Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States

MARYANNE KELTON, MICHAEL SULLIVAN, ZAC ROGERS, EMILY BIENVENUE AND SIAN TROATH*

In 2018 Mark Zuckerberg contended: 'In a lot of ways Facebook is more like a government than a traditional company.'[1] Similarly, in 2019 Microsoft President Brad Smith mused: 'We, as a global technology sector, need to become a trusted and neutral digital Switzerland.'[2] While corporate posturing is an element in these statements, the digital platforms were claiming or aspiring to exercise a form of sovereignty alongside the state. In this article we attempt to understand how the power of digital platforms challenges traditional conceptions of state sovereignty. We argue that the challenge arises from the power of what we define as the 'virtual sovereignty' of the digital platforms in the United States. They possess virtual sovereignty through their commercial development of and control over critical software and hardware, and the consequent effects on human behaviour. Our aim is to consider how sovereignty and power in the US might be reconceptualized to accommodate new socio-technical spaces created by the internet and mediated by digital platforms. Virtual sovereignty refers to the digital platforms' acquisition of 'infrastructural' power, which is a defining feature of state sovereignty, in the evolving virtual territories of our digital age.

Private US internet capital and digital platforms such as Alphabet (of which Google is a subsidiary), Meta, Amazon, Apple and Microsoft are acquiring forms of infrastructural power exercised traditionally by the US state. As understood by Weiss and Thurbon, as well as Mann, infrastructural power comprises: (1) extractive power, which is the capacity to permeate society, and extract and deploy resources with social consent and legitimacy. Importantly, extractive capacity comprises the extraction of both material and human resources, including for

* This article was funded in part by the Defence Science & Technology Group's Strategic Research Investment-Modelling Complex Warfighting grant DST-RA-8381 and Agile Command and Control STaR Shot Theatre-level Enhanced Strategic Awareness grant DSP-RA-11320. The views expressed here are the authors' own and in the case of Emily Bienvenue do not represent the official view of the Australian Defence Department. The authors are particularly grateful to the journal editors, the anonymous reviewers, and Gerry Redmond and Christina Mathieson for their very helpful advice.

[1] Mark Zuckerberg, cited in H. Farrell, M. Levi and T. O'Reilly, 'Mark Zuckerberg runs a nation-state, and he's the king', *Vox*, 10 April 2018, https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 14 Sept. 2022.)

[2] Brad Smith, 'The need for a digital Geneva Convention', speech delivered at RSA conference 2017, audio transcript 14.21 mins, https://www.youtube.com/watch?v=C-YvpuJO6pQ.

International Affairs **98**: 6 (2022) 1977–1999; DOI: 10.1093/ia/iiac226

example, 'mobilizing support for defensive and aggressive military action';[3] and (2) transformative power, which is the capacity to initiate, sponsor and harness substantial technological innovation for state benefit.[4] We argue that these digital actors are acquiring infrastructural power in critical internet technologies. Eichensehr's work on 'supplemental sovereigns' and Pasquale's consideration of internet companies as 'merchant sovereigns' point to messy, layered power relations among digital platforms and the state.[5] We aim to clarify some of these messy relationships by describing the respective roles of and relationships between digital platforms and state sovereignty. This article locates virtual sovereignty and the social sources of infrastructural power in the hardware and software of the digital stack: the stack being the aggregated layers of digital infrastructure comprising the human–computer interface, terrestrial sensors, local digital cellular and regional communications networks, internet gateways including subsea cables, landing points and satellite systems, and geospatial value, resource and supply chains. The stack combines human, societal, computational and physical forms.[6] We use a heterodox social science approach to the social construction of technology, which enables us to understand sovereignty, power and infrastructure in a more holistically, socio-technically informed manner, while eschewing the linearity of technological determinism.[7]

Sovereignty and power are contested concepts, and their examination in the digital stack is hampered by its opacity and amorphous nature. Our purpose is to initiate a study of virtual sovereignty by focusing on the United States and the challenges to its relatively open system. The US is an obvious choice of location to begin this study because of the origins of the digital platforms in Silicon Valley. In 2019, five of the top ten global digital platforms were headquartered in the United States.[8] As Barrinha and Renard argue, while there has been some erosion of US dominance, the global internet's root servers remain predominantly American.[9]

Public and private power in the United States are not binary opposites. The exercise of infrastructural power by the digital platforms does not necessarily mean a commensurate decline in state capacity.[10] The generation and exercise of extractive and transformative power are not zero-sum games. Networks of public and private power are dynamic and fluid, or 'messy'. Private infrastructural

[3] Linda Weiss and Elizabeth Thurbon, 'Power paradox: how the extension of US infrastructural power abroad diminishes state capacity at home', *Review of International Political Economy* 25: 6, 2018, p. 784.

[4] Weiss and Thurbon, 'Power paradox', pp. 783–4; Michael Mann, 'Infrastructural power revisited', *Studies in Comparative International Development* 43: 3–4, 2008, pp. 355–65; Michael Mann, *The sources of social power: a history of power from beginning to AD 1760*, vol. 1 (Cambridge: Cambridge University Press, 1986), pp. 1–3.

[5] Kristen Eichensehr, 'Digital Switzerlands', *University of Pennsylvania Law Review* 167: 665, 2019, p. 668; Frank Pasquale, *From territorial to functional sovereignty: the case of Amazon*, Law and Political Economy Project, 6 Dec. 2017, https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/.

[6] Zac Rogers and Emily Bienvenue, 'Combined information overlay for situational awareness in the digital anthropological terrain: reclaiming information for the warfighter', *Cyber Defense Review* 6: 3, 2021, pp. 96–9.

[7] e.g. Petter Tornberg and Justus Uitermark, 'For a heterodox computational social science', *Big Data and Society* 8: 2, 2021, pp. 1–13; Daniel McCarthy, ed., *Technology and world politics* (Abingdon: Routledge, 2018).

[8] Forbes, *Top 100 Digital Companies*, https://www.forbes.com/top-digital-companies/list/#tab:rank.

[9] André Barrinha and Thomas Renard, 'Power and diplomacy in the post-liberal cyberspace', *International Affairs* 96: 3, 2020, p. 750.

[10] Linda Weiss, 'The state-augmenting effects of globalization', *New Political Economy* 10: 3, 2005, pp. 345–53; Linda Weiss, 'Globalization and the myth of the powerless state', *New Left Review*, no. 225, 1997, pp. 3–27.

power also accrues with the active support, or acquiescence, of the state, though such power is not always exercised by the digital platforms in the interest of US national security, especially if commercial interests are threatened.[11] Our argument is simply that private internet capital in the United States opens new vistas in virtual spaces for the exercise by digital platforms of the infrastructural power more usually exercised by the sovereign state.

Our initial assessment is that the role played by the digital platforms via the digital stack has implications for the US state's capacity to exercise what Weiss and Thurbon call 'structural power' in the national interest.[12] They define 'structural power' as the state's capacity to project power internationally, or the 'outward facing' manifestation of domestic infrastructural power.[13] Beyond the focus of our study, one possible geopolitical implication of any manifestations of 'virtual sovereignty' may be the effect on the US state's capacity to engage in great power competition and strategic rivalry with near-peer competitors, such as China. US state power may fracture because domestic and foreign domestic actors use digital platforms in support of commercial or otherwise hostile strategic interests. Apposite here is Mazarr's 2022 study of the drivers of great power, which explains:

> In the struggle for advantage among world powers, it is not military or economic might that makes the crucial difference but the fundamental qualities of a society: the characteristics of a nation that generate economic productivity, technological innovation, social cohesion, and national will.[14]

The article proceeds below in five sections. First, we examine some of the classic International Relations literature on state sovereignty and power, using Jackson's and Krasner's work on authority, legitimacy, power and control in territorial space.[15] Second, we draw on the work of Mann, and Weiss and Thurbon, on infrastructural power to propose the emergence of virtual sovereignty in the United States.[16] Third, we illustrate how US digital platforms may acquire sovereign powers across the virtual territories of the digital landscape by exercising aspects of infrastructural power defined previously as the prerogative of the sovereign territorial state. We compare the infrastructural power of private internet capital, via its control over software and hardware, which creates the digital stack, with that exercised historically by the US state. A type of 'virtual sovereignty' is exercised through the digital platforms' largely unregulated control over the curation of thought and behaviour via their algorithms and commercialization of

[11] Laura DeNardis, *The global war for internet governance* (New Haven, CT: Yale University Press, 2014).

[12] On the China challenge, see David Dollar and Ryan Hass, *Getting the China challenge right*, Brookings, 25 Jan. 2021, https://www.brookings.edu/research/getting-the-china-challenge-right/; Wilson Center, 'Compendium of recommendations on China policy for the Biden administration', 8 Jan. 2021, https://www.wilsoncenter.org/article/compendium-recommendations-china-policy-biden-administration.

[13] Weiss and Thurbon, 'Power paradox', p. 780.

[14] Michael Mazarr, 'What makes a power great: the real drivers of rise and fall', *Foreign Affairs* 101: 4, 2022, pp. 52–63.

[15] Robert Jackson, 'Sovereignty at the millennium', *Political Studies* 47:3, pp. 423–30, 1999; Stephen Krasner, *Sovereignty: organized hypocrisy* (Princeton: Princeton University Press, 1999).

[16] Weiss and Thurbon, 'Power paradox,' pp. 779–810; Mann, 'Infrastructural power revisited', pp. 355–65; Mann, *The sources of social power*, pp. 1–3.

big data. Fourth, we reflect on whether private internet capital may exercise some form of transformative power because of the US state's arguably diminishing role in leading technological innovation and development in the national economy. Fifth, we review the claims of the digital platforms that exhibit signs of virtual sovereignty. We conclude that while private internet capital and digital platforms in the United States acquire considerable power to shape individual thought and behaviour, facilitate cross-border flows of 'fintech' and acquire some aspects of transformative economic power, questions about the legitimacy and recognition of their 'virtual sovereignty' remain unanswered.

Sovereignty

Here we engage with Jackson's conceptualization of sovereignty as comprising authority, rights and the power to control within a territorially bounded state.[17] Historical time and place have implications for the realization of sovereign attributes. Sovereign authority and power were reconsidered as a consequence of European integration, for example, producing post-traditional and pluralist conceptions of sovereignty.[18] Similarly, our purpose is to consider whether the power of the digital platforms in the United States demonstrate some attributes of the sovereign.

Jackson observed that though sovereignty has been a much contested concept, it comprises views of authority and rights, and of power and capability.[19] He argues that these basic components are complemented by international political and legal practices, whereby the government of a territory claims sovereignty which is then recognized by others.[20] Avbelj concludes that traditional definitions of sovereignty are 'single, absolute, indivisible, territorial and statist', and are often used normatively to enshrine international stability,[21] as well as to assert a state's claim to a monopoly over the legitimate use of violence. Krasner argues that sovereignty consists of a 'bundle of properties', including territory, recognition, autonomy and control, though few states possess all four attributes. State practice also illustrates that 'domestic autonomy has frequently been transgressed'.[22] Krasner proposes four typologies of sovereignty: domestic, interdependent, international legal, and Westphalian. As such, the rise of digital platforms in the United States has the potential to extend Krasner's argument about 'transgression' when challenging sovereignty; however, the idea of virtual sovereignty does not fulfil Krasner's definition of the international legal form of

[17] Robert Jackson, 'Sovereignty at the millennium', *Political Studies* 47: 3, pp. 423–30, 1999, p. 424; Georg Sorenson, 'Sovereignty: change and continuity in a fundamental institution', *Political Studies* 47: 3, pp. 590–604; Saskia Sassen, 'Embedded borderings: making new geographies of centrality', *Territory, Politics, Governance* 6: 1 2017, pp. 5–155; Daniel Deudney, 'The Philadelphian system: sovereignty, arms control, and balance of power in the American states-union, circa 1787–1861', *International Organization* 49: 2, 1995, pp. 191–228.
[18] Matej Avbelj, 'Theorizing sovereignty and European integration', *Ratio Juris* 27: 3, 2014, pp. 344–63.
[19] Jackson, 'Sovereignty at the millennium', p. 424.
[20] Jackson, 'Sovereignty at the millennium', p. 425.
[21] Avbelj, 'Theorizing sovereignty and European integration', p. 348.
[22] Krasner, *Sovereignty*, pp. 221, 224.

sovereignty, which requires legal recognition by other sovereign states or entities in the international system.[23]

Both Crawford and Beaulac note that the legitimacy of the social contract between ruler and ruled confers authority, whereby the individual bestows authority on the state to rule and provide domestic order in a states-based international system.[24] If, as Deudney contends, state sovereignty recedes when the legitimacy of the social contract no longer holds in the mind of the individual, then it is remiss not to question whether digital platforms in the United States are assuming some of the authority of the sovereign state.[25] This question, asked by Crawford, resonates with Deudney's argument that sovereignty can be located in multiple sites in a polity—a multiplicity which, in the end, has the effect of creating alternative authority structures.[26] Pluralist, pooled or layered conceptualizations of sovereignty are much discussed in analyses of the shared *state* and regional sovereignty of European integration.[27] The question of the acquisition of sovereign authority in the United States by digital platforms warrants similar consideration. Context is important here, too, as the rise of the new geopolitical competition sits alongside the primacy of transnational risk, reinvigorating attention to national politics and the question of the sovereign's capacity to protect in the new risk context.[28]

The possession and exercise of authority within a bounded territory are key attributes of sovereignty. Traditionally, territory was delimited largely by land borders, but in 1982 the Indonesian state's declaration of 'archipelagic sovereignty' over its waters was recognized under the United Nations Convention on the Law of the Sea (UNCLOS). What, then, of the nature of 'virtual territory' in a digital context? While Mann argued in the 1980s that 'where states are strong, societies are relatively territorialised and centralised',[29] the socio-technical literature on the materiality of new territories created by the critical software and hardware in the digital stack also suggests a question about whether digital platforms exercise some degree of virtual sovereignty. According to Libicki, the technological substrate of digital space consists of a physical layer of machines and networks of communication signals; a syntactic control layer of software, which formats and structures signals for computer systems and networks; and a semantic information repository, where meaning is derived from the electronic signals.[30] Such critical

[23] Krasner, *Sovereignty*, p. 9.

[24] Matthew Crawford, 'Algorithmic governance and political legitimacy', *American Affairs* 3: 2, 2019, pp. 73–94; Stephane Beaulac, 'Emer de Vattel and the externalization of sovereignty', *Journal of the History of International Law* 5: 2, 2003, pp. 237–92.

[25] Deudney, 'The Philadelphian system', *International Organization* 49: 2, 1995, pp. 199–200; Crawford, 'Algorithmic governance and political legitimacy', pp. 73–94.

[26] Deudney, 'The Philadelphian system', p. 194.

[27] Andrew Moravcsik, *The choice for Europe: social purpose and state power from Messina to Maastricht* (Ithaca, NY: Cornell University Press, 1998); Avbelj, 'Theorizing sovereignty and European integration'; Richard Bellamy and Dario Castiglione, 'Three models of democracy, political community and representation in the EU', *Journal of European Public Policy* 20: 2, 2013, pp. 206–23; William Wallace, 'The sharing of sovereignty: the European paradox', *Political Studies* 47: 3, 1999, p. 521.

[28] Ulrich Beck and Daniel Levy, 'Cosmopolitanized Nations', *Theory, Culture & Society* 30: 2, 2013, pp. 3–31.

[29] Michael Mann, 'The autonomous power of the state: its origins, mechanisms and results. *European Journal of Sociology* 25: 2, 2010, p. 212.

[30] Martin Libicki, *Cyberdeterrence and cyberwar* (Santa Monica, CA: RAND, 2009), pp. 12–13.

infrastructure comprises what Bratton calls the 'digital stack', which 'refers to a transformation in the technical infrastructure of global systems … which produces new geographies and new territories'.[31] Rogers and Bienvenue, following Bratton, argue that the 'digital stack' consists of five layers of aggregated infrastructure from the human–computer interface to the geospatial value and supply chains.[32] The layers act as 'gateways' accommodating influential 'gatekeepers' who exert power over the flow of information across the 'digital stack'.[33]

It is possible to imagine that digital platforms acquire infrastructural power as the consequence of a private commercial logic which relies on accumulating and controlling big data by limiting regulation of domestic and global competition beyond weak US anti-trust laws. This commercial logic maximizes global returns on US private equity investment which finances the design and construction of the digital stack's global software and hardware infrastructure, which is 'constituted by the relationships between devices as much as the relationships between people', vanquishing competition and managing consumers for commercial gain.[34] The question, then, is whether the authority of the social contract between the citizen and the state is challenged by the authority of the commercial contract between consumer and digital platform.

The social sources of power

Weiss and Thurbon, and Mann, argue that a state's extractive and transformative powers enable the sovereign state to determine government policy, provide national security and direct technological innovation.[35] According to Mann, a state's ability to translate infrastructural power into effective governance is grounded in social consent,[36] and a state's autonomous power derives from its necessity and the multiplicity of administrative and security functions.[37] Societies where a state's infrastructural power is exercised consensually are 'messy' because they are composed of, in Mann's words, 'multiple overlapping and intersecting sociospatial networks of power'.[38] The state possesses the capacity to 'penetrate civil society and implement its actions across its territories'. Historically, the state grows in potency as the media, through which institutions and communications systems penetrate civil society, become more digitally immersive and pervasive.[39] Lazar takes Mann's insights a step further, however, by pointing out that, as computational systems intensify power relations, explainability, contestability

[31] Benjamin Bratton, *The stack: on software and sovereignty* (Cambridge, MA: MIT Press, 2016), pp. xviii, 375.
[32] Rogers and Bienvenue, 'Combined information overlay', pp. 96–9.
[33] Rogers and Bienvenue, 'Combined information overlay', pp. 96-9.
[34] Philip Howard, *Pax technica: how the internet of things may set us free or lock us up* (New Haven, CT: Yale University Press, 2015), p. 35.
[35] Weiss and Thurbon, 'Power paradox', pp. 783–4; Mann, 'Infrastructural power revisited', pp. 355–66; Mann, *The sources of social power*, pp. 1–3.
[36] Mann, 'The autonomous power of the state'; Mann, 'Infrastructural power revisited', p. 355; Mann, *The sources of social power*.
[37] Mann, 'The autonomous power of the state', p. 194.
[38] Mann, *The sources of social power*, p. 1.
[39] On technological development and its effects on power, see Mann, 'Infrastructural power revisited', p. 355.

and accountability become more important for the sovereign state's legitimacy and authority.[40]

In an era of real-time accumulation and commercialization of big data by digital platforms, the exercise of infrastructural power is not limited to a state's 'territorially demarcated' physical space.[41] The digital stack provides private internet capital with commercial and surveillance opportunities to shape individual choices via algorithmically generated accumulation and sale of big data in real time, often without the knowledge of the consumer and in violation of the individual's right to privacy.[42] The exponential and unending automated generation of big data enables US digital platforms to intermediate new organizational forms interconnecting networks of private internet capital in virtual territories where competition and state regulation do not operate.[43] As a result, control of open and secure data is moving beyond the US state's extractive and transformative power,[44] creating a disconnect between what Weiss and Thurbon call the sovereign state's 'territorially-centred autonomy' and, in this case, the digital stack.[45] This suggests that US digital platforms, financed by private internet capital, acquire extractive and transformative capacities 'both by virtue of, and at the expense of, the US state itself'.[46]

Cohen argues that the digital economy disrupts how the US state traditionally exercises infrastructural power because it does not control the collection and distribution in real time of algorithmically generated big data:

> [The] locus for those activities is the platform, a site of encounter where interactions are materially and algorithmically intermediated. Platforms—including online marketplaces, desktop and mobile computing environments, social networks, virtual labour exchanges, payment systems, trading systems, and many, many more—have become the sites of ever-increasing amounts of economic activity and also of ever-increasing amounts of social and cultural activity … [the platforms] are not contiguous physical spaces but rather are defined using protocols, data flows, and algorithms. Both technically and experientially, however, they are clearly demarcated spaces with virtual borders that platforms guard vigilantly.[47]

As private internet capital seeds the creation and development of innovative and immersive technologies for global citizens, humans are increasingly woven into convergent fabrics of the Internet of Everything (IoE), artificial intelligence (AI) and big data—and, if Meta has its way, the Metaverse—within the spatial webs of the digital stack. Rene and Mapes argue that in this networked, virtual world of augmented and virtual reality, headsets, smart glasses, wearables and sensors, we consumer/citizens will

[40] Seth Lazar, 'Legitimacy, authority, and the political value of explanations', arXiv research sharing platform, Computers and Society section, Cornell University, 19 Aug. 2022, https://arxiv.org/abs/2208.08628.
[41] On territorially demarked spaces, see Michael Mann, 'The autonomous power of the state', pp. 187–8.
[42] Salome Viljoen, 'Democratic data: a relational theory for data governance', *Yale Law Journal* 131: 2, 2021, pp. 654–781.
[43] Bruce Schneier, 'The battle for power on the internet', *The Atlantic*, 24 Oct. 2013.
[44] Julie Cohen, *Between truth and power: the legal constructions of informational capitalism* (New York: Oxford University Press, 2019), p. 41.
[45] Weiss and Thurbon, 'Power paradox', p. 782.
[46] Weiss and Thurbon, 'Power paradox', p. 803.
[47] Julie Cohen, 'Law for the platform economy', *University of California, Davis, Law Review* 51: 133, 2017, pp. 136 and 200.

project our information, ideas, and imaginations into the world around us, weave them into every conversation, displaying them in our cities, in the places we work, learn and live. With intuitively placed information, AI-assisted interaction, cryptographically secure information, and digital payments, a new kind of network is emerging. One where the Web becomes the World. [48]

If the Web indeed 'becomes the World', and given the social origins of power identified by Mann and by Weiss and Thurbon, we are able to suggest that a form of 'virtual sovereignty' is coming into existence in the United States because digital platforms exercise features of the state's infrastructural power. At a minimum, the digital platforms disrupt the ability of the sovereign state to exercise its traditional powers in the United States because of their development and control of the digital stack's hardware and software. This begs an important question. Have private internet capital and US digital platforms acquired any of the authority, rights or legitimacy of state sovereignty?

Extractive power: authority, control and the digital platforms

Extractive power through critical technologies

In this section we examine the capacity of corporate actors to exercise authoritative control in the United States via their command of extractive power in the critical infrastructures of the digital stack. The means by which the sovereign state extracts and exercises power, transmits its commands and controls information is increasingly held or shared by private commercial platforms. They create and deploy commercially viable digital software and hardware across layers of the stack's human–computer interface and geospatial land, subsea and space domains.

Physical infrastructure, such as submarine cables, satellites, cloud storage and bandwidth, is created within global wealth and supply chains consisting of US and non-US private and state-owned companies. In 2021, Google was a major investor in approximately 8.5 per cent of the global network of submarine cables, which extends to more than 1.12 million kilometres.[49] Winseck argues that a 'consortia' approach to ownership of the digital infrastructure allowed greater multilateral heterogeneity after the resurgence in global capital flows following on from the 2008 global financial crisis. Private and state-backed tech companies flooded the Indo-Pacific, which hosts the largest number of users and greatest volume of global internet traffic.[50] Owners of the physical infrastructure include Indo-Pacific states, which are financed by both government and private internet capital, often in consortia with US digital platforms such as Google.[51] Meta's 2Africa cable is financed in conjunction with China Mobile.

[48] Gabriel Rene and Dan Mapes, *The Spatial Web* (Gabriel Rene, 2019), https://hi.1lib.limited/book/21257024/e94ac1, p. 27.

[49] Tyler Cooper, 'Google owns 63,605 miles and 8.5% of submarine cables worldwide', *Broadbandnow*, 30 Nov. 2021, https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/.

[50] Dwayne Winseck, 'The geopolitical economy of the global internet infrastructure', *Journal of Information Policy*, vol. 7, 2017, pp. 242–3; Howard, *Pax technica*, p.16.

[51] Winseck, 'The geopolitical economy of the global internet infrastructure', pp. 242–3.

Networks of fibre optic cables (see table 1 below) are part of a new critical infrastructure built largely since 1988. By 2017 the global fibre optic network carried 99 per cent of global internet traffic.[52] The digital platforms' development and control of vast networks of physical infrastructure often intersected, both positively and negatively, with the geopolitical interests of the state.

Subsea fibre optic cable ownership is a commercial imperative for digital platforms because bandwidth is increasing exponentially to accommodate big data with low latency. Fibre optic cable provides advantages of scale and a network for future technologies.[53] The major users are private commercial content and cloud service providers. New capacity is added when required at considerable cost savings. By 2020 the fibre optic cable network accounted for two-thirds of capacity, largely replacing traditional carriers.[54] Other new high-speed, low-cost global internet connections and storage include Google's US fibre-based home internet service which sews fast internet coverage into fixed-line internet protocols (IP) and 'last yards' (the final distance to the device) connectivity; [55] and Alphabet's Project Taara, which provides rural and remote wireless data transmission via laser light beams.[56] Digital platforms also extend their authoritative control over the physical infrastructure of the digital stack through a suite of low Earth orbit satellite constellation projects. These include Google's Space-X project, which consists of 1,000 satellites of different sizes orbiting at varying altitudes,[57] and its 2016 acquisition of Webpass to facilitate better connections between customers and ground stations.[58] In 2020 Amazon announced Federal Communications Commission approval for its Project Kuiper, which consists of a 'constellation' of 3,236 low-orbit satellites with low latency.[59]

The private owners of the cloud's physical infrastructure and platform services are largely big global digital platforms, including Amazon, Microsoft, Google and IBM.[60] US digital platforms reach across the stack, extending their service provision to global financial technology wherever a commercial opportunity arises. In 2020 Apple launched a credit card, while Google announced plans to develop consumer

[52] Winseck, 'The geopolitical economy of the global internet infrastructure', p. 237.

[53] Alan Mauldin, 'Rising tide: content providers' investment in submarine cables continues', *TeleGeography*, 27 May 2016, https://blog.telegeography.com/rising-tide-content-providers-investment-in-submarine-cables-continues.

[54] *Telegeography*, 'Executive summary: Telegeography global bandwidth research service', Washington DC, PriMetrica; *Telegeography*, Submarine cable map, https://www.submarinecablemap.com/.

[55] Blair Levin and Larry Downes, 'Why Google fiber is high speed internet's most successful failure', *Harvard Business Review*, 7 Sept. 2018, https://hbr.org/2018/09/why-google-fiber-is-high-speed-internets-most-successful-failure; Maggie Tilman, 'What is Google Fi and how does it work?', Pocket-lint.com, 23 Feb. 2021, https://www.pocket-lint.com/phones/news/google/147278-what-is-google-fi-and-how-does-it-work.

[56] Katyanna Quach, 'Forget that Loon's balloon burst, we just fired 700TB of laser broadband between to cities, says Alphabet', *The Register*, 17 Sept. 2021, https://www.theregister.com/2021/09/17/alphabet_project_taara_congo/.

[57] Steven Musil and Richard Nieva, 'SpaceX lands $1 billion from Google and Fidelity', CINet, 20 Jan. 2015, https://www.cnet.com/news/google-reportedly-in-satellite-investment-talks-with-spacex/.

[58] Ben Schoon, 'Google "Fiber Webpass" is a rebrand of the wireless gigabit internet service', *9to5google*, 21 Feb. 2020, https://9to5google.com/2020/02/21/google-fiber-webpass-rebrand/.

[59] Amazon, 'Amazon receives FCC approval for Project Kuiper satellite constellation', 30 July 2020, https://www.aboutamazon.com/news/company-news/amazon-receives-fcc-approval-for-project-kuiper-satellite-constellation.

[60] Raj Bala, Bob Gill, Dennis Smith, David Wright and Kevin Ji, 'Magic quadrant for cloud infrastructure and platform services', *Gartner*, 27 July 2021.

Table 1: Indicative Google and Meta submarine cables, 2022

Google submarine cables	*Landing points*	*Ownership*
FASTER	Bandon, OR, US; Chikura and Shima, Japan; Tanshui, Taiwan	Google, KDDI, Singtel, China Telecom, China Mobile, TIME dotCom
Grace Hopper	Bude, UK; Bellport, US; Bilbao, Spain	Google
Dunant	Saint-Hilaire-de-Riez, France; Virginia Beach, VA, US	Google
Havfrue/AEC-2	Wall, NJ, US: Leckanvy, Ire; Kristiansand, Norway; Blaabjerg, Denmark	Aqua Comms, Bulk Infrastructure, Meta, Google
Pacific Light Cable Network proposed	El Segundo, CA, US; Toucheng, Taiwan; Baler, Philippines	Google, Meta
Unity/EAC Pacific	Chikura, Japan; Redondo Beach, CA, US	Telstra, Google, Singtel, KDDI, Airtel (Bharti), TIME dotCom
Meta submarine cables		
Amitie	Bude, UK; Le Porge, France; Lynn, MA, US	Aqua Comms, Meta, Microsoft, Orange, Vodafone
Asia Pacific Gateway	South Korea-Japan-China-Philippines-Taiwan-Vietnam-Malaysia-Thailand	NTT, China Telecom, China Unicom, Chunghwa Telecom, KT, Starhub, LG Uplus, China Mobile, Viettel Corporation, VNPT International, Meta, TIME dotCom
MAREA	Virginia Beach, VA, US; Bilbao, Spain	Meta, Microsoft, Telxius
2Africa	16 countries in Africa and 23 countries overall, incl UK, India, Oman	China Mobile, MTN, Meta, Orange, Saudi Telecom, Telecom Egypt, Vodafone and WIOCCUS
Echo (ready for service 2023)	Eureka, CA, US; Ngeremlengui, Palau; Agat and Piti, Guam, US; Changi North, Singapore; Tanjung Pakis, Indonesia	Google, Meta

Source: *TeleGeography*, Submarine cable map, 2 March 2022, https://www.submarinecablemap.com; Alan Mauldin, 'Rising tide'.

bank accounts. Apple's replacement of Intel with its own ARM-based processors in 2020 revealed a pattern of corporate consolidation, independent capacity and authoritative control.[61]

Private US internet capital is highly mobile, financing global digital services and infrastructure where a business case warrants investment. The unprecedented commodification of networks, services and data is largely unregulated, or beyond regulation, by the US state, unlike traditional telecom providers, while the digital platforms reach into every aspect of connectivity and service provision.[62] Table 2 shows how Alphabet's strategic reach evolved across multiple layers of the digital stack, from internet provision to global health services. As Rick Osterloh of Google stated:

> If you look across all of Google's products, from Search to Maps, Gmail to Photos, our mission is to bring a more helpful Google for you. Creating tools that help you increase your knowledge, success, health, and happiness. Now when we apply that mission to hardware and services, it means creating products like … Pixel phones, wearables, laptops, and Nest devices for the home.[63]

The extractive power of the digital platforms accrues through their network power in the digital stack. Market service diversity and variegation mean that its random yet controlling modular structure constrains 'outsider options'. This ensures 'stickiness' to the network as it evolves globally.[64] According to Cohen, the digital stack's stickiness 'comprehensively reshapes the conditions of economic exchange' in rematerialized and legalized *terra nullius* networks which are not possible in traditional markets.[65]

Extractive power at the human–computer interface

In 1986 Mann reflected on the 'invention of new organizational techniques that greatly enhanced the capacity to control peoples and territories'.[66] Following on from Mann, Crawford observed that: 'In ever more areas of life, algorithms are coming to substitute for judgement exercised by identifiable humans who can be held to account'.[67] According to Crawford, the capacity of private internet capital to finance digital platforms which shape individual choice and behaviour is not necessarily commensurate with state interests, or the tolerant pluralism, accountability and transparency necessary for a functional liberal democracy.[68]

[61] ARM processors are Advanced Reduced Instruction Set Computer Machines also now produced by ARM Ltd: Samuel Gibbs, 'Apple ditches Intel for ARM processors in Mac computers with Big Sur', *Guardian*, 23 June 2020.

[62] World Economic Forum in collaboration with Accenture, *Digital Transformation Initiative: Telecommunications Industry*, Cologny/Geneva, Jan. 2017, p. 11, https://www.accenture.com/_acnmedia/accenture/conversion-assets/wef/pdf/accenture-telecommunications-industry.pdf.

[63] Rick Osterloh, 'Made by Google', New York, 15 Oct. 2019, https://www.youtube.com/watch?v=XKmsYB54zBk&t=.

[64] Cohen, *Between truth and power,* pp. 41–51; Manuel Castells, *The rise of the network society* (Oxford: Blackwell, 1996).

[65] Cohen, *Between truth and power*, p. 50.

[66] Mann, *The sources of social power*, p. 3.

[67] Crawford, 'Algorithmic governance and political legitimacy', p. 1.

[68] Matthew Crawford, 'Testimony before the US Senate Judiciary Committee, Subcommittee on Antitrust, Competition Policy and Consumer Rights', Washington DC, 15 June 2021.

Table 2: A selection of Alphabet's subsidiaries, 2022

Alphabet's subsidiary companies (selection only)	*Sector*
Calico	Health and biotech
CapitalG	Finance
Firebase	App development
Fitbit	Health and recreation
Google Youtube	Video-sharing
Google Search	Internet services
Google Maps	Internet services
Google Photos	Internet services
Google Workspace for Education	Internet services and education
Google Ads DoubleClick	Ad management, business software and data analytics
Google Android OS	Operating system
Google AI	Artificial intelligence
Google Jigsaw	Tech incubator and internet safety
Google Kaggle	Machine learning and data science
Google Nest	Smart home products
Google Fiber	Internet access
Google Cloud	Database and storage
Google Looker	Business and data analytics
Google TensorFlow	Chip technology and machine learning
Google Sensorvault (internal)	Database and storage
Google WebPass	Internet access: satellite ground stations to customers
GV	Finance
Deep Mind	Machine learning and AI
Intrinsic	Software for industrial robots
Isomorphic Labs	Deep Mind application to drug discovery
Sidewalk Labs	Tech infrastructure and climate-positive infrastructure
Verily	Health, life sciences, and biotech
Waymo	Autonomous vehicles
Wing	Drone delivery
X	Research and development

Source: Company home pages, accessed 2 Sept 2022. For a full list of these sources, please contact the author or the *International Affairs* editorial office.

Frances Haugen, a former Facebook manager, testified to the profit-making machine-learning models that 'amplif[y] division, extremism, and polarization'.[69] Economic incentives for users of smart devices to stay online and use apps to divulge maximum information for 'panoptic sorting' are profitable for businesses and advertisers, as is the escalation of seditious and incendiary content, and the consumers' emotional hunger for more celebrities and social influencers.[70] The legitimacy of state sovereignty, established via a social contract and involving the relinquishment of some individual freedoms for security and public services, is eroded and, in part, replaced by virtual sovereignty, the legitimacy of which is not established by commercial contracts between digital platforms and individual consumers. The purpose of the social contract in legitimizing state sovereignty is transcended. Services provided by digital platforms are not transparent, contestable or accountable. There is no digital equivalence of the legitimacy of state sovereignty in the social sources of power.

Private internet capital in the United States exercises extractive power by financing the rapid accumulation, storage and real-time commercial extraction, or commodification, of big data.[71] Digital platforms micro-target individual consumer tastes and desires, shaping consumption patterns and spatial connections in real time on a society-wide scale.[72] How, by whom, and what technology is used in the United States to shape and reshape the behaviour of surveilled consumers?[73] At an individual level, protection of individual rights requires not only shelter from data collection but also protection from biases and value judgements inherent in the algorithms running the surveillance system.[74] Informed consent cannot be given because digital trends are largely unseen and unfelt by consumers,[75] requiring critical epistemic examination of the 'surveillant assemblage' which produces a 'data derivative' or 'shadow self'.[76] This 'performativity' is also known as the decontextualization of the self from the meaning of 'real lives'.[77] Big data

[69] Statement of Frances Haugen, United States Senate Committee on Commerce, Science and Transportation, 4 Oct. 2021.

[70] Lina M. Khan and David E. Pozen, 'A skeptical view of information fiduciaries', *Harvard Law Review* 133: 497, 2019, pp. 526–8; Woodrow Hartzog, *Privacy's blueprint: the battle to control the design of new technologies*, (Cambridge, MA: Harvard University Press, 2018), p. 5; Oscar Gandy, *The panoptic sort: a political economy of personal information* (Boulder, CO: Westview, 1993).

[71] OECD, *OECD digital economy outlook 2017* (Paris, 2017), pp. 202–06; OECD, *OECD digital economy outlook 2020* (Paris, 2020), pp. 130–53.

[72] Samantha Bradshaw and Philip Howard, *Challenging truth and trust: a global inventory of organized social media manipulation* (Oxford: Oxford Internet Institute, University of Oxford, 2018), p. 21.

[73] David Lyon, 'Surveillance, Snowden, and big data: capacities, consequences, critique', *Big Data and Society* 1: 2, 2014, p. 7; Sara Degli Esposti, 'When big data meets dataveillance: the hidden side of analytics', *Surveillance and Society* 12: 2, 2014, pp. 209–25.

[74] Tobias Matzner, 'Surveillance as a critical paradigm for big data?' in Ann Rudinow Sætnan, Ingrid Schneider and Nicola Green, eds, *The politics of big data: big data, big brother?* (Abingdon: Routledge, 2018), ch. 5, pp. 68–86 at pp. 76–7.

[75] Frank Pasquale, *The black box society: the secret algorithms that control money and information* (Cambridge, MA: Harvard University Press, 2015); Shoshana Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (London: Profile, 2019); Stuart Mills, '#DeleteFacebook: from popular protest to a new model of platform capitalism?', *New Political Economy*, 8 Dec. 2020, pp. 851–68.

[76] Kevin Haggerty and Richard Ericson, 'The surveillant assemblage', *British Journal of Sociology* 51: 4, 2000, p. 606; Louise Amoore, *The politics of possibility: risk and security beyond probability* (Durham, NC: Duke University Press, 2013), p. 61.

[77] Tobias Matzner, 'Beyond data as representation: the performativity of big data in surveillance', *Surveillance &*

is sought by companies which create personalized predictive profiles to 'actuate' behaviour by nudging, herding and manipulating. Further complicating the issue of human comprehension of the shaping effects of technology and assemblages is the effect of cognitive decline induced by addiction to smart device use itself.[78]

In a key 2014 study, Facebook (now Meta) data scientist Adam Kramer and his co-authors claimed 'that emotions expressed by others on Facebook influence our own emotions, [and] constitute experimental evidence for massive-scale contagion via social networks'.[79] Publication of this research by the Proceedings of the National Academy of Sciences was followed by a statement of editorial concern. It noted that, although Facebook's data collection was legally 'consistent with Facebook's Data Use Policy, to which all users agree prior to creating an account, constituting informed consent for this research', it nonetheless 'may have involved practices that were not fully consistent with the principles of obtaining informed consent and allowing participants to opt out'.[80] Facebook revealed a desire for, and claim to, not only a capacity to shape emotion and behaviour, but also the forfeiture of individual rights through onerous terms and conditions.

The success of this business model requires normalization of online addictive behaviour.[81] Hartzog argues digital technology is not value-neutral and that 'design decisions' are extraordinarily powerful, particularly as they are informed by risk-taking innovation and experimentation.[82] In 2010, for example, Facebook conducted unpublished micro-targeted advertising experiments on 61 million users in order to maximize profits from advertising on individually targeted news feeds.[83] This online 'ad tech' ecosystem is key evidence of the exercise of infrastructural power by digital platforms. Their monopolistic practices leverage network effects on individual choices to curate the information environment in ways unseen by the consumer. Abuses of monopoly power amount to an unprecedented capacity to dominate not only the online advertising marketplace, but also consumers' access to information flows.[84] Google defended its practices and rejected concerns over privacy, though the veracity of its defence was undermined in 2016 when it was exposed violating what it claimed it was offering protection against.[85]

Google and its parent company Alphabet exhibit monopolistic tendencies across markets with hitherto unexamined implications for the state of liberal

Society 14: 2, pp. 197–210 at pp. 205–7; Haggerty and Ericson, 'The surveillant assemblage', pp. 606–07.

[78] Joseph Firth, John Torous, Brendon Stubbs, Josh Firth, Genevieve Steiner, Lee Smith, Mario Alvarez-Jiminez, John Gleeson, Davy Vancampfort, Christopher Armitage and Jerome Sarris, 'The "online brain": how the internet may be changing our cognition', *World Psychiatry* 18: 2, 2019, pp. 119–29; Adrian Ward, Kristen Duke, Ayelet Gneezy and Maarten Bos, 'Brain drain: the mere presence of one's own smartphone reduces available cognitive capacity', *Journal of the Association of Consumer Research* 2: 2, 2017, pp. 140–54.

[79] Adam Kramer, Jamie Guillory and Jeffrey Hancock, 'Experimental evidence of massive-scale emotional contagion through social networks', *Proceedings of the National Academies of Science* 24: 111, 2014, p. 8788.

[80] Inder Verma, 'Editorial expression of concern and correction', *Proceedings of the National Academies of Science* 29: 111, 2014, p. 10779.

[81] David Courtwright, *The age of addiction: how bad habits became big business* (Cambridge, MA: Belknap, 2019).

[82] Hartzog, *Privacy's blueprint*, p. 8; Bill Davidow, 'Skinner marketing: we're the rats, and Facebook likes are the reward', *The Atlantic*, 10 June 2013.

[83] Paul Starr, 'The new masters of the universe: big tech and the business of surveillance', *Foreign Affairs* 98: 6, 2019, pp. 191–7.

[84] Dina Srinivasan, 'Why Google dominates advertising markets', *Stanford Technology Law Review* 24: 1, 2020, p. 173.

[85] Julia Angwin, 'Google has quietly dropped ban on personally identifiable web tracking', *ProPublica*, 21 Oct. 2016.

democracy in the United States. The 2020 *Investigation of competition in digital markets* concludes its section on Google by stating that, 'absent interventions, the barriers to entry and network effects in this market mean there is a high potential for single-homing and an overall concentrated market'.[86] The report states simply in its overall findings that 'Google increasingly functions as an ecosystem of interlocking monopolies',[87] in clear breach of anti-trust laws. Facebook (prior to its rebranding as Meta) similarly accrued influence by stealth over the global information environment of some 1.79 billion daily users in 2019,[88] if not in plain sight then via the manipulation of holes in the state's laws and regulations. The 2020 House report stated that Facebook 'maintained its monopoly through a series of anticompetitive business practices', adding that the absence of competition resulted 'in worse privacy protections for its users and a dramatic rise in misinformation on its platform'.[89]

As social networks became the primary way for consumers to communicate, especially for the generation of 'digital natives', Facebook's monopoly delivered several auxiliary advantages. Accruing increasingly detailed psychographic dossiers on its users while pretending to value their privacy, Facebook leveraged its status as the dominant social platform to sell access to its consumers to an ecosystem of data brokers hungry for personal data and unscrupulous about the privacy invasions that access entailed.[90] Facebook's infamous experiment on user emotions demonstrates the extent of the closed information loop it knew it was building.[91]

Extractive power, digital disruption and foreign interference

One of the attributes of sovereign power and control is the capacity to maintain autonomy and exclude the social and political influence of foreign actors.[92] Digital disruption in times of international uncertainty affects the state's extractive power: its ability to gain consent from, and transmit commands to, civil society. The US state is vulnerable not only to hostile foreign actors, but also to disaffected domestic actors using digital platforms and social media to launch socio-cognitive attacks against the state's legitimacy. The state's vulnerabilities to the power of the digital platforms are highlighted by its inability either to successfully prosecute a non-partisan case for Russian interference in the 2016 presidential election, or to close the bipartisan divide over the insurrection on 6 January 2021. In both examples, the state's liberal democratic resilience was weakened.

[86] US House of Representatives, *Investigation of competition in digital markets*, majority staff report and recommendations, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary, Washington DC, 2020, p. 247.
[87] US House, *Investigation of competition in digital markets*, p. 15.
[88] US Securities and Exchange Commission, *Facebook, Inc.*, Form 10-Q Quarterly Report, 30 June 2020, p. 27.
[89] US House, *Investigation of competition in digital markets*, p. 14.
[90] Dana Srinivasan, 'The antitrust case against Facebook', *Berkeley Business Law Journal* 16: 1, 2019, pp. 38–101.
[91] Evan Selinger and Woodrow Hartzog, 'Facebook's emotional contagion study and the ethical problem of co-opted identity in mediated environments where users lack control', *Research Ethics* 12: 1, 2016, pp. 35–43.
[92] Krasner, *Sovereignty*, p. 221.

Hostile actors are intent on disrupting and redistributing power in the United States by exploiting the alleged 'technical neutrality' and political agnosticism of US digital platforms.[93] Such actors use the critical technologies of the digital platforms to amplify a raft of domestic social and political problems besieging the United States,[94] which the state demonstrates little capacity to counter, let alone control. Liberal democratic resilience is weakened further, as is the state's capacity to extract consent and transmit command. Moreover, as the US state's capacity to exercise infrastructural power at home is challenged, so too is its capacity to sustain the capacity to legitimately project outward-facing structural power as a global power. Rebecca Hersman provides a pertinent example of how strategic stability could be compromised in the nuclear age.[95]

Russia's strategic and tactical information, or hybrid, warfare, was first deployed against its borderlands before being conducted against a vulnerable United States in 2016.[96] DiResta and colleagues stated in testimony to Congress that Russia used a suite of tactics to influence US politics, from human exploitation tradecraft to narrative laundering.[97] The US state's capacity to govern its territorially bounded population was weakened by foreign troll farms creating 'alternative facts', and domestic social media influencers complaining about the 'deep state' and 'fake news'. Trust in information, except in the echo chambers of an individual's preferred choice of information sources, was eroded. General Paul Nakasone, Director of the National Security Agency and Chief of Cybersecurity Command, argued that 'corrosive threats with strategic effects' during the Trump administration included disruption of state power in the form of manipulation of the expressed will of the people in elections; access to personal identity information; and intellectual property theft.[98] The US House Intelligence Committee concluded that Russia's

[93] Paul Nakasone, 'Strategic competition: the rise of persistent presence and innovation', interview at RSA conference, 6 March 2019, https://www.youtube.com/watch?v=Apd2ReXB6vk.

[94] Maryanne Kelton, Michael Sullivan, Emily Bienvenue and Zac Rogers, 'Australia, the utility of force and the society-centric battlespace', *International Affairs* 95: 4, 2019, pp. 859–76; Francis Fukuyama, 'The decay of American political institutions' *The American Interest* 9: 3, 2014, pp. 6–19; Dani Rodrik, 'Populism and the economics of globalization', *Journal of International Business Policy* 1: 1–2, 2018, pp. 1–22; Julie Azari, 'It's the institutions, stupid: the real roots of America's political crisis', *Foreign Affairs* 98: 4, 2019, pp. 52, 54–60; James Andrew Lewis, *Rethinking cybersecurity: strategy, mass effect, and states*, report of the CSIS Technology Program (Lanham. MD: Rowman & Littlefield, 2018).

[95] Rebecca Hersman, 'Wormhole escalation in the new nuclear age', *Texas National Security Review* 3: 3, 2020, pp. 90–109.

[96] Rand Waltzman, 'The weaponization of information', testimony before the Committee on Armed Services, Subcommittee on Cybersecurity, US Senate, 27 April 2017, p. 7; James Wirtz, 'Cyber war and strategic culture: the Russian integration of cyber power into grand strategy', in Kenneth Geers, ed., *Cyber war in perspective: Russian aggression against Ukraine* (Tallinn: NATO Publications, 2015); Gregory Treverton, Andrew Thvedt, Alicia Chen, Kathy Lee and Madeline McCue, *Addressing hybrid threats* (Stockholm: Centre for Asymmetric Threat Studies, 2018); Nathaniel Gleicher, Margarita Franklin, David Agranovich, Ben Nimmo, Olga Belogolova and Mike Torrey, *Threat report: the state of influence operations 2017–2020*, Facebook, May 2021; Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright and Ben Johnson, *The tactics and tropes of the internet research agency*, New Knowledge Report for US Senate Select Committee on Intelligence, 17 Dec. 2019, p. 99; *Russian active measures, campaigns and interference in the US election*, Report of the Select Committee on Intelligence, US Senate, 2, 116 Congress, First Session, 2019.

[97] DiResta et al., *The tactics and tropes of the internet research agency*, pp. 4–6; Jen Weedon, William Nuland and Alex Stamos, 'Information operations and Facebook', *Semantic Scholar*, 27 April 2017, pp. 8–11, https://pdfs.semanticscholar.org/f633/771f0f586aaa89120a9003e2b24dddaf4d89.pdf?_ga=2.224208979.912145205.1573018665-1324331680.1573018665.

[98] Paul Nakasone, 'Strategic competition: the rise of persistent presence and innovation', interview at RSA

Internet Research Agency (IRA) noted similar concerns and the 'exposure of IRA content to more than 126 million Americans' via Facebook, and 288 million impressions (numbers of people who have seen the tweet) of Russian bot tweets on Twitter.[99]

The challenges for the state's control over the exercise of extractive power are understood by sections of the US administration. Choucri and Clark argue that the US state is attempting to realign the exercise of infrastructural power with its national security interests. They argue:

> This autonomy and power of the private sector all but assures that the state system anchored in sovereign authority will make every effort to redress or to 'rectify' a seeming anomaly in international relations—that is by reasserting the dominance of state sovereignty over cyber matters.[100]

As hostile foreign actors exacerbated domestic socio-cognitive vulnerabilities by engaging in society-centric digital disruption, the US Congress endeavoured to reassert the state's extractive power.[101] To this end, in 2018 the United States attempted to call the digital platforms to account in congressional hearings.[102] Consideration was given in a draft of the 2022 Digital Platform Commission Act to increasing oversight and regulation of the digital platforms, as it was in the American Data Privacy and Protection Act, and a number of specific anti-trust bills, including the Open App Markets Act and the American Choice and Innovation Online Act. While the US state will always attempt to hold challenges to its authority and control to account,[103] its attempts after 2015 to bring the digital platforms to account were not convincing. Even if legislation with the aim of doing so is enacted, questions remain about the effectiveness of any new state regulatory oversight.

We also note that the US digital actors are dependent on global supply and value chains, often in financial partnerships, technology-sharing arrangements and consortiums, sometimes with state-owned and private corporations of declared strategic competitors. The business models of private internet capital which finance US digital platforms resemble what Seabrooke and Wigan describe as the often stealthy practices of global 'wealth chains', which they as 'linked forms of capital seeking to avoid accountability during processes of pecuniary wealth creation', concluding that they are 'articulated not only through cartographic and sovereign spaces', but also through hybrid financial products.[104] We extend

conference, 6 March 2019, https://www.youtube.com/watch?v=Apd2ReXB6vk.

[99] US House of Representatives Permanent Select Committee on Intelligence, *Exposing Russia's effort to sow discord online: the Internet Research Agency and advertisements*, https://intelligence.house.gov/social-media-content/default.aspx; Timothy Snyder, *The road to unfreedom* (London: Vintage Arrow, 2019), pp. 228–59.

[100] Nazli Choucri and David Clark, *Integrating cyberspace and international relations: the co-evolution*, working paper 2012-29 (Cambridge, MA: MIT, 2012), p. 12.

[101] Ariel Levite and Jonathan (Yoni) Shimshoni, 'The strategic challenge of society-centric warfare', *Survival* 60: 6, 2018, p. 96; Jonathan Zittrain, '"Netwar": the unwelcome militarization of the internet has arrived', *Bulletin of the Atomic Scientists* 73: 5, 2017, pp. 300–04.

[102] See e.g. US Senate Committee on the Judiciary and Senate Committee on Commerce, Science, and Transportation, *Facebook, social media privacy, and the use and abuse of data*, 10 April 2018.

[103] Choucri and Clark, *Integrating cyberspace and international relations*, p. 12.

[104] Leonard Seabrooke and Duncan Wigan, 'Global wealth chains in the international political economy: the

their concept to include the digital stack as a non-'cartographic and sovereign space'. Similarly, we extend Weiss and Thurbon's conclusion that globalization of intellectual property rights and patents diluted the domestic sources of US infrastructural power in relation to the role of private internet capital and the digital platforms, enabling the latter to bypass the national security interests of the United States when commercially advantageous to do so.[105] The state's legal monopoly over territorial sovereignty is challenged.

Transformative power and the digital platforms

Weiss and Thurbon describe the relationship between state and corporate actors as one of 'governed interdependence'.[106] The question is whether the digital platforms' exercise of extractive power enables them also to exercise a degree of the state's transformative power and thus a degree of virtual sovereignty. At the outset of the post-Second World War era, the US state consolidated its hegemonic position globally through control and management of technological innovation in what Weiss describes as 'spin around relations' with the private sector.[107] Over the subsequent decades of the Cold War, the state provided capital, project management, sponsorship and, by dint of the national security state, vast resources, linking universities with intelligence agencies to generate and commercialize technological innovation.[108] Yet by 2018, the private corporate sector's share of US research and development (R&D) exceeded the historically dominant share of the national security state by a factor of three. The private corporate sector's share of R&D was even greater in the military-industrial complex.[109]

Digital platforms exercise aspects of transformative power to command and control change in the digital economy, at the partial expense of the national security state.[110] Lewis argues that 'commercial incentives and national security needs usually do not line up'.[111] From the late 1980s, private companies, beginning with AOL and Altavista, then Google, Meta, Apple and Amazon, garnered the controlling power of innovation in the digital stack.[112] While Silicon Valley benefited initially from the state's financial backing, including ideas for the World Wide Web, the Defense Advanced Research Projects Agency (DARPA) and the

governance of global wealth chains', *Review of International Political Economy* 21: 1, 2017, pp. 257, 261.

[105] Weiss and Thurbon, 'Power paradox'.

[106] Weiss and Thurbon, 'Power paradox', pp. 784–5.

[107] Linda Weiss, *America Inc.? innovation and enterprise in the national security state* (Ithaca, NY: Cornell University Press, 2014).

[108] Weiss, *America Inc.?*; Mariana Mazzucato, *The entrepreneurial state* (London: Demos, 2011), p. 20.

[109] John Sargent, 'US research and development funding and performance: fact sheet', R44307 (Washington DC: Congressional Research Service, 4 Oct. 2021).

[110] John Shanahan, 'Emerging technologies and peer competition: the vanishing luxury of time', 12th Annual Strategic Multilayer Assessment (SMA) Conference held jointly with Department of Homeland Security, *The evolving anatomy of conflict in a dynamically changing world*, Joint Base Andrews, 21–22 May 2019, pp. 10–18, https://nsiteam.com/social/wp-content/uploads/2019/08/2019-SMA-Conference-Proceedings_FINAL.pdf; Kathleen Hicks and Michele Flournoy, 'Donald Trump has failed: our national cohesion and security can't wait another five years', *DefenseOne*, 9 June 2020.

[111] James Andrew Lewis, *Mapping the national security industrial base* (Washington DC: Center for Strategic and International Studies, May 2021).

[112] Barrinha and Renard, 'Power and diplomacy in the post-liberal cyberspace', p. 750.

National Science Foundation to give assistance to Sergey Brin and Larry Page's Google,[113] private internet capital eventually replaced state-dominated funding for emerging digital technologies.[114] Potentially lucrative business models for commercial exploitation of the global digital economy attracted substantial private internet capital in digital platforms without the state as incubator and beneficiary client. Webb also argues a lack of technological expertise in the digital economy within successive US Administrations, and Congress after 2000 contributed to the failure of the US state to respond to the advocacy of the digital platforms for 'permission-less innovation'.[115] The digital platforms, financed by private internet capital, grew their capacity to exercise structural power because high-tech domestic manufacturing was offshored to global supply chains, in the form of 'transacted forms of capital operating multi-jurisdictionally for the purposes of wealth creation and protection'.[116] The state then became more vulnerable to digital disruption and complex technological and financial interdependencies among de-territorialized digital platforms.

The national security state also became concerned about the erosion of reciprocal public/private relationships.[117] In 2018, then Chairman of the Joint Chiefs of Staff, Joseph Dunford, argued that tech companies needed to review their interest and work with the military because the US industrial base and human capital were the primary sources of the state's 'competitive advantage'.[118] In 2019, citing Project Maven, the Pentagon's AI Algorithmic Warfare project, as an example of the depth of the public/private breakdown, Lieutenant General John Shanahan, Director of the Joint Artificial Intelligence Center, argued that:

> Maven underscores just how deep the chasm is between the commercial tech community and the AI capabilities of DoD and our traditional defense industrial base. This is nearly a complete reversal from how we operated over the previous 50 years; commercial tech is far outpacing DoD's ability to keep up … Commercial tech companies have focused on these AI long lead tasks for more nearly two decades, and they have reaped astonishing benefits … We need to spend as much time working with the National Security Innovation Base as we do with the Defense Industrial Base. It's not one or the other. It must be both. Or we will fail.[119]

[113] Jeff Nesbit, 'Google's true origin partly lies in CIA and NSA research grants for mass surveillance', *Quartz*, 8 Dec. 2017, https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/; Virginia Higgins, *Alliance capitalism, innovation and the Chinese state: the global wireless sector* (Basingstoke: Palgrave Macmillan, 2015), p. 17.

[114] Sargent, 'US research and development funding and performance'.

[115] Amy Webb, *The big nine* (New York: Public Affairs, 2019); Tom Wheeler, *Time to fix it: developing rules for internet capitalism* (Cambridge, MA: Harvard Kennedy Shorenstein Center on Media, Politics and Public Policy, Aug. 2018).

[116] Seabrooke and Wigan, 'Global wealth chains', p. 2; Madeline Carr, *US power and the internet in international relations: the irony of the information age* (Basingstoke: Palgrave Macmillan, 2016), p. 123; Philip Mirowski and Edward Nik-Khah, 'Private intellectuals and public perplexity: the economics profession and the economic crisis', *History of Political Economy* 45: 5, 2013, pp. 279–311.

[117] Robert Work and Greg Grant, *Beating the Americans at their own game: an offset strategy with Chinese characteristics* (Washington DC: Center for a New American Security, 2019).

[118] Joseph Dunford, Joint Chiefs of Staff interview, Halifax International Security Forum, Halifax, Nova Scotia, 17 Nov. 2018, https://halifaxtheforum.org/forum/2018-halifax-international-security-forum/saturday-november-17/#agenda.

[119] Shanahan, 'Emerging technologies and peer competition', p. 13.

An examination of Silicon Valley's defence contracting over the period 2015–2020 reveals a variegated response to the state's technological initiatives.[120] While Maven is an example of military–internet capital tensions in the United States, it does not mean that relationships between defence and the digital platforms are broken. DARPA, the Defence Innovation Unit, AFWERX and Futures Command actively sponsor ideas in conjunction with the digital platforms.[121] A prospective contract in 2022 for the Joint Warfighting Cloud Capability, including top-secret clearance work, involved Google, Oracle, Microsoft and Amazon Web Services because the state recognized their capacity for technological innovation.[122] Our point is not that the state has lost its capacity to exercise transformative power. State sovereignty has not been replaced. Nonetheless, our understanding of the social sources of state power, as traditionally conceived, is challenged by the new sources of social power in the digital economy. The question is the extent to which the challenges to the way we understand state sovereignty signal the emergence of what we suggest is a type of virtual sovereignty. No matter how this question is answered, it is worth asking, because any reconceptualizing of sovereignty disrupts international relations during an era of increasing geopolitical uncertainties and tension.

Virtual sovereignty? Private internet capital and the digital platforms

Let us summarize the observations about power and sovereignty in the digital age that we suggest are worthy of critical attention. Are the US digital platforms demonstrating any attributes of sovereign authority, legitimacy, power and control over the virtual territories of the digital economy? Are they exercising power as a virtual sovereign? We have suggested that they exercised extractive power and control through their ownership and control of the critical software and hardware, creating the virtual territories of the digital stack. We have also argued that the US digital platforms exercise extractive power because their smart social media devices shape individual cognition, emotions and behaviour. With respect to the attributes of authority and legitimacy, however, the digital platforms do not necessarily act with consumers' sufficient, let alone active, consent, particularly given the absence of transparency, explainability and accountability. Onerous terms and conditions for an anxious consumer's desire to access a digital platform's products and services are relieved by a single click without any realization of what has been consented to. How power is exercised here in billions of individual consumer choices and whom it favours is not difficult to deduce. Lazar argues that for a state or digital platform to exercise sovereignty legitimately, citizens must

[120] Jack Poulson, 'Reports of a Silicon Valley/military divide have been greatly exaggerated', *Tech Inquiry*, 7 July 2020, https://techinquiry.org/SiliconValley-Military/.

[121] Poulson, 'Reports of a Silicon Valley/military divide have been greatly exaggerated'; Issie Lapowsky, 'Inside the room where tech actually vies for military jobs', *Wired*, 12 March 2019, https://www.wired.com/story/inside-air-force-demo-day-tech-companies/.

[122] Jim Garamone, *Joint warfighting cloud capability award planned for December*, US Department of Defense, 31 March 2022, https://www.defense.gov/News/News-Stories/Article/Article/2984496/joint-warfighting-cloud-capability-award-planned-for-december/.

not only give consent, but also establish that consent has been given. According to Lazar, 'consent's moral effectiveness depends in part on its being public; the same is true for authorization'.[123] Any social contract between virtual sovereignty and the citizen/consumer is difficult to establish in the absence of transparent procedural legitimacy and security.

Rising economic and racial inequality in the United States, coupled with public debt of more than US$22 trillion in 2019, diminished civil confidence in the legitimacy of the state. Belief in liberal democracy was questioned on social media.[124] The ensuing polarization of politics exacerbated congressional partisanship to the strategic advantage of foreign adversaries. Rodrik argues that widening socio-economic gaps produced by neo-liberal hyperglobalization were amplified for US citizens in social media spaces. This set the conditions, according to Rodrik, for the post-2016 populist political backlash in the United States, which first elected Donald Trump as president and then resulted in the 6 January 2021 attack on Congress and its aftermath.[125] For Rodrik, reducing socio-economic gaps requires the US state to commit to the 'domestic sphere in the policy hierarchy' and 'demote the international' at a time when the state's capacity to do so is declining and the demands of the 'international' are growing.[126] Given the transformative power exercised by digital platforms, the question is whether the state exercises sufficient extractive power to do so in the digital stack.

The answer to that question appears to be no, because the digital platforms, for commercial gain, enable hostile foreign and domestic actors to conduct influence and interference campaigns. Furthermore, they are also driven by commercially motivated business models to buy and sell technology and data to private companies and state-owned enterprises in global supply chains regardless of strategic competition or ill-intent against the United States. The platforms exercise infrastructural power in both aspects by monopolizing the accumulation of big data in real-time cloud storage in digital 'panopticon' and 'chokepoint' forms beyond the geopolitical norms of the Westphalian territory-centric global order.[127] Though the digital platforms defend user rights against state regulation and 'interference', Scott concludes that traditional distinctions between public and private power are blurred when private actors are 'seeing like a state'.[128]

With respect to transformative power specifically, private internet capital's support for start-ups and the digital platforms' commitment to large commercial research budgets far outweigh those of the US state, even in the fields of national defence and security. In some key areas, the US state has relinquished much

[123] Lazar, 'Legitimacy, authority, and the political value of explanations', pp. 7–11.
[124] Peter Trubowitz and Peter Harris, 'The end of the American century? Slow erosion of the domestic sources of usable power', *International Affairs* 95: 3, 2019, pp. 619–39.
[125] Rodrik, 'Populism and the economics of globalization'; Michael Mazarr, *Mastering the grey zone: understanding a changing era of conflict* (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, 2015).
[126] Dani Rodrik, 'Globalization's wrong turn and how it hurt America', *Foreign Affairs*, July–Aug. 2019, https://www.foreignaffairs.com/articles/united-states/2019-06-11/globalizations-wrong-turn.
[127] DeNardis, *The global war for internet governance*; Henry Farrell and Abraham Newman, 'Weaponized interdependence: how global economic networks shape state coercion', *International Security* 44: 1, 2019, pp. 42–79.
[128] James Scott, *Seeing like a state: how certain schemes to improve the human condition have failed* (New Haven, CT: Yale University Press, 2020), p. 1.

of its interest in and capacity to initiate and sponsor technological innovation. In 2019, the Trump administration's Deputy Assistant for Technology Policy, Michael Kratsios, declared the 'neutrality' of digital platforms by arguing that the 'best way forward for America was for Silicon Valley to chart its own course independently without government intervention'.[129] The presence of powerful former digital platform executives in US government administrations blurs the lines between the power of private international capital and the interests of the state.[130]

All of this stands in direct contrast to US international leadership during the Cold War after 1945. At this time, hegemony was supported and sustained by corporate America's industrial and financial enhancement of the state's diplomatic and military power, forging a symbiotic relationship of mutual dependence and benefit.[131] Since the dawn of the digital age, the power and profits of US corporations are secured increasingly not only by this symbiotic relationship, but also via global production and distribution chains outside US markets and beyond state regulation. Public/private relationships in the United States shifted from the state's extractive and transformative facilitation of innovation and incubation of dual-use technologies in the service of the national security state to private internet capital which finances the digital platforms' technological innovation in search of commercial gain.[132]

Conclusion

We have suggested that distinctions between the infrastructural power of the sovereign state and the digital platforms in the United States are blurred in the digital economy. The digital platforms seem to acquire some of the extractive and transformative powers traditionally ascribed to the sovereign state. We accept the development of new virtual territories in a digital stack where a form of 'virtual sovereignty' appears to exhibit the authority and control, though perhaps not the legitimacy, associated with the US state's exercise of infrastructural power. Digital platforms are the digital stack's software and hardware gatekeepers and exclusive service providers. Traditional sovereignty rests on international recognition of claims to territorial monopoly and the legitimate use of violence. The business models of the digital platforms secure private internet capital's investment in the software and hardware upon which a consumer's smart devices and apps rely. The prospect of massive financial rewards from unregulated access to AI, the Internet

[129] Cited in Webb, *The big nine*, p. 86.

[130] See e.g. Kate Conger and Cade Metz, '"I could solve most of your problems": Eric Schmidt's Pentagon offensive', *New York Times*, 3 May 2020.

[131] Weiss, *America Inc.?*; Fred Block and Matthew Keller, 'Where do innovations come from? Transformations in the US economy, 1970–2006' in Fred Block and Matthew Keller, eds., *State of innovation*, (Abingdon: Routledge, 2016), ch. 8, pp. 154–72; Walter Isaacson, *The innovators* (New York: Simon & Schuster, 2014); Kurt Campbell and Jake Sullivan, 'Competition without catastrophe: how America can both challenge and coexist with China', *Foreign Affairs*, Sept.–Oct. 2019, https://www.foreignaffairs.com/articles/china/competition-with-china-without-catastrophe.

[132] Weiss, *America Inc.?*; Isaacson, *The innovators*.

of Things, big data and cloud storage lies beyond the sovereign state's monopoly over regulation and control in the service of national security.

US digital platforms and the private internet capital supporting them influence individual consumer cognition and behaviour in profound ways through the command of innovation, unchecked violations of individual privacy, and real-time collection and purchase by intermediaries of big data then offered for sale to willing advertisers and social influencers. With private internet capital's investment in the platform's capacity to extract and distribute big data comes the capacity for malicious domestic and foreign actors to undermine civil society's consent for state legitimacy. Governance is made more complex by the increasing power of private internet capital and the digital platforms, though we are not arguing that the US state has ceded sovereignty. The US state remains powerful, and the extent to which the digital platforms have acquired legitimacy and authority, which an understanding of sovereignty demands, remains open to debate, given deficiencies in virtual sovereignty's consent, accountability and transparency in the United States.

We strongly suggest further research is carried out into the idea of virtual sovereignty across different types of states in international society. Given that the US state's legitimacy and resilience as a liberal democracy are challenged by hostile domestic and foreign actors, studies of how China and other states operate in the global digital economy to exercise infrastructural and 'outward-facing' power with different political and social arrangements are timely. Such studies are likely to have profound implications for understanding sovereignty and power in international society.