kong in terms of contribution to gross domestic product, the unique territorial situation of the SAR makes it amenable to data centre development. The gateway is a figure of the border: a device of entry and exit capable of opening and closing. Yet it is not a switch with only two settings, on and off. As figure, it invokes the possibility of filtering, speeding up or slowing down, letting some through and shutting others out, including differentially as well as excluding. The ground against which this figure emerges is the contested terrain of Tseung Kwan O. This ground is not only physically contingent, given that it is reclaimed from the sea and susceptible to leachate leakage from the

landfill, but also contingent in a social and political sense, subject as it is to urban conflicts and design protocols that privilege vertical relations of circulation and habitation above grounded practices of sociality.

The presence of the waste dump at Tseung Kwan O adds a layer of complexity to these relations. Although its adjacency to the data centre cluster is a matter of urban planning that seems fortuitous with respect to data centre operations, the proximity of the landfill creates a spectacle that beckons analysis. China's great firewall has been crucial to its data sovereignty concerns and has guided the choice of many international companies to establish data centres in the less restrictive Hong Kong. In the field of waste management, the National Sword policy, which restricted the import of recyclable waste to China in 2018, has placed pressure on Hong Kong's landfills, reshaping their operations and physical form. The border between Hong Kong and mainland China thus insinuates itself into the data centre cluster and the waste facility alike.

The Hong Kong-China land border is a porous barrier with an expiration date. Despite the presence of walls and a closed frontier area, population movements as well as the construction of bridges, tunnels, artificial islands and a high-speed rail link have tested this border as something fixed in time. Given the liberal precepts governing social and economic life in Hong Kong and the contrasting political styles of the mainland party-state, the Hong Kong-China border has become, for many, a symbol of a supposed civilizational split between East and West. In a sense, the Hong Kong protest movements of 2019–2020 can be read as a struggle for the strengthening of this border in the face of extradition and security legislation that was eventually smuggled in under cover of the pandemic.

Hong Kong's unique positioning tests the assumption that national boundaries and capitalist systems are coterminous. In the wake of China's opening to the global market since 1978, the contrast between a planned economy on the mainland and free market capitalism in Hong Kong can no longer stand. There

is a need to understand the co-evolution and deep interconnections between these economies and their role in shaping geopolitical relations, especially the wake of Beijing's plans for Hong Kong to form part of a Greater Bay Area economic powerhouse comprising also Guangdong and Macau.

Hong Kong's government has deliberately encouraged the data centre industry, setting up a Data Center Facilitation Unit in 2011 to offer advice on matters such as statutory processes and compliance requirements. Bolstered by such efforts, the emergence of the Tseung Kwan O cluster lies in earlier governmental initiatives. Ngai-Ling Sum and Bob Jessop detail two reports received by the Hong Kong government in the 1990s: *The Hong Kong Advantage*, prepared by Harvard University, and *Made by Hong Kong*, prepared by the Massachusetts Institute of Technology. The former recommended that Hong Kong should focus on financial services, and the latter suggested intense capital investment in advanced technological and manufacturing facilities. While the first path has definitely shaped the path of financial capitalism in Hong Kong, the latter did not completely disappear in terms of policy. In 2002, the government established the Hong Kong Science and Technology Parks Corporation, which runs the Tseung Kwan O Industrial Estate.

The emergence of the industrial estate links to land reclamation and development plans initiated in the early 1980s to build Tseung Kwan O as one of Hong Kong's nine new towns. The reclamation that allowed the development of the estate finished in 1997. The adjacent SENT Landfill opened in 1994, itself partially occupying reclaimed land and run by Green Valley Landfill Limited, a subsidiary of Veolia. The story of relations between the data centre cluster and the landfill often takes on secondary importance to a narrative that describes how the waste dump affects quality of life and housing prices in nearby housing estate developments, which were also part of the new town plan.

Tseung Kwan O is now home to over 400,000 residents. The data centre cluster provides a border that separates the landfill from large housing estates,

such as LOHAS Park to the north. A dense development of residential towers, some up to seventy-six stories high, LOHAS (which stands for Lifestyle of Health and Sustainability) Park consists of several complexes with names like The Capitol, Le Prestige and Malibu.

This residential arrangement packs volumetric urbanism into a tight compact of three-dimensional circulation networks that join shopping malls, transport interchanges and apartment buildings. The verticality of LOHAS Park also provides a kind of olfactory wall that absorbs stench from the SENT landfill. Although the dump receives only building waste since early 2016, the question of how fumes emanating from it interact with nearby housing occupies local activism. Protests against a proposed extension to the landfill, approved in 2014, led to tumultuous events in Hong Kong's Legislative Council, including the unfurling of a Nazi flag by a councillor. There is even a big data analysis of the landfill's impact on LOHAS Park that correlates resident complaints with rising real estate prices to conclude that publicity associated with protest draws buyers who discover that only part of the estate experiences odor. It is credible to imagine that the datasets analyzed by this study are stored in data centres in Tseung Kwan O Industrial Estate, which now houses over ten large-scale facilities run by Chinese and international companies. However, the question of how spatial proximity between data and waste informs the more general relation between the two is complex and contested.

The topographical border between the data centre cluster and the landfill cannot simply double for the conceptual border between data and waste. There is a need to ask how the operations that govern the movement, collection and treatment of data and waste respectively redouble on the physical border between the facilities in Tseung Kwan O. Data centres establish such complex relations of continuity and difference, connecting servers, clients, users and firms. A single external query can generate a massive amount of internal traffic, as servers in a facility share and extract data before coordinating and returning a response.

Waste circuits also configure a two-way relation between extensive relations that bring distant objects and sites into proximity and intensive practices of collecting, sorting, dismantling, recycling and so on. Changes of intensive formatting, such as the restriction of the SENT landfill to construction and demolition waste, radiate out. But variations from afar can also affect local practices, as became evident in Hong Kong when the mainland introduced the National Sword policy, leaving the city to cope with a deluge of refuse that otherwise would have moved across the border.

Given the propensity of both data and waste circuits to support fungible schemes, we can ask how the topography of geographical location crosses the topology of network variations in the generation of economic value resulting from these circuits as well as from their intersections. Such a style of analysis means not only probing how the production of space inflects the circuit of capital. It also implies investigating how capital's operations tangle with each other to produce variegations of capitalism such as those that straddle the Hong Kong-China border while also sculpting distinct contours of extraction, exploitation and accumulation in different material locations.

In considering the relations among data and waste, a focus on bordering takes us beyond casual parallelisms: cataloguing the useless information stored in data centres, tracing the role of data analytics in waste management, quantifying the energy burnt keeping backup diesel generators idling over in data centres, understanding spam economies and so on. These are all worthwhile empirical projects, but lest they merely affirm visions of waste as rubbish, trash or excess, we need to inquire how the economies they support operate in the nexus of spatial relations. In this way, we can discern how digital infrastructures articulate operations of capital to changing geopolitical formations.

A longer version of this text was published by *e-flux Architecture*.

Image (opposite) Ned Rossiter


DO NOT STACK

Images (above and opposite) Ned Rossiter


PSB
PSB
PSB

011

THE DISPOSITIF OF DISTRIBUTION AND THE GEOPOLITICS OF DATA

Florian Sprenger

With the rise of smart media, the internet of things and ubiquitous technologies in the last decade, the power of calculation has been transferred from isolated, locally bound end-devices into environments on a large scale. 'Everyware', as Adam Greenfield termed these technologies, operates spatially independent in a network and is at best context-sensitive on the basis of large amounts of sensorial data collected by end-devices. Beginning with the establishment of mobile laptops and tablets, popularized globally with the smartphone and projected with the rise of the internet of things, digital technologies gain more and more independence from geographical space and transform our environments into spatially distributed networks. At least this is what companies tell us and what users experience. The infrastructural foundations of this process might reveal another outlook. Computers evidently have not only become devices of daily use but migrate into more and more objects that communicate with each other. The technical permeation of our surroundings nevertheless depends upon external storage and centralized processing powers because miniaturization and automatization foster the construction of smallest components with few applications but a high degree of interconnectedness. The centres of these processes are data centres.

In the face of the enormous amounts of data and the comforts of ubiquitous access, almost no new gadget abstains from cloud services and externalized data storage. The mechanisms of economic extraction that are connected to these technologies are based on a centralized analysis of collected user data. The foundations of this new dispositif of digital cultures are not only infrastructures of distribution that enable mobile addressing and constant availability in the form of digital networks. Rather, an intensification and centralization of more and more ambitious services takes place in the background. Many of the developments of the internet of things abstain from local storage and these services have no place and no time on the user's devices themselves. But not only users utilize data centres, often without noticing. Many institutions and companies outsource storage capacities to external

providers which have the necessary knowledge, promise data security and in the end turn out to be economically more favourable than local, company-owned data centres. The service of data centres has become a global industry – big players afford to build their own network of data centres, others rent capacities from external suppliers. Today, computing at the edge, that means in spatial distribution, mobile and miniaturized, is possible only when it is accompanied by computing at the centre. Data centres turn out to be a signum of our present.

But what exactly happens with data in data centres remains opaque – not only because their operations are kept as an industrial secret but also because data at the core of a data centre are invisible. There is no public in a data centre – customers don't know each other and can only be connected by the providers. The windowless buildings with metal panelling, usually huge boxes with two walls for optimized heat isolation, prevent any view of the inside. On the rare occasions at which a company gives access to these hallways, only endless server racks and the measures for their protection become visible – secured against fire, earthquakes and terrorist attacks. The huge rooms with servers never sleep and don't know night-time. All the more important it is thus to develop a conceptual language to cope with the geopolitical and media-technological dimension of these interconnected phenomena. What makes them so decisive for our present and the near future are not only the new uses and applications, but a new entanglement of space and technology. The centralized storage of user data and their consequential examination, the restructuring of software, and the ubiquitous availability of data raise a series of media-theoretical questions reaching from possible surveillance to the reterritorialization of national territories through extraterritorial data centres.

In this sense, the triad of storage, transmission and processing can help us to understand the operational modes of data centres at least heuristically. That data centres may offer all three modes in a bundle, and that this combination accounts for their productivity, does not mean that the distinction between these three operations

becomes obsolete. Rather, this triad, which was introduced as the basis of his technologically oriented media theory by Friedrich Kittler referring to the computer architecture developed by John von Neumann, can lead us to an attempt to classify the different operational modes of data centres.

Storage and backup, availability and accessibility are only a customer-friendly offer that hides its materiality under the name of the cloud. Data centres are also used for the postprocessing of data, for the analysis of big data, and for the local convergence of datasets between cooperating institutions or companies. Cloud-based software such as Microsoft Office 365 or Adobe Cloud Services transform the supply of software into a service that is provided on centralized servers and not on local computers. No social media, no online shopping, no video streaming, and no NSA-surveillance without data centres and their capacity for data processing. But also, the transmission of data through digital networks hinges upon respective infrastructures: every internet node is a data centre at which, during the act of packet switching, data is temporarily stored for further distribution (and possibly surveillance).

The centralization fostered by data centres is bound to the massive distribution of networked devices without storage, because storage takes space and is inert. The outsourcing of intensive processes of storage, calculation, and energy into data centres is one of the presuppositions of the distribution of devices. The smart objects of the internet of things and cloud-based smartphones are bound to data centres and constantly exchange data. This centralization is also an economic concentration on the big five Amazon, Apple, Facebook, Google and Microsoft. The geopolitics of data is an element of the chains of value extraction of digital networks. It is no coincidence that Amazon is the largest supplier of cloud services for institutions and companies. Centralization, in this sense, is also an economic model. These processes of concentration undermine the common idea of democratization through digital networks and thus contradict the supposed horizontal alignment of geographical differences.

Accordingly, the material signum of our times are not only mobile devices, but also data centres and the resulting separation of data collection and data processing. The billions of end devices in the hands of users are confronted by a few gigantic server farms. What appears as a cloud to the users and makes services such as search engines, music and video streaming, online shopping and social networks possible is a complex and capitalized ensemble of millions of servers with specialized software and often also self-designed hardware. Such data centres, called 'landhelds' by Google because of their demand for land, determine the connectivity of handhelds. Bruce Sterling calls the actors and winners of this process of concentration stacks: vertically integrated companies, whose business model consists in the constant economic utilization of data from users who use their infrastructure. To sustain this process, the stacks need influence both at the endpoints of devices, gadgets and sensors, and capacities for data analysis in the background of the cloud.

Data centres are places both of acting with data and of dealing with the possibility of acting with data. Depending upon their geographical location, their technical configuration and their target groups, they offer different modes of operation with data. They can accomplish all the tasks that a personal computer offers regarding the data on its hard drive, but they also offer the chance of cross-connecting locally stored data – apart from their quantities of storage and the speed of processing itself.

For each of its different modes of operation, the productivity offered by data centres is based on the local storage of data – that means on their collection at a centre and the materiality of their availability. Data centres can exist without a network, without external access and without the possibility of cross-connection. But the common denominator of all data centres is the local concentration of data of different heritage. This concentration is bound to the de-centralization that digital networks brought with them and that reaches a new stage of escalation with ubiquitous media and the internet of things.

These different options offered by data centres to handle data cannot be separated from their spatial relations: data centres are centres at which decentralized distributed data are collected at one place. For this reason, the selection of an advantageous location is so important: on the one hand are the climatic conditions and the energy resources of the location, on the other hand is the connection to existing networks, for example undersea-cables or important internet nodes. In this sense, a breakdown of the different uses and operations of data centres should include an analysis of the spatial relations of data. The infrastructural characteristic of a data centre consists in the fact that it offers access here and there: as a cloud-service or as software-as-a-service, as a platform for streaming or as a centre of calculation for the internet of things, as low-latency-processing or big data-analysis – the centres at which data centres centre data are local to be global, and accessible all the time from every location – downtimes and maintenance notwithstanding.

In this regard, the analysis of the spatial relations brought forth by data centres should include a discussion of the materiality and temporality of their infrastructures. The term data centre itself implies the materiality of data, since immateriality has no centre – it is everywhere at once. Such centrelessness is often attributed to supposedly immaterial digital networks that in fact are material through and through. Information seems to have no weight, to be independent of its location and distribution in time and space. But there is no data without carrier, no message without a medium that binds it in space and makes it addressable in time. It is no coincidence that the increasing general interest in infrastructures and their materialities goes hand in hand with the importance of data centres for digital cultures – to think about the digital remains shallow without accounting for the infrastructures of its distribution.

Seen on this level, data centres are both centres of data at which they are collected and centres at which they are accessed and processed. They are, in other words, archives and information desks at the same time. They are centres of data and centres for

data. In both cases they are infrastructural centres in a decentralized network. As centres in a network, they are the condition for the further diffusion of the network. While the historical development of this network was propelled by an imperative of decentralization and finally of distribution, as obvious in Paul Baran's famous network diagram, the importance of data centres can be understood as a counter-movement towards centralization – and consequently also to proprietarization – of data and infrastructures. From the start, the architecture of the internet was construed to ensure redundancy by the multiplication of nodes. The attempt to make data accessible from different locations meant to optimize the number of possible connections between nodes in a way that guaranteed low costs and stability. Though this did not result in an egalitarian distributed network as imagined by Baran to prevent the nuclear destruction of central nodes, even the distributed internet of the present, in which several nodes gather large amounts of traffic while many small nodes remain insignificant, is formed by a spatial distribution which creates stability via redundancy. This structure is currently transformed by a new geopolitics of data whose centres carry the contrary tendency in its name (even though many providers promise to mirror data at different locations so that data centres themselves are interconnected).

For the logic of the Cold War, which still lingers in the background of these developments, data centres seem anachronistic. Locations of centralized calculative power, such as Singapore or Hong Kong, make excellent targets for possible attacks on global infrastructures. Their destruction would result in a chain reaction of crises and cut off the global distribution of data. Even when governmental order is totally disrupted, security of data is supposed to be assured. These examples are not intended to call for the real danger of a nuclear war but help to situate the current meaning of data centres for the architecture of global connectivity. With the new infrastructure of concentration, the old scenario of crisis returns, which becomes visible in the self-descriptions and advertisements on the homepages of data centres:

the latent crisis, which is the background to the attempts of the providers to secure redundancy of data, can grow into an imaginary apocalypse quickly. Data centres sustain their evidence from their presumed security: data centres are necessary because they can be destroyed, not because they cannot be destroyed. It is this destruction, in which the loss of all data would result in the end of the world, that forces digital cultures to be constantly engaged in preparations.

Taking these introductory observations as a background, a media-theoretical analysis of data centres can be oriented towards three complexes of questions:

1. **What are the spatial relations that these technologies create? If data centres are both political institutions and digital infrastructures, then they realize new modes of power. How can we in this sense refer the relation of data centres to their networks on the relation of surroundings and surrounded that is central for current technologies?**
2. **What are the modes of operation of data centres? Under which conditions do they store, process and transmit data?**
3. **How can we describe the imaginary that goes hand in hand with data centres as dominant technologies? The fact that the world's largest data centre is run by the NSA needs special attention in this context: the dream of a transparent universal archive gains a new dimension with data centres. But this imaginary is at the same time haunted by the apocalypse.**

These preliminary questions stake out the field on which a media-theoretical investigation of data centres could be based. Such investigations are possible only as collaborative projects: the digital cultures of the present cannot be reduced to social or technological questions. Consequently, the materiality of their infrastructures is bound to the imaginary of their evidence.

Images (above and opposite) Ned Rossiter

Data

Data is not given. Data is always cooked, even when it's raw. Data is hoarded, processed, and transmitted. Data is media, but it also portends futures predetermined by patterns. Data is both pattern and plan. Data indulges in queries. Such probes or declarations allow data to be arranged relationally, to be farmed, milled, and modelled. Data becomes information by virtue of patterning and not content. Data unhinges from its base. Data plots for correlation but eludes proof or cause. Like labour and capital, data is extracted and exploited. Data serves. Data is not master. Data is not sovereign, power is.

数据

数据是不给的。数据总是被煮熟的，即使它是原始的。数据被囤积、处理和传输。数据是媒体，但它也预示着由模式预先确定的未来。数据既是模式又是计划。数据沉溺于查询中。这样的探测或声明允许数据被关系性地安排，被耕种、碾磨和建模。数据由于模式化而不是内容而成为信息。数据从它的基础上解脱出来。数据绘制了相关的图画，但没有证据或原因。像劳动和资本一样，数据被提取和利用。数据服务。数据不是主人。数据不是主权者，权力才是。

Farm

Farms manipulate environments to cultivate growth and maximize yield. Two conditions are necessary for farming: land and water. From the neolithic revolution to genetic modification, these variables have been constants. Hydraulic empires have mutated into sites of monocultural extraction. Whatever the yield, farm produce is siloed and processed into usable form. For the physiocrats, farms produced the wealth of nations. Today farming is a game of accumulation that generates its own territories and borders. Farms require labour, beyond the machine. We need a new *tableau economique*.

农场

农场操纵环境以培养增长和最大限度地提高产量。耕作有两个必要条件：土地和水。从新石器时代的革命到基因改造，这些变量一直是不变的。水力帝国已经变异为单一文化的开采地。无论产量如何，农场的产品都被储存起来，加工成可用的形式。对于生

理学家来说，农场产生了国家的财富。今天，农业是一种积累的游戏，它产生了自己的领土和边界。农场需要劳动力，超越机器。我们需要一个新的经济表。

Circuits

Circuits cut through territory, making it anew. Circuits define data's territorial reach, and then expand beyond this ambit. In today's capitalism circuits are directly productive. Without circuits data goes nowhere. Control of circuits does not *ipso facto* imply control of data. Circuits control resistance, yet resistance is the underside of control. When circuits are broken, transmission ends. Circuits are underwritten by the abstract nature of the forms that propel circulation. Circuits are not cycles. Circuits do not lead back to where they began. Circuits are not infrastructures of totality.

循环

线路切开领土，使其焕然一新。电路定义了数据的领土范围，然后又扩展到这个范围之外。在今天的资本主义中，电路是直接的生产力。没有电路，数据就无从谈起。对电路的控制并不当然地意味着对数据的控制。电路控制阻力，但阻力是控制的底层。当电路被破坏时，传输就会结束。电路是由推动流通的形式的抽象性质所支撑的。电路不是循环。线路并不回到它们开始的地方。电路不是整体性的基础设施。

Territory

Territory organizes power across spatial scales and technical systems. Territory has legacies, even if they are unforeseen. Territory cannot be reproduced. Territory has no simulacrum. Zone, corridor, concession, enclave – these are names for global territories that parallel and rival the territorial forms of the state. Data makes territory of its own accord. But data is also increasingly territorialized, subject to sovereign prerogatives that limit its scope. The tension between data's territorializing capacities and its subjection to existing territoriality crosses political struggle today.

领土

领土跨越空间尺度和技术系统来组织权力。领土有遗产，即使它们是不可预见的。领土不能被复制。领土没有模拟物。区域、走廊、特许权、飞地--这些都是全球领土的名称，它们与国家的领土形式并行不悖，并与之抗衡。数据以自己的方式制造领土。但数据也越来越领土化，受到限制其范围的主权特权的制约。数据的领土化能力和它对现有领土性的服从之间的紧张关系贯穿了今天的政治斗争。

Labour

Labour is not work. Labour is the name of subjectivity under the domination of capital and state. Labour is animated by energy, unrest and movement. Labour inheres in bodily and cognitive relations. Labour is subject to abstraction that seeks to reduce it to temporal measure. The tension between abstract and living labour constitutes political struggle. This tension crosses bodies and souls. Labour sits at the client end of server relations. It contributes to the heterogenization of global space even as it is subject to intensification and diversification. Labour time is real-time. Living labour has no time.

劳动

劳动不是工作。劳动是在资本和国家的支配下的主体性的名称。劳动是由能量、动荡和运动激发的。劳动存在于身体和认知的关系中。劳动受制于试图将其还原为时间尺度的抽象化。抽象劳动和活生生的劳动之间的张力构成了政治斗争。这种张力跨越了身体和灵魂。劳动位于服务关系的客户端。它为全球空间的异质化做出了贡献，即使它受到了强化和多样化的影响。劳动时间是实时的。生活劳动没有时间。

Topology

Topology arranges architecture. Topology articulates changes in structures and spaces of power. Data centres fold topologies into networked forms: fixed or flexible, tree-based or recursive, optical or hybrid. Topology turns media and machines into systems of organization. Topological space modulates territory in ways that conform to parameters. The politics of space rubs against the grain of code. Topology tests the boundaries between physics and logic. Topology specifies how

signals act on networks. Topology engulfs forms in their own variation.

拓扑学

拓扑学安排了建筑。拓扑学阐明了权力结构和空间的变化。数据中心将拓扑结构折叠成网络形式：固定或灵活，基于树或递归，光学或混合。拓扑学将媒体和机器变成了组织的系统。拓扑空间以符合参数的方式调节领土。空间的政治与代码的纹理相摩擦。拓扑学测试了物理学和逻辑学之间的界限。拓扑学规定了信号如何作用于网络。拓扑学将形式吞噬在它们自己的变化中。

Ontology

Ontology excludes. It shares with territory parameters that define domains. The ontology of data centres catalogues relations between things in time and space (Kittler). Ontology compartmentalizes variables needed for computation and arranges them in layers. Ontology allows machines to think without interference of humans. Ontology provides representations of terrains that follow functions. Ontology does more than classify. Ontology declares authority over contingency, yet contingency unsettles the security of ontology. Topology tolerates faults. Ontology casts them aside.

本体论

本体不包括。它与定义领域的领土参数共享。数据中心的本体编列了事物在时间和空间上的关系（基特勒）。本体将计算所需的变量分门别类，并将它们分层排列。本体论允许机器在没有人类干扰的情况下进行思考。本体论提供了遵循功能的地形表征。本体论所做的不仅仅是分类。本体论宣布了对突发事件的权威，然而突发事件却使本体论的安全性受到影响。拓扑学能容忍错误。本体学将它们抛在一边。

Switch

The switch controls. On/Off. But there are consequences of the switch beyond its control. Switches foster monopolies and congestion. Switching is neither substitution nor exchange. Data centres link switches to switches: top of rack, end of rack, core switches, edge switches, aggregation switches, distribution switches,

access switches. Switches are not routers. Switches create networks. Routers connect networks. Switches are enslaved by binary logics. Even if they are analogue, they cannot mediate between their settings. Switches have no capacity for synthesis.

开关

该开关控制。开/关。但开关也有其控制之外的后果。开关促进了垄断和拥挤。交换机既不是替代也不是交换。数据中心将交换机连接到交换机：机架顶部、机架末端、核心交换机、边缘交换机、聚合交换机、分配交换机、接入交换机。交换机不是路由器。交换机创建网络。路由器连接网络。交换机被二进制逻辑所奴役。即使它们是模拟的，它们也不能在其设置之间进行调解。交换机没有合成的能力。

Packet

Packets venture across time and space. They are probes into the world. Packets decide through protocols, which govern the destination and arrival of data. Packets prompt decisions but do not make them. The relation between a packet and its externalities carries no residue. Pathways consist of switch-points without a trace. Preference is given to packets whose contents are known (Sprenger). But data acquires meaning from its relations and not its content. Packets travel independently of their capacity to give meaning or make form.

Packets can be taken, but never given.

数据包

数据包是跨越时间和空间的冒险。它们是进入世界的探测器。数据包通过协议来决定，这些协议管理数据的目的地和到达。数据包提示决定，但不做决定。数据包和它的外部性之间的关系没有任何残留物。路径由没有痕迹的交换点组成。优先考虑那些内容已知的数据包（Sprenger）。但是，数据从其关系而不是其内容中获得意义。数据包的旅行与它们赋予意义或形成形式的能力无关。数据包可以被拿走，但永远不会被给予。

Port

Ports are either opened or closed. They bridge systems and traffic data. Ports do not terminate movement, they harbour connections. Ports transform the materials that

pass through them. They are not only media of exchange but also infrastructures of change. Ports join servers into topologies. Ports have standards that proliferate differences. Ports are transport protocols with assigned numbers. Ports can be registered or ephemeral, which is to say only temporarily allocated. Firewalls close ports. Routers configure networks by port forwarding. Ports can be pinged. Once data passes through a port, it can be traced.

端口

端口要么打开，要么关闭。它们是系统和交通数据的桥梁。港口并不终止流动，它们是连接的港湾。港口改变了通过它们的材料。它们不仅是交流的媒介，也是变化的基础结构。港口将服务器连接成拓扑结构。端口有标准，使差异扩散。端口是具有指定编号的传输协议。端口可以是注册的，也可以是短暂的，也就是说，只是临时分配的。防火墙关闭端口。路由器通过端口转发来配置网络。端口可以被ping。一旦数据通过一个端口，它就可以被追踪。

Point of presence

Point of presence is the guard to entry. Data centres valorize point of presence as territorial distinctions. Without point of presence capital has no connection and is without peers. Point of presence duplicates content and multiplies storage. Point of presence is an interface. You will never see its design. The point of presence is the switch to distribution. Points of presence are both on the ground and in the air. They are hardware and signal, each governed by protocol. Points of presence anchor ontology to space. The point is that with no part, a site of meeting without division.

临场点

存在点是进入的警卫。数据中心将存在点作为领土的区别来评价。没有存在点，资本就没有联系，就没有同行。存在点复制了内容，增加了存储。存在点是一个界面。你将永远看不到它的设计。存在点是分配的开关。存在点既在地面也在空中。它们是硬件和信号，每一个都受协议的约束。存在点将本体固定在空间上。点是没有部分的，是一个没有分裂的聚会场所。

Server

Servers do not wait, they store and transmit. Servers are polysexual machines – they connect and infect without discrimination. Servers make everything a service: software as a service, platform as a service, infrastructure as a service. Servers are legalised rent machines with a license to extract and exploit on the premise of exchange. They are hooked on economies of abundance. Servers automate services, dispensing with the labour of inspection. Data centres arrange servers in racks and rows. But servers never simply stack. Servers make stacks overflow.

服务器

服务器不等待，它们存储和传输。服务器是多性的机器--它们无差别地连接和感染。服务器使一切成为服务：软件即服务，平台即服务，基础设施即服务。服务器是合法的租赁机器，拥有在交换的前提下提取和利用的许可证。他们迷上了富足的经济。服务器使服务自动化，免除了检查的劳动。数据中心将服务器排列在机架和行中。但服务器从来不是简单的堆叠。服务器使堆栈溢出。

Client

Clients function through the obligation to exchange. They flip into servers according to protocols of distribution. Data centres collocate servers but dislocate machines that act as clients. Yet clients covet the placement of their servers in data centres for purposes of peering or directly connecting to other clients' servers. While clients are topologically subordinate to servers, they proliferate topographically. Servers orient geopolitics around uneven geographies of distribution. Clients are disposed from periphery to periphery. Data centers build territories and connect labour forces by spreading their client base. Client-server architectures run jobs and partition tasks. Labour vacated the scene long ago.

客户

户端通过交换的义务发挥作用。他们根据分配协议翻转到服务器。数据中心把服务器放在一起，但把作为客户的机器放在一起。然而，客户觊觎他们的服务器在数据中心的位置，以实现对等或直接连接到其他客户的服务器。虽然客户在拓扑上从属于服务

器，但他们在拓扑上也会扩散。服务器围绕着不平衡的地理分布定位地缘政治。客户端被从外围配置到外围。数据中心通过扩展其客户群来建立领土并连接劳动力。客户机-服务器架构运行工作和划分任务。劳动力很早就离开了现场。

Colocation

Colocation puts firms in cages. Server racks cross-connect through peering points. Without windows and immersed in climate-controlled air, colocation is a lonely affair. Meet-me-rooms secure data exchange, not liaisons. Colocation strives for reliability – power has backups, never insurgencies. Colocation raises the frequency of trade and lowers latency. Colocation is expansive: replicating with modules, conforming to standards, governed by protocols. Colocation scales, but only in its own image. Dedicated resources and enclosed suites attract clients inspired by constrained servers. Colocation bonds business.

主机代管

主机代管将企业关在笼子里。服务器机架通过对接点交叉连接。没有窗户，沉浸在气候控制的空气中，主机托管是一件孤独的事情。会客室确保数据交换，而不是联络。主机代管追求的是可靠性--电力有备份，而不是叛乱。主机代管提高了交易的频率，降低了延迟。主机代管具有扩展性：用模块进行复制，符合标准，受协议约束。主机代管的规模很大，但只是在其自身的形象上。专门的资源和封闭的套房吸引了受到限制的服务器启发的客户。主机代管为业务提供了保障。

Cooling

Cooling warms the outside. Data is cool. Servers heat things up. Cooling is about power. Cooling is not air conditioning, it lubricates efficiencies. Cooling is heat extraction. Data centres divide into hot aisles and cold aisles. Cooling architectures distribute air. Cooling never ends, it is continuous and comes in cycles. Thermal analysis enables data analytics. Cooling requires alcohol, even if it is never delirious. Coolants such as glycol double as anti-freeze. Servers are power hungry. Cooling optimizes fan operation. Heat is the waste of data economies. Cooling extracts.

冷却

冷却使外部变暖。数据是凉的。服务器使东西发热。冷却是关于动力的。冷却不是空调，它可以润滑效率。冷却是提取热量。数据中心划分为热通道和冷通道。冷却架构分配空气。冷却永远不会结束，它是连续的，是循环的。热分析实现了数据分析。冷却需要酒精，即使它从未神志不清。乙二醇等冷却剂可作为防冻剂。服务器很耗电。冷却优化了风扇的运行。热量是数据经济的浪费。冷却提取。

Latency

Latency is not speed. Latency separates shock from symptom. Latency conceals. Latency flaunts epistemologies of the surface even as it stays in the closet. Low latencies kill time. Low latency indexes the optimization of speed. High finance loves low latency. A melancholia prevails as the subdued claw of the digital, restless with contingency. Latency carries the promise of emancipation from the trauma of infection. Latency struggles against the time elapsed during incubation. Latency is drag. Latency attenuates.

延迟

延迟不是速度。延迟将冲击与症状分开。潜伏期是隐蔽的。潜伏期炫耀着表面的认识论，即使它停留在柜子里。低延迟会杀死时间。低延时索引了速度的优化。高级金融喜欢低延迟。一种忧郁症盛行，作为数字的压抑的爪子，不安于应急。延迟带来了从感染的创伤中解放出来的承诺。潜伏期与孵化过程中所经历的时间作斗争。潜伏期是拖累。潜伏期会减弱。

Johannes Bruder is Head of Research at the Institute for Experimental Design and Media Cultures, FHNW University of Applied Sciences and Arts Northwestern Switzerland.

Sarah Cashman is a motion graphics artist and virtual production generalist at Mod.

Maya Indira-Ganesh is Course Co-leader of the Master of AI Ethics and Society programme at the Leverhulme Centre for the Future of Intelligence.

Rolien Hoyng is Assistant Professor in the School of Journalism and Communication, Chinese University of Hong Kong.

Tsvetelina Hristova is Postdoctoral Fellow at the Institute for Culture and Society, Western Sydney University.

Michela Ledwidge is Director at Mod and specialized in realtime and virtual production.

Liam Magee is Associate Professor and Director of Engagement at the Institute for Culture and Society, Western Sydney University.

Nancy Mauro-Flude is Lecturer in Digital Media in the School of Design, RMIT University.

Luke Munn is a media studies scholar based in Tāmaki Makaurau, Aotearoa New Zealand.

Brett Neilson is Professor at the Institute for Culture and Society, Western Sydney University.

Tanya Notley is Associate Professor in the School of Humanities and Communication Arts, Western Sydney University.

Ned Rossiter is Professor of Communication in the School of Humanities and Communication Arts and Director of Research at the Institute for Culture and Society, Western Sydney University.

Florian Sprenger is Professor of Virtual Humanities at Ruhr-Universität Bochum.

Stefan Yong is a doctoral candidate in the History of Consciousness Department, University of California Santa Cruz.

Editors	Tsvetelina Hristova, Brett Neilson and Ned Rossiter
Design	Paul Mylecharane and Kim Mumm Hansen at Public Office http://public-office.info
Publisher	Low Latencies book series, Open Humanities Press, London
Printing	Wilco Art Books, Netherlands

http://datafarms.org
info@datafarms.org

ISBN (print): 978-1-78542-126-6
ISBN (PDF): 978-1-78542-125-9

Open Humanities Press is an international, scholar-led open access publishing collective whose mission is to make leading works of contemporary critical thought freely available worldwide. openhumanitiespress.org

With support from: Australian Research Council, Western Sydney University, Chinese University of Hong Kong, Singapore Management University, University of Bologna, King's College London and Leuphana University.

What is at stake in naming data centres as data farms? These installations are essentially hangars packed with computers. They congregate servers, switches and wires that facilitate the storage, processing and transmission of data in high volumes and at fast speeds. Data centres present a scale of operations, potentially planetary in scope, that intensifies and multiplies the productive and extractive capacities of digital technologies. The economic advantages that accrue to parties with servers in these installations derive not only from opportunities for peering and networking but also from inputs to client machines that may be situated at vast distance. Yet data centres have precise locations, often clustering where there is access to energy, skills, land concessions, tax exemptions or undersea cables. There are no data centres without land and water. Like the 'dark satanic mills' associated with the factories of the industrial revolution, data centres burn fossil fuels. Yet, despite these continuities with agrarian and industrial activity, the data economy generates stark figurations of territory, power and circulation.

ISBN (print): 978-1-78542-126-6
ISBN (PDF): 978-1-78542-125-9