



**Manuscript version: Author's Accepted Manuscript**

The version presented in WRAP is the author's accepted manuscript and may differ from the published version or Version of Record.

**Persistent WRAP URL:**

<http://wrap.warwick.ac.uk/136687>

**How to cite:**

Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

**Copyright and reuse:**

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

**Publisher's statement:**

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: [wrap@warwick.ac.uk](mailto:wrap@warwick.ac.uk).

# *Always in Control?*

## *Sovereign States in Cyberspace*

Sarah Mainwaring

### **Abstract**

*For well over 20 years, we have witnessed an intriguing debate about the nature of cyberspace. Used for everything from communication to commerce, it has transformed the way individuals and societies live. But how has it impacted the sovereignty of states? An initial wave of scholars argued that it had dramatically diminished centralised control by states, helped by a tidal wave of globalisation and freedom. These libertarian claims were considerable. More recently, a new wave of writing has argued that states have begun to recover control in cyberspace, focusing on either the police work of authoritarian regimes or the revelations of Edward Snowden. Both claims were wide of the mark. By contrast, this article argues that we have often misunderstood the materiality of cyberspace and its consequences for control. It not only challenges the libertarian narrative of freedom, it suggests that the anarchic imaginary of the internet as a 'Wild West' was deliberately promoted by states in order to distract from the reality. The internet, like previous forms of electronic connectivity, consists mostly of a physical infrastructure located in specific geographies and jurisdictions. Rather than circumscribing sovereignty, it has offered centralised authority new ways of conducting statecraft. Indeed, the internet, high-speed computing and voice recognition were all the result of security research by a single information hegemon and therefore it has always been in control.*

**Key Words:** cyberspace; boundaries; power; sovereignty; surveillance; USA.

### **Introduction**

Cyberspace is now ubiquitous. Carrying most of our communications, accelerating commerce, increasingly connecting our toasters and toothbrushes, it is transforming the way individuals and societies operate. Long understood as a place of enhanced individual freedom, a romantic vision of this 'space' still dominates many popular imaginaries. Often framed as metaphorical 'Wild West', cyberspace became understood as a place in which authority, boundaries and geography were weak or even did not apply. While attractive, this understanding of cyberspace is misplaced. The libertarian understanding of cyberspace has failed to grasp the extent to which sovereign states historically developed the internet for their strategic advantage. Consequently, more recent attempts by states like Russia and China to assert control or influence over cyberspace are misunderstood as individual, isolated attempts by authoritarian states to master the internet. Rather than anomalies, this article suggests that the long-standing appetite of sovereign states to assert power over and through cyberspace stretches back to the Second World War. More importantly, we should question whether this misunderstanding has not been convenient for governments, enabling them to defend their surveillance practices as an attempt to assert order in a supposedly anarchic space. Tracing the historical trajectory of these developments, the current debate about the 'weaponization of cyberspace' is recast. Rather than a special place from which the 'weary giants' of government were excluded, it was simply an extension of their security activities. The image of cyberspace has been constructed in a way that has misdirected our understanding of the nature of communications technology.

It is not surprising that cyberspace was romantically imagined as a boundless space of freedom. The term was invented in 1984 by the writer William Gibson in the context of his novel '*Neuromancer*' which speaks eloquently of a different 'kind' of space, 'a consensual hallucination experienced daily

by billions... in every nation.’ Emphasising the novelty of a ‘space’ in which individuals and communities could connect beyond traditional (State) mechanisms of control and governance, this ‘space’ was framed through meta-level metaphors, eagerly seized upon by libertarians throughout the 1990s. Perhaps the most famous of these was John Perry Barlow, American poet, cattle rancher, privacy campaigner and lyricist for the Grateful Dead. Responding to the US governments attempts to censor the internet in 1996, he issued a declaration of independence for cyberspace, dismissing states as the ‘weary giants of flesh and steel.’<sup>1</sup> Barlow’s influential language was distinctly utopian and has echoed down the decades. Typically, in 2011, Nicholas Negroponte, creator of *Wired* magazine observed: ‘this is just the beginning, the beginning of understanding that cyberspace has no limits, no boundaries.’ By equal turns, some of this discussion is disturbingly dystopian. Eric Schmidt, long-standing chairman of Google, warns us that: ‘The Internet is the first thing that humanity has built that humanity doesn’t understand, the largest experiment in anarchy that we have ever had.’<sup>2</sup> But what all these narratives have in common is a sense of anarchy and a distinct underappreciation of the ongoing processes by which states are making this space. By contrast, I argue here that the widely accepted libertarian vision of cyberspace has often been convenient, enabling states to conjure up a vision of cyberspace as an untamed ‘Wild West’ of criminality and rebellion in order to legitimate their security activities. This, in turn, raises the bigger question of whether Governments have enabled or encouraged us to misunderstand cyberspace, casting a cloak of obscurity over their activities.

The majority of current accounts within International Relations remain somewhat deterministic, offering ahistorical and non-materialist approaches in which the internet simply accelerates the corrosive effects of globalisation in eroding the authority of the state.<sup>3</sup> As Geoffrey Herrera observed, much of the literature on this subject understands the internet as, at best, a simple accelerator of globalisation and at worst a threat to the future of the nation-state system.<sup>4</sup> Herrera, one of the few International Relations scholars to reflect at length on this subject, argues that writing about the internet often takes the form of a technological determinism that is ‘vastly at odds’ with the historical record.<sup>5</sup> This article extends Herrera’s significant critique, highlighting the ways in which sovereign states have shaped the development of cyberspace. In particular, it challenges the ‘placeless-ness’ narrative, emphasising the importance of the material, physical and historical dimensions of these technologies together with the control this affords.<sup>6</sup>

This effort to recast our understanding of cyberspace draws on the ideas of French philosopher, Henri Lefebvre. Writing in the 1960s, in response to the urban planning of French cities, Lefebvre critiqued the way space was understood as scientific, objective and pure. His celebrated text ‘The Social Production of Space’ changed how space was understood, introducing politics and society to geographical analysis. Created through social relations, he argued that space should be understood as a process. Consequently, researchers and geographers had to think about why space was created, not just

---

<sup>1</sup> John Perry Barlow, ‘A Declaration of the Independence of Cyberspace’, Electronic Frontier Foundation, available at: {<https://www.eff.org/cyberspace-independence>} accessed 1st October 2019

<sup>2</sup> Jerome Taylor, ‘Google Chief: My Fears for Generation Facebook.’ *Independent*, 22 October 2011. Available at: {<http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-chief-my-fears-for-generation-facebook-2055390.html>.} Accessed 27<sup>th</sup> November 2018.

<sup>3</sup> See for example Kevin Robins, ‘Cyberspace and the world we live in’, *Body & Society*, 1:3-4 (1995), pp.135-155; Martin Dodge and Rob Kitchin, *Mapping cyberspace* (London: Routledge, 2003); Christian Fuchs, *Internet and society: Social theory in the information age* (London: Routledge, 2007).

<sup>4</sup> See for example Ryan Henry and Edward Peartree, ‘The Information Revolution and International Security’ (Washington, CISI, 1998); Ronald Deibert, ‘Circuits of Power: Security in the Internet Environment’, in J. Rosenau and J.P. Singh (eds.), *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (New York: SUNY, 2002), pp.115–42; Robert Latham, *Bombs and Bandwidth: The Emerging Relationship Between IT and Security* (New York: The New Press, 2003); Yale Ferguson and Richard Mansbach, *Remapping Global Politics: History’s Revenge and Future Shock* (Cambridge: Cambridge University Press, 2004).

<sup>5</sup> Geoffrey Herrera, ‘Cyberspace and sovereignty: thoughts on physical space and digital space’, in Myriam Dunn Cavelty and Victor Mauer (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (London: Routledge, 2016), pp.81-108.

<sup>6</sup> Ibid. See also Geoffrey Herrera, *Technology and international transformation: The railroad, the atom bomb, and the politics of technological change* (New York: SUNY Press, 2012).

what was ‘in’ it.<sup>7</sup> Underlying the politics of space, he was at pains to emphasise the way cities and urban planning were the products of history, politics and social relations, rather than simply ‘natural space’.<sup>8</sup> In many ways, cyberspace is not dissimilar to the 1960s French urbanism that sparked Lefebvre’s ideas. Originating in the American defence industry, cyberspace has evolved in ways that fit remarkably well onto the map of Westphalian sovereign states. Governments of all kinds have produced cyberspace for their strategic advantage. In Lefebvre’s language, cyberspace ‘is also a means of control, and hence of domination, of power.’<sup>9</sup> This article seeks to explore the diverse and often conflicting ways states have seen and used cyberspace in this way.

Lefebvre’s ideas were further developed by Doreen Massey’s writings on globalisation.<sup>10</sup> Critiquing many of the abstracted and utopian notions of globalisation, she pointed out that it ‘doesn’t float above the earth, it is operated by the same material, social, embedded processes of people in branch plants, in production factories, in research organisations, making decisions which may or may not work out all around the world.’<sup>11</sup> Similar observations might be made about cyberspace which has also been described as a floating cloud or libertarian tool of freedom that has reduced governmental power and authority. This space did not emerge organically but is the product of interrelations, ‘constituted through interactions, from the immensity of the global to the intimately tiny.’<sup>12</sup> Moreover, viewed as a product of fluid, ongoing relations, the idea that cyberspace has arrived as a complete entity is also challenged in favour of a continuum.

Unsurprisingly, geographers have been consistently important in urging us to appreciate the importance of territory as a process.<sup>13</sup> Most prominently, Gerard O Tuathail argues that cyberspace, much like the contemporary world financial system ‘is not the product of natural forces... but of a new working relationship between States and markets promoted, in part, by the States themselves... geography is not so much disappearing as being restructured, rearranged and rewired.’<sup>14</sup> Importantly, he suggests that our misunderstanding of cyber is part of an attempt to ‘denaturalise and limit the power of States while naturalising the virtues of the markets.’<sup>15</sup>

The possibility that this new ‘space’ enhances state power through surveillance is critically important, and is largely overlooked within the libertarian consensus.<sup>16</sup> The debate over the role of communications technologies and the Arab Spring typifies this narrative.<sup>17</sup> Initially, these events were hailed as evidence of the transformative impact of telecommunications technology across North Africa and the Middle East. Typically, Howard and Hussain suggested that this ‘space’ created through Social Media and other platforms represents a substantive shift from historical mechanisms of social governance and ordering. Reducing entry costs of traditional forms of heavily regulated media like

---

<sup>7</sup> Henri Lefebvre, *The Production of Space* (London: Wiley-Blackwell, 1991)

<sup>8</sup> Henri Lefebvre, ‘Reflections on the Politics of Space,’ *Antipode*, 8:1 (1976), p. 31

<sup>9</sup> Lefebvre, *The Production of Space*, p. 26.

<sup>10</sup> Doreen Massey, *for space* (London: Sage, 2005).

<sup>11</sup> Doreen Massey, *Power Geometries and the Politics of Space-Time* (Heidelberg: University of Heidelberg Press, 1999), p.50

<sup>12</sup> Massey, *for space*, p.9

<sup>13</sup> Juliet J. Fall, ‘Artificial States? On the enduring geographical myth of natural borders,’ *Political Geography*, 29:2 (2010), pp.140-47.

<sup>14</sup> Gearoid O Tuathail, ‘Borderless worlds? Problematising discourses of de-territorialisation,’ *Geopolitics*, 4:2 (1999), pp.139-154.

<sup>15</sup> *Ibid.*, p.147.

<sup>16</sup> Our conception of state power and surveillance derives from David Lyon, *Surveillance Society: Monitoring Everyday Life* (London: McGraw-Hill, 2001).

<sup>17</sup> Naila Hamdy and Ehab Gomaa, ‘Framing the Egyptian uprising in Arabic language newspapers and social media,’ *Journal of Communication*, 62: 2 (2012), 195-211; Sahar Khamis, Paul B. Gold, and Katherine Vaughn, ‘Beyond Egypt’s “Facebook Revolution” and Syria’s “YouTube Uprising:” Comparing Political Contexts, Actors and Communication Strategies,’ *Arab Media & Society*, 15:1 (2012); S. Khamis, & K. Vaughn, ‘We Are All Khaled Said: The potentials and limitations of cyberactivism in triggering public mobilization and promoting political change,’ *Journal of Arab & Muslim Media Research*, 4:1 (2012), 145-163; M. Nanabhay & R. Farmanfarmaian, ‘From spectacle to spectacular: How physical space, social media and mainstream broadcast amplified the public sphere in Egypt’s revolution,’ *Journal of North African Studies*, 16:4 (2011), 573-605.

television commercials or radio channels, social movements were liberated through both ubiquity and anonymity. 'When physical spaces for public conversation and debate closed down,' they argue, 'the Internet provided virtual spaces for political communication.'<sup>18</sup> Cyberspace was framed as empowering social movements and dissenting individuals, providing an alternative space that facilitates freedom of expression or association.<sup>19</sup>

More recently, scholars have revised their view in two ways. First, they have become more sceptical about the role of social media in generating the Arab Spring and, secondly, they have argued that states have since become more adept at controlling it.<sup>20</sup> Slowly but surely, they have moved in the direction of the iconoclastic technology critic Evgeny Mozrov, accepting that authoritarian states like China have successfully countered Google and built their own local intranet or 'splinternet'.<sup>21</sup> But even this narrative is incorrect, overlooking the significant ways in which sovereign states in the liberal democratic sphere have consistently exerted control and authority over these technologies, albeit in more hidden ways.

Indeed, surveillance experts have now begun to speak of a sinister innovation called 'social media intelligence'. David Omand, a former Director of GCHQ and Carl Miller of DEMOS have sketched out a whole new terrain of state-driven forecasting activity that draws on data from things like twitterfeed. Social media intelligence (SOCMINT) includes a range of techniques and technologies that facilitate the watching of social media networking sites such as Facebook or Twitter. Although this has been around for many years, typically with police analysts scanning protester chat rooms, the move is towards using bigger data for spotting trends and undertaking sentiment analysis. The result is something that hovers in the liminal space between intelligence and behavioural social science, offering the holy grail of predicting future political events. The way in which social media, once seen as a voice from below, has become the latest intelligence tool for those watching from above, is perhaps indicative of the direction of travel.<sup>22</sup>

Ultimately, cyberspace has transformed how we might understand future governance. Rather than signalling the decline of the importance of Westphalian States, it has enabled sovereign power to evolve, creating new means of governance and reinforcing centralised power and authority in significant ways. All of these realities are lost in the romantic vision of cyberspace as a libertarian playground of de-territorialised freedom. Emphasising the historic and enduring importance of sovereign authority to cyberspace recovers its intrinsically material, territorial, and state-based origins that can be fortified, not challenged, under globalizing conditions. The underlying physical infrastructure of Cyberspace is important not just because it is based on physical lands or ran by people. It is important because States have been able to use these physical components to control and exert influence through this 'space.' In an age of nation-state hacking and grand disinformation campaigns, the willingness of states to exploit cyberspace shows little sign of abating. We perhaps need a stronger appreciation of the long history of these tendencies, finally appreciating the true scale and impact of states in cyberspace. At root, as Lefebvre suggests, it 'is not a scientific object removed from ideology or politics; it has always been political and strategic.'<sup>23</sup>

## Materiality

Perhaps the most fundamental way cyberspace has been used by states is one of the most well-hidden. Lost within a romantic understanding of cyberspace as a 'mysterious world,' we overlook the way

---

<sup>18</sup> Philip Howard & Muzammil Hussain 'Democracy's Fourth Wave? *Digital Media and The Arab Spring* (Oxford: Oxford University Press, 2013), p.5.

<sup>19</sup> Nevertheless, there is quite a lot of work on how state bordering practices for example Louise Amoore, *The politics of possibility: Risk and security beyond probability* (Duke University Press, 2013); Louise Amoore, 'Algorithmic war: Everyday geographies of the War on Terror,' *Antipode* 41:1 (2009) pp.49-69.

<sup>20</sup> C. Byun, & E.J. Hollander, 'Explaining the intensity of the Arab Spring', *Digest of Middle East Studies*, 24: 1 (2015), 26–46; A. Smidi & Saif Shahin, 'Social Media and Social Mobilisation the Middle East: A Survey of Research on the Arab Spring, *India Quarterly*, 73: 2 (2017) pp.196-209.

<sup>21</sup> Michael Meyer, Evgeny vs. the internet', *Columbia Journalism Review*, Jan/Feb 2014.

<sup>22</sup> David Omand, Jamie Bartlett, and Carl Miller, 'Introducing social media intelligence (SOCMINT),' *Intelligence and National Security*, 27:6 (2012), 801-823.

<sup>23</sup> Henri Lefebvre, 'Reflections on The Politics of Space,' *Antipode*, 8:1 (1976), p.31

cyberspace has been constructed and designed by state authorities. Hidden in plain sight, the physicality and infrastructure of cyberspace remains attached to and reliant upon a physical territory. This enables States to control and influence these electronic environments, often for their advantage. While the view of figures like Dan Hunter who see cyberspace as a ‘global commons’<sup>24</sup> is attractive, it overlooks the significance of these physical and geographical dimensions. It is to these, perhaps mundane aspects of cyberspace, that this article now turns. Echoing Mark Graham, we must recognise that cyberspace is not an ‘abstract space or digital global village’ but a constructed network or system of information exchange. Sovereign authorities are central to this construction, often making some of the most important decisions about its location and design. Despite perceptions of the internet as a global commons and public good, the internet has been constructed along geographical lines that are remarkably congruent with established borders and boundaries. Consequently, we need an alternate, nuanced and more ‘spatially grounded’ way of understanding how cyberspace has developed over time.<sup>25</sup>

Why are the physical or territorial components of cyberspace are so frequently overlooked? The most persistent users of misleading meta-level metaphors are Presidents and Prime Ministers. Their purpose is to frame threat complexities in terms of an unruly environment that is imperfectly policed and beyond law and order. On 28 March 2018, UK leader Theresa May, outlining her new National Cyber Security Strategy, was at pains to draw a distinction ‘between the cyber and physical worlds’, while a week before, her Secretary of State with responsibility for this area, Matt Hancock, unveiled new regulations for electronic commerce as heralding a future in which the internet would cease to be the ‘Wild West’.<sup>26</sup> Similarly, in 2016, Obama deployed almost the same language at the G-20 Summit in Hangzhou, China, insisting that ‘we cannot have a situation where this “space” becomes the Wild Wild West’, and calling for measures that would enable greater surveillance and offensive capabilities within this domain.<sup>27</sup> Despite their frequency, these statements have a negative consequence, obscuring the very real, significant dependencies of this environment on physical attributes and control.

Recently, the Tongan population experienced this physicality. In January 2019, an undersea fibre optic cable connecting Tonga to the internet through the Indian Ocean was damaged. Risking the population’s communications, healthcare and labour market, the event forced Tonga to rely on one single satellite dish for its communications and national infrastructure. The satellite link offered less than one per cent of the capacity offered by the severed cable and the result was a huge disruption. Tom Westbrook of Reuters reported that the incident was ‘throwing communications across the tiny and isolated country into chaos.’<sup>28</sup> Most strikingly, reports indicated how it ‘prompted hundreds of people to queue outside a government telecom office where the signal is most reliable... hours have been extended to midnight to handle crowds of officials, business people and ordinary folk logging on to access cash remittances, buy plane tickets and chat.’<sup>29</sup>

Few internet users pause to consider the journey their data takes between each transaction. A mere 400 fibre optic cables carry 99% of transoceanic data, comprising ‘the physical links that bind our digital world together.’<sup>30</sup> The mode of transport is undersea cables that look rather like garden hosepipes, laid down by specialist ships across the bottom of the ocean. Far removed from images of

<sup>24</sup> Dan Hunter, ‘Cyberspace as Place and the Tragedy of the Digital Anti-commons’, in Paul Schiff Berman (ed.) *Law and Society Approaches to Cyberspace* (London: Routledge, 2017), pp.59-139.

<sup>25</sup> Mark Graham, ‘Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?’, *The Geographical Journal*, 179:2 (2013), pp.177-182.

<sup>26</sup> Chris Baynes, ‘New laws to tackle “Wild West” internet will make UK “safest place in the world” to be online, Matt Hancock claims’, *Independent*, 20 May 2018.

<sup>27</sup> Nick Allen, 2016, ‘Barack Obama warns of Cold War-style “cyber arms race” with Russia’, *Telegraph*, 5 September 2016. Available at: (<https://www.telegraph.co.uk/news/2016/09/05/barack-obama-warns-of-cold-war-style-cyber-arms-race-with-russia/>) Accessed 2<sup>nd</sup> April 2019.

<sup>28</sup> Tom Westbrook, ‘Severed Cable Sends Tonga ‘Back to Beginning of the Internet.’, Reuters, 23<sup>rd</sup> January 2019 Available at: (<https://www.reuters.com/article/us-tonga-internet/severed-cable-sends-tonga-back-to-beginning-of-the-internet-idUSKCN1PI0A8>) Accessed 2<sup>nd</sup> April 2019

<sup>29</sup> Westbrook, ‘Severed Cable Sends Tonga ‘Back to Beginning of the Internet.’.

<sup>30</sup> Garrett Hinck, ‘Cutting the Cord: The Legal Regime Protecting Undersea Cables.’ *Lawfare Blog*, November 2017. Available at (<https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables>) Accessed 2<sup>nd</sup> April 2019



ethereal 'clouds' void of physical territory, these cables of glass and metal form the backbone of the internet and they are often strangely fragile. Alexandra Chang of *Wired* magazine observed how 'they are for the most part poorly armoured, rarely patrolled and only occasionally monitored.'<sup>31</sup> Andrew Blum, the author of *Tubes*, a fascinating archaeological journey to the centre of the internet, also finds their vulnerability rather remarkable.<sup>32</sup>

A further striking example of our misunderstanding of cyberspace is the idea of the 'Cloud'.<sup>33</sup> This is an example of the problem of using metaphors and grand statements to describe an industrial mixture of server farms, data warehouses and software as service.<sup>34</sup> Obscured through an image of our data being transported into a 'cloud' above us, instead the industrial skeleton of cyberspace exists in the forms of fibre optic cables, metal pylons and satellite dishes, human resource and water supplies. In fact, the industrial skeleton of cyberspace continues to exist in the form of miles of fibre optic cables, metal pylons and satellite dishes, together with server farms in vast metal sheds that demand considerable amounts of water and electricity.<sup>35</sup> One of the largest is the Next Generation Data Europe centre in Newport, Europe's major data centre facility. Over 19,000 server cabinets plus storage are displaced across three floors that cover 750,000 square feet and - while impressive - it has little resemblance to a cloud.<sup>36</sup>

Discussing examples of this infrastructure uncovers the rather mundane ways cyberspace is governed and maintained in the 21<sup>st</sup> century. Many geographers have commented on this hidden aspect of cyberspace, but few have speculated as to the rationale. From the perspective of the everyday user, they are seemingly happy that the wiring is hidden behind and beneath user interfaces. Shannon Mattern explores this idea, suggesting that it is easy to forget 'how they delimit our agency and how they are defining the terrain we are interfacing with.'<sup>37</sup> Extending this idea of the physicality of cyberspace, Louise Amoore reminds us that 'as computer science began to document the emergence of cloud computing, geography came to have a specific meaning, defined by where data and programs are spatially stored.'<sup>38</sup> DeNardis, similarly reminds us that, 'root servers are housed in buildings and run by people.'<sup>39</sup> But what does this tell us about the power of states and corporations?

Rather than being unbridled or organic, we need to recognise that 'at the core of the internet is a series of components that are infrastructural: internet exchanges, national backbone networks, regional networks and local networks.'<sup>40</sup> As Saskia Sassen suggests, we should recognise that the digital networks of cyberspace are not only comprised of hardware and software but societal structures and power dynamics that also have considerable materiality: 'There is no purely digital economy, just as there is no virtual corporation or community.'<sup>41</sup> Connections between the 'real' and 'cyber' worlds are all around us, located under pavements and along motorway pylons. Hidden in plain sight, these infrastructure layers clearly demonstrate both the physicality of cyberspace and its connections with sovereign territories.

Simultaneously, they highlight connections between cyberspace and 'old industrial cities' as centres of power, traditionally associated with sovereign control. Graham writes forcibly on this,

---

<sup>31</sup> Alexandra Chang. 'Why Undersea Cables are More Vulnerable than You Think.' *Wired Magazine*. 2<sup>nd</sup> April 2013. Available at: (<https://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/>) Accessed 2<sup>nd</sup> April 2019

<sup>32</sup> Andrew Blum, *Tubes: A Journey to the Center of the Internet* (New York: Ecco, 2012).

<sup>33</sup> Paul Jaeger, Jimmy Lin, and Justin Grimes, 'Cloud computing and information policy: Computing in a policy cloud?' *Journal of Information Technology & Politics*, 5:3 (2008), pp.269-83.

<sup>34</sup> Rajkumar Buyya, et al., 'Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,' *Future Generation computer systems*, 25:6 (2009), pp.599-616.

<sup>35</sup> Amoore, 'Cloud Geographies,' p.5.

<sup>36</sup> Philip Stafford, 'Next Generation Data explores listing', *Financial Times*, 28 June 2010.

<sup>37</sup> Shannon Mattern, 'Interfacing Urban Intelligence,' in Rob Kitchin, Sung-Yueh Perng (eds.) *Code and The City*. (London: Routledge, 2016), pp.49-60.

<sup>38</sup> Louise Amoore, 'Cloud Geographies: Computing, Data, Sovereignty', *Progress in Human Geography*, 42:1 (2018) pp.4-24.

<sup>39</sup> Laura DeNardis. 'The Internet Design Tension between Surveillance and Security,' *IEEE Annals of the History of Computing*, 37:2 (2015), pp.72-83

<sup>40</sup> Sassen, *Territory, Authority, Rights*, p.330

<sup>41</sup> *Ibid.* p. 341

arguing that the reliance on metaphors obfuscates ‘complex relations between new communications and information technologies and space, place and society’. Rather than developing organically and sporadically, the concentration of ‘virtual cities’ within metropolitan cities of New York and London (for example) are used to demonstrate that, as with television, radio and printing technologies, ‘any cursory examination of the Internet and the World Wide Web shows that much of the traffic represents and articulates real places and spaces.’<sup>42</sup> Thus, not only is cyberspace socially constructed and contingent, it is created and implemented for specific uses and needs, notably ‘the very cultural roots of modern capitalist society.’<sup>43</sup> Social scientists might give more weight to these connections, understanding cyberspace within its social, political and historical context. Seen through the lens of Victorian industrialism, cyberspace becomes viewed as the latest social technology, impacting society in similar ways that the steam-engine and teleprinter did before.

Lawyers have been quicker than many to identify the physical and historical connections between internet technology and sovereignty, often viewing these things through the prisms of ownership or jurisdiction. Mark Lemley is one example, offering a typically materialist prescription, arguing that no-one is ‘in’ cyberspace. The internet, he suggests, is merely a protocol, a piece of code that permits computer users to transmit data between their computers using existing communications networks. There were computer networks before the internet that similarly relied on telephonic exchange of data.<sup>44</sup> By emphasising historic connections between the *telegram*, the *television* and *telecommunication*, Lemley directly questions the validity of viewing cyberspace as a mysterious and separate world when similar approaches to the telegram and television are absent: ‘People may speak occasionally of being ‘lost in’ or ‘transported’ by a television show, a movie, or even a book, but we hardly surrender our understanding that ‘television space’ is merely a series of images transmitted to us.’<sup>45</sup>

Understood as *both* physical infrastructure *and* social relations, cyberspace is, as Stanley Brunn argues, transforming the nature of states and what it means to have power in the 21<sup>st</sup> century, but not displacing them.<sup>46</sup> Rather than being void of physical or political territory, global networks are the product and reproduction of political, historical and social relations. Within these networks, geography and place remain important, embedded this infrastructure within sovereign parameters. We thus need to challenge Steven Spiegel’s claims that the post-Cold-War era was one characterised by the ‘diminishing role of geography.’<sup>47</sup> While the last twenty years have undoubtedly been characterised by globalised communications and the oft-celebrated ‘information revolution,’<sup>48</sup> sovereignty and physical territory remain important.

Within this new context, sovereignty and state authority is changed, not erased. Travelling and existing between diverse infrastructural ‘layers,’ power and governance are transformed. Those seeking to find a useful mezzanine between the ethereal, the cultural or physical have been attracted to the idea of layers. Klimburg suggests a four-layer model that incorporates i) the physical or hardware layer; ii) the logic layer (code); iii) the data layer (photographs, e-mails, data); and iv) the social layer. But he adds that in reality, the internet resembles the telephone systems from which it grew: ‘the backbone of the Internet is made of cables that run across continents and under the seas, with a smattering of satellite links as well.’<sup>49</sup> Bratton’s much-discussed analysis simply extends Klimburg’s idea further, exploring the six layers of “The Stack”, independent but intrinsically connected: Earth, Cloud, City, Address, Interface and user.<sup>50</sup>

---

<sup>42</sup> Stephen Graham, ‘The end of geography or the explosion of place? Conceptualising space, place and information technology,’ *Progress in Human Geography*, 22:2 (1998), p.173.

<sup>43</sup> Graham, ‘The end of geography or the explosion of place?’

<sup>44</sup> *Ibid.*, pp.522-4.

<sup>45</sup> *Ibid.*, p.523.

<sup>46</sup> S. D. Brunn, ‘Towards an understanding of the geopolitics of cyberspace: Learning, re-learning and un-learning’, *Geopolitics*, 5:3 (2000), p. 146

<sup>47</sup> S. L. Spiegel, ‘Traditional space vs. cyberspace: The changing role of geography in current international politics’, *Geopolitics*, 5:3 (2000), p. 115

<sup>48</sup> *Ibid.*, p.123

<sup>49</sup> Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (London: Penguin, 2014), p.31.

<sup>50</sup> Bratton, *The Stack*.



Importantly, both models emphasise the relationship between sovereign authority, electronic networks and physical infrastructure. Simply put – they highlight the connections between the ‘electronic’ and ‘physical’ worlds. This is important, adding further weight to the challenge this article poses to the libertarian understanding of cyberspace. Less romantic and attractive than mystery, cyberspace is composed of cables, data centres, protocols, energy supply, buildings and people. At once physical *and* electronic, these layers combine to create what Bratton terms ‘new spaces in its own imaginary: clouds, networks, zones, social graphs, ecologies, megacities, formal and informal violence, weird theologies, all imposed on the other.’<sup>51</sup> Sovereign authority exists within this new environment, adapting and responding to changes around it.

### **State sovereignty and national boundedness**

The dexterity this physical infrastructure affords sovereign states is not insignificant. Building and expanding particular networks, governments have been remarkably adept at shaping the form and nature of cyberspace for strategic or political ends. China is perhaps the most widely discussed, famously constructing her ‘Great Firewall of China’ to advance the country’s comprehensive censorship system.<sup>52</sup> The manner in which China was able to vanquish Google and now appears to be able to defeat even complex anonymising software for browsing the web underlines the degree of control. Recent revelations of possible connections between Huawei and the Chinese Government are seen by some as the latest in a series of efforts to control and influence this so-called ‘fluid’ space.<sup>53</sup> These events, however, are often incorrectly viewed by the libertarian narrative in isolation. Rather than single events or attempts by particular ‘rogue’ states to subvert the existing status quo, this is perhaps indicative of a widespread appetite and ability of states across the globe to extend their authority by working together. Typically, the cybersecurity treaty signed by China and Russia in 2015 which was largely about containing threats from dissident elements.<sup>54</sup>

The weaponization of cyberspace for strategic advantage is perhaps the clearest example of this trend. Sitting awkwardly with acclamations of the untamed ‘Wild West’ by premiers, is emerging evidence of advanced states intentionally harvesting the power of cyberspace for their military and political advantage. We perhaps need to pay far more attention to these examples. This use of offensive measures in this context is something that many government officials have been rather anxious to avoid discussing, and have therefore only recently surfaced in the academic literature. Yet it is now clear that these practices actually began during the 1980s, suggesting that the US National Security Council mapped a geostrategic mindset from the surveillance leviathans of the Cold War directly into cyberspace.<sup>55</sup>

In May 2017, the world received a sudden reminder of the dangers of cyberspace in the form of the WannaCry ransomware attack. This was a global cyberattack by crypto-worm, a self-propagating virus, which focused on computers running the Microsoft Windows operating system. It worked by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency in return for the release of the data. Although Microsoft had released updates to close the vulnerability, WannaCry continued to spread amongst organizations that had not updated their computers, or who were using Windows systems that were no longer supported. Although Microsoft released further emergency patches, Wannacry was mostly stopped because of the chance discovery of a kill switch that prevented it from spreading. Impacting some 200,000 computers across 150 countries, and with costs estimated in the billions of dollars, security experts pointed to North Korea or agencies working for the country, as the

---

<sup>51</sup> Ibid., p.52.

<sup>52</sup> Oliver Farnan, Joss Wright, and Alexander Darer, ‘Analysing Censorship Circumvention with VPNs via DNS Cache Snooping,’ *2019 IEEE Security and Privacy Workshops*; Shin Joung Yeo, ‘Geopolitics of search: Google versus China?’ *Media, Culture & Society*, 38:4 (2016) pp. 591-605; Daniel Anderson, ‘Splinternet behind the great firewall of China,’ *Queue*, 10:11 (2012), p.40.

<sup>53</sup> Nigel Inkster, ‘The Huawei Affair and China’s Technology Ambitions,’ *Survival* 61:1 (2019), pp.105-11.

<sup>54</sup> Adam Segal, ‘When China Rules the Web: Technology in Service of the State,’ *Foreign Affairs*, 97 (2018) p.10.

<sup>55</sup> Fred Kaplan, *Dark Territory: The Secret History of Cyber war* (New York: Simon and Schuster, 2016) pp.57-87.

culprit.<sup>56</sup> In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.<sup>57</sup>

With no immediately identifiable author, the attack appeared to validate the Wild West view of a libertarian cyber-space, inhabited by criminals and paedophiles, a world in which States were weak and losing control. The subsequent attribution to North Korea only seemed to underline the idea of rogue actors. However, over time a rather different story emerged that pointed instead to the world's information hegemon and underlines how organisations like America's NSA and Britain's GCHQ work to maintain information supremacy. Although the press initially suggested that Wannacry was 'released' by an individual hacker, and then blamed North Korea, in fact, the North Korean hackers were mere middlemen. WannaCry was built around an exploit called EternalBlue, developed by the codebreakers of the United States National Security Agency (NSA) for older Windows systems. EternalBlue was then stolen and leaked by a group called 'The Shadow Brokers' a few months before the attack. As Amy Zegart, Stanford University's top intelligence expert has argued, this was a problem of NSA's own making. In other words, the wildest part of the Wild West was actually being developed by the most powerful government in the world to attack other governments.<sup>58</sup>

Statements by Microsoft officials hint at the possibility that both Microsoft and the NSA were aware that this electronic weapon had been leaked, producing a 'patch' or 'cure' for systems through updates in March 2017, perhaps explaining why many of the systems successfully targeted were running old software that had not been updated, notably the UK National Health Service computer systems.<sup>59</sup> This not only demonstrates the curious power relations that exist in cyberspace, it also reminds us that sovereign states remain central to the stability or instability of the internet, working 'behind the screens' of the average computer user scrolling through their social media. This apparently 'uncontrollable space' remains commanded by traditional 'weary giants', at least in terms of the exclusive ability to manufacture advanced persistent threats.<sup>60</sup>

Accordingly, President of Microsoft, Brad Smith, has been vocal about states in cyberspace. He used the Wannacry attack to argue that sovereign entities and their territories enjoy too *much* power, not too little. If there was a potential for chaos on the internet, it lay not with drug dealers prowling the dark web but with the military-intelligence complex: 'Governments of the world should treat this attack as a wake-up call. This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem.'<sup>61</sup> In 2017, speaking at RSA, the world's most important internet security conference, he outlined his ideas for a Digital Geneva Convention focused on restricting what he called the growing problem of electronic attacks by states on citizens in times of peace. While the issue of precise nature of the partnerships between government and industry in the development of 'Cyber-vulnerabilities' is beyond the scope of this paper, this episode is a clear example of states using cyberspace as a tool of statecraft. It also alludes to a broader question of liability, raising the possibility that courts may find states to be both the source and the legally culpable body for some attacks, ultimately paying compensation to corporations and citizens. The fact that the CIA appointed an experienced lawyer in 2008 to consider legal liabilities arising from its cyberwarfare and information programmes underlines the fact that these activities have become routine for the United States for quite some time.<sup>62</sup>

The United States is not the only country that has disassembled. For decades, the more powerful governments have framed cyberspace through the anarchic language of the 'dark web,' justifying measures that allow them to further extend their control. The Indian Government is one example.

---

<sup>56</sup> Richard J. Aldrich, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (London: Collins, 2<sup>nd</sup> edition, 2019), pp.560-73.

<sup>57</sup> Thomas Bossert, 'It's Official: North Korea Is Behind WannaCry', *Wall Street Journal*, 18 December 2017.

<sup>58</sup> A. Zegart, 'The NSA Confronts a Problem of Its Own Making', *The Atlantic*, 29 June 2017.

<sup>59</sup> James Titcomb, 'Microsoft slams UK government over global cyber-attack.' 15<sup>th</sup> May 2017 Available at: <https://www.telegraph.co.uk/technology/2017/05/15/microsoft-slams-us-government-global-cyber-attack/> Accessed 2<sup>nd</sup> April 2019.

<sup>60</sup> Zegart, 'The NSA Confronts a Problem of Its Own Making'.

<sup>61</sup> Brad Smith, 'The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack.' Microsoft Blog, 2017 Available at: <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/> Accessed 2<sup>nd</sup> April 2019.

<sup>62</sup> Private information.

Crafting an image of this environment as an uncontrollable ‘dark place,’<sup>63</sup> draconian encryption policies were justified in 2015, pressuring internet companies to share access to encrypted data with law enforcement agencies. Echoing similar accusations that emerged in Britain and the United States as the result of the revelations made by Edward Snowden, Morsi’s Government, leading the world’s largest democracy, was accused of devising a ‘snooping and spying orgy’ through such policies.<sup>64</sup> Such brazen activities by the world’s largest democracies sit awkwardly with suggestions by writers like Haufler that the internet’s decentralisation and fluidity restrict efforts to ‘design and implement effective regulations through top-down, government-by-government approaches.’<sup>65</sup>

India’s attempts to regulate and compartmentalise cyber-‘space’ are further illustrated by the new Information Technology Act, obliging all companies wishing to collect data on citizens to do so through agreed standards, obtaining consent and privacy policies, influencing standards for data retention and processing within national boundaries.<sup>66</sup> Considering India’s command of 43% of the global business outsourcing for the Information Technology sector, the Indian intervention is significant, with a potential future global impact. This stands in contrast not only to the libertarian presentation of an ethereal space, but also to neoliberal assertions that ‘frontiers are irrelevant to electronic flows and marketing,’<sup>67</sup> a growing body of evidence suggests that ‘walled gardens’ may be emerging across the ‘global commons’ of cyberspace, somewhat removed from visions of a ‘place for enacting dreams of freedom’.<sup>68</sup>

BRICS nations are also pushing back against the cloud. Mandating the storage of Brazilian data on its own servers in response to the Snowden affair, Brazil’s approach to data sovereignty stands in direct contrast with those who champion the emergence of the global ‘data-cloud’ as undermining hierarchical control of data by states and the confirming rise of the global corporates.<sup>69</sup> Similarly, the BRICS’ signing of the Final Acts of the World Conference on International Telecommunications in 2012 and preference for localisation of data sovereignty extends this point, standing in explicit opposition to Western hesitancy towards ‘erecting Schengen zones for data.’<sup>70</sup> Drawing on Foucault, Jeremy Crampton argues that the very ‘mapping’ of cyberspace is imbued with competition, adding that this ‘space’ has been ‘made’ or ascribed meaning through the application of boundaries/territories by the powerful. In doing so, this ‘space’ has been socially constructed and understood in ways that echo the understanding of the physical world.<sup>71</sup>

Does this potentially mean the end of the world-wide-web? The information and communications industry have been quick to note the importance of these developments. Writing in 2015, Microsoft’s Eric Schmidt identified what he called the emergence of the ‘Splinternet:’ in other words different cyberspaces which fit remarkably well onto the old political maps of nation-states. He insists that the ‘Web has become a battleground for wars initiated by States.’<sup>72</sup> Rather than a global, trans-national ‘space’ of freedom, cyberspace is instead increasingly intertwined with, and constrained by, the complexities of territorial politics.

While the role and agency of powerful states like America, Russia and China are often discussed as examples of illegitimate attempts by nations to infiltrate cyberspace, they are at best, the

---

<sup>63</sup> Allie Coyne. ‘Australian govt will introduce decryption laws before end of year.’ 14<sup>th</sup> July 2017 ITNEWS. Available at: {<https://www.itnews.com.au/news/australian-govt-will-introduce-decryption-laws-before-end-of-year-468360>} Accessed 23<sup>rd</sup> March 2019.

<sup>64</sup> Reuters Report. ‘Uproar over Indian encryption law forces government to retreat.’ 22<sup>nd</sup> September 2015. Available at: {<https://www.reuters.com/article/us-india-encryption-law/uproar-over-indian-encryption-law-forces-government-to-retreat-idUSKCN0RM1CO20150922>} Accessed on 2<sup>nd</sup> April 2019.

<sup>65</sup> Virginia Haufler, *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy* (New York: Carnegie Endowment for International Peace, 2011).

<sup>66</sup> Polatin-Reuben & Wright, ‘An Internet with BRICS Characteristics’, p.4

<sup>67</sup> Manuel Castells, ‘Network Society’ in Frank Webster, *Theories of the Information Society* (London: Routledge, 2014), pp. 98-123.

<sup>68</sup> Malcomson, *Splinternet*, p.7

<sup>69</sup> Vincent Mosco, *To The Cloud: Big Data in a Turbulent World* (London: Routledge, 2016).

<sup>70</sup> Polatin-Reuben & Wright, ‘An Internet with BRICS Characteristics’, p.1

<sup>71</sup> Jeremy Crampton, *The Political Mapping of Cyberspace* (Chicago: University of Chicago Press. 2003).

<sup>72</sup> Scott Malcomson, *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web* (New York: OR Books, 2015), p. 7.

tip of the cyber iceberg.<sup>73</sup> Academic experts researching the secretive world of cyberweapons not only assert their long history but also their proliferation. In the last decade, states of all sizes have entered the field, often with parallel programmes in different departments and ministries of the same government. Like any new weapon, its very ‘newness’ brings with it prestige, resources and funding. Poltain and Wright consider this idea, identifying a spectrum of approaches adopted by states to control data generated in and passing through their territories in a way that establishes a form of ‘data sovereignty.’<sup>74</sup> Indeed, their work similarly supports the earlier argument regarding the importance of the physical architecture of cyberspace, again identified as a key pillar of national defence and security.<sup>75</sup>

Military lawyers such as Franzese have confidently asserted the rapid securitization of cyberspace. Used for everything from intelligence gathering and analysis and military plans to probing networks for their strategic advantage it is now the fifth domain of warfare. Drawing comparisons with other ‘domains of statecraft’ like air and space, cyber becomes a sovereign utility, used for the advancement of national security. For Franzese, as with new technologies of air and sea that challenged pre-existing legal and social frameworks in similar ways, ‘a regime of Sovereignty’ should be established, encouraging States to ‘recognise cyberspace is a sovereign domain and to develop the technical capability to exert their sovereignty in cyberspace.’<sup>76</sup> By doing so he argues, the silence that currently dominates aggressive state activity in cyber-space may reduce, establishing rules of ‘acceptable State behaviour’ in this domain. Before doing so, we need to reflect on this behaviour’s historic legacy, seen in its broader context. Ultimately, the historic ability of States to gain strategic advantage through cyber technologies contradicts both the global commons and deterministic neoliberal narratives about diminished states.

### Arab Spring: A Cyber Trojan-horse?

What of claims about cyberspace accelerating social movements and civil society?<sup>77</sup> Emphasising the effect of global free communications, many still argue that the most significant and meaningful impact of cyberspace is the way it allows individuals to bypass oppressive regimes, acting and organising rapidly and covertly to bewilder security agencies. Sociologist Manuel Castells is one of the most prominent proponents of this view, and over the last twenty years, his vision of a ‘networked society’ has been hugely influential. He has emphasised the impact of the *individualisation* of cyberspace, destabilizing the nation-state’s legitimizing institutions. Moving in sympathy with the libertarian ideal of cyberspace, Castells suggests the resultant effects included the opening of global markets and the further weakening of the nation-state.<sup>78</sup> In the 1990s, enthusiasm for communications technologies as a means of spreading democracy informed many aspects of US foreign policy and indeed notions of soft power.<sup>79</sup>

The Arab Spring re-energised this logic, giving vivid examples of the way that cyberspace, and in particular social media platforms like Twitter, were advancing freedom in the Middle East. Key figures leading the revolutions in the Maghreb, also in Egypt, Yemen and Bahrain seemed to be adept in the use of digital technologies and had been deliberately upskilled by NGOs. Similarly, YouTube

<sup>73</sup> W.L. Bennett and Steven Livingston, ‘The disinformation order: Disruptive communication and the decline of democratic institutions’, *European Journal of Communication*, 33:2 (2018), pp.122-139.

<sup>74</sup> Dana Polatin-Reuben & Joss Wright, ‘An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet’ (Oxford: FOCI, 2014). Available at : <https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf> (pp.1-10)

<sup>75</sup> Erica Borghard and Shawn Lonergan, ‘The logic of coercion in cyberspace’, *Security Studies*, 26:3 (2017), pp.452-81.

<sup>76</sup> Patrick Franzese, ‘Sovereignty in cyberspace: Can it exist’, *Air Force Law Review*, 64:1 (2009), p.10.

<sup>77</sup> Zeynep Tufekci and Christopher Wilson, “Social media and the decision to participate in political protest: Observations from Tahrir Square.” *Journal of Communication*, 62:2 (2012) pp.363-379; Habibul Haque Khondker, ‘Role of the new media in the Arab Spring,’ *Globalizations*, 8:5 (2011), pp.675-679.

<sup>78</sup> David Bell, *Cyberculture Theorists: Manuel Castells and Donna Haraway* (London: Routledge, 2006).

<sup>79</sup> Joseph S. Nye, ‘Public diplomacy and soft power,’ *The annals of the American academy of political and social science* 616.1 (2008): 94-109.



and other video archiving platforms allowed citizen journalists, together with exiles and refugees, to communicate through mobile phones, cameras and consumer electronics, broadcasting and operating independently to both state boundaries and traditional political parties.<sup>80</sup> In 2013, Philip Howard and Muzammil Hussain argued in their influential book *Democracy's Fourth Wave?* for the liberating effect of cyberspace and social media. Authoritarian leaders, they insisted, were crippled by an army of '20 and 30 year-olds without ideological baggage, violent intentions or clear leadership.'<sup>81</sup> In contrast to previous media forms like the printing press and the radio, the peer-to-peer components of cyberspace offered a platform to 'organise, build networks, and create social capital and political action.'<sup>82</sup> Following the immolation of Mohammed Bouazizi in Libya, their analysis found social media (notably Facebook/Twitter) to have been pivotal in disseminating information and raising awareness, 'putting a human face on political oppression.'<sup>83</sup>

Yet almost a decade on, these optimistic conclusions stand in need of some qualification. Scholars are now less convinced of the catalytic effect of social media on these events. Moreover, during the last decade, we have seen Middle Eastern governments gradually recover control over their territories. Importantly, cyberspace has remained central to this resurgence. Like China, Russia, Brazil and India, they have used this strategic technology to 'censor, surveil, and disrupt protesters and to actively cultivate alternative nationalist movements using 'bots' and armies of fake users'. Ironically the technologies that many academics saw as vehicles of liberation, have now been revealed as squashing civil society. Where they have not mastered the internet, they have simply shut it down, blocking encrypted communications.<sup>84</sup> Therefore, while social media and networked technology can facilitate community and social organisation, they simultaneously offer sovereign states new ways of asserting or extending their control and authority. At their most extreme, Dana Moss has shown how authoritarian governments can use the internet to pursue their own diaspora abroad. Internet communication technologies can in fact globalize social control by regimes and impact anti-regime diasporas. Syria has successfully used these techniques to deter many from using the internet to contest the Assad regime.<sup>85</sup>

In April 2017, the Turkish Government turned to these electronic forms of statecraft. They restricted common platforms like Wikipedia, social media and even dating sites following the assassination of the Russian Ambassador to Turkey. Fearing they were losing virtual control of their citizens, the government acted swiftly and concisely, cutting off access to swathes of the population, as if to remind their populous of their underlying ability to influence these 'free' spaces.<sup>86</sup> In contrast to the 'liberation technology' narrative, Rod and Weidmann highlight the instrumental, strategic value of internet technology for government agencies connected to processes of surveillance, monitoring and control. Having conducted a large-N analyses of authoritarian countries for the years 1993–2010 they concluded firstly that 'regimes aiming to prevent any independent public sphere are more likely to introduce the Internet'. They also suggest that their findings indicate that the internet has did not contribute to a global shift towards democracy during this period.<sup>87</sup>

Rather than liberating, social media platforms become an additional layer of bureaucracy and control. Applying for licenses and collecting data on the viewing histories of their citizens, internet-related technology thus becomes indicative of government presence and surveillance. Propagating 'correct values' and identifying domestic opposition movements, this directly challenges the liberation

---

<sup>80</sup> Alexandra Dunn, 'Public as Politician? The Improvised Hierarchies of Participatory Influence of the April 6<sup>th</sup> Youth Movement Facebook Group,' Working Paper. Cambridge, CRASSH, 2010, pp.1-20.

<sup>81</sup> Philip Howard & Muzammil Hussain, *Democracy's Fourth Wave?* p.3

<sup>82</sup> Ibid. p.66.

<sup>83</sup> Ibid. p.47.

<sup>84</sup> Jack Goldsmith, 'The failure of internet freedom', *Emerging Threats* (New York: Knight First Amendment Institute, 2018), pp.9-12.

<sup>85</sup> Dana M. Moss, 'The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora,' *Globalizations*, 15:2 (2018), pp.265-282.

<sup>86</sup> Agence France-Presse & Telegraph Reporters. 'Turkey blocks access to WhatsApp, Facebook and Twitter.' November 2016 Available at: {<https://www.telegraph.co.uk/technology/2016/11/04/turkey-blocks-access-to-whatsapp-facebook-and-twitter/>} Accessed 5<sup>th</sup> January 2019.

<sup>87</sup> Espen Rod & Nils Weidmann, 'Empowering activists or autocrats? The Internet in authoritarian regimes', *Journal of Peace Research*, 52:3 (2015), pp.338-51.

narrative. This is a significant intervention, at a time when social media and other platforms are under intense scrutiny for conceding to requests from suspect government organisations. Consequently, despite the temptation and allure of the libertarian narrative of individual empowerment, governments remain able to affect Net transaction costs, applying filters, cyber-fences and other mechanisms to effectively regulate Net transactions.<sup>88</sup> As Daniel Drezner concludes, despite its promise and potential for liberation, ‘when necessary, governments of every stripe have been willing to disrupt or sever internet traffic in order to ensure that their ends are achieved.’<sup>89</sup>

Perhaps Rod and Weidman’s most significant contribution is their suggestion that it is precisely this networking potential that creates an ‘incentive for control’ for autocratic elites, concerned with containing public sentiment and opinion, with 82% (28/34) of countries studied having some form of internet censorship or other.<sup>90</sup> Graham also explores this idea, arguing that we must ‘debunk the substitution-ist myths of technological determinism... allowing us to reveal the socially contingent effects of new technologies... and ways in which some groups, areas and interests may benefit... while others actually lose out.’<sup>91</sup> Therefore, while cyberspace enables individuals to communicate across national boundaries, the freedom and privacy they experience is often illusory. The platforms through which social movements (and other organisations) operate remain embedded within broader systems of hierarchy and centralisation, predominantly connected to physicality and territory.

There is also little question that states have sought to exaggerate the extent to which privacy technology provides protesters and insurgents with effective cloaking in the expectation that this will yield more data. Indeed, one of the main vexations that American intelligence officers expressed with the Snowden revelations was that individuals were suddenly apprised of this state capability.<sup>92</sup> In 2003, it was noticeable that the US occupation forces in Baghdad gave the population a modern mobile phone network even before restoring water and medical services, since this allowed them to gather intelligence on the insurgents who used it.<sup>93</sup> If engaged in a long-term struggle, the internet is potentially a trap for social movements, since it strips away the very anonymity that protesters and rebels have historically required to survive. Reliant on apps, platforms and other electronic tools that remain embedded within the ‘global network,’ that allocates everyone a number, often their IP address. Cyberspace may give the protester short-term ‘flash mob’ advantage, but over time it probably tips the balance of advantage back in favour of the security forces of Sovereign states. In the wake of the Snowden revelations, we need to ask whether there has ever been a time in which major states have ceded authority over this environment, while minor states seem to have caught up relatively quickly.<sup>94</sup> What we have seen over the last decade points not so much to anarchy but instead to the growing ability of sovereign entities to utilise cyberspace for their strategic advantage, often in secret. Meanwhile, their warnings about electronic ‘anarchy’ validate controversial policies that may otherwise have been rejected by their parliaments and populations.

### **Longer Histories of Involvement**

Perhaps the most fundamental misconception of our understanding of the relationship between cyberspace and sovereignty is a perception of newness. Historicising these issues, as well as grounding them in geography, is important if we are to fully appreciate the long-term use of cyberspace by sovereign states for their strategic advantage. Sovereignty has been fortified, not eradicated, under globalising conditions.<sup>95</sup> To date, the International Relations literature has not only conformed mostly

---

<sup>88</sup> *ibid.*

<sup>89</sup> Daniel Drezner ‘The Global Governance of the Internet: Bringing the State Back In’, *Political Science Quarterly*, 119:3 (2004), p.490.

<sup>90</sup> Rod & Weidmann, ‘Empowering activists or autocrats?’

<sup>91</sup> Stephen Graham, ‘The end of geography or the explosion of place?’ pp.165-185.

<sup>92</sup> Edward Epstein, *How America Lost Its Secrets: Edward Snowden, the Man and the Theft* (New York: Vintage Press, 2017)

<sup>93</sup> Mark Urban. *Task Force Black* (London: Little, Brown, 2010).

<sup>94</sup> David Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber Power* (London: Routledge, 2011), p.60.

<sup>95</sup> On recent intelligence scholarship see Lewis Herrington, ‘The debatable land: spies, secrets and persistent shadows.’ *International Affairs*, 94:3 (2018), pp.645-55; Jules Gaspard, ‘Intelligence without essence: rejecting



to the myth of libertarian romanticism, it has tended to analyse state interventions in this realm as surprising, episodic or untypical. Arguably this interpretation, which often commands considerable consensus, stands in need of adjustment.<sup>96</sup>

More than a century ago, the infosphere formed a central tool of state advantage. Military communications and technical surveillance practices across the globe, beginning with the telegraph, were adopted and exploited by states to exercise control and also increase warning in an era of increasing strategic mobility. Indeed, historians have described the telegraph as the ‘Victorian internet.’<sup>97</sup> The electronic intelligence revolution that many associate with Alan Turing and Bletchley Park had in fact mostly arrived by 1918. As Dan Larsen has demonstrated, these surveillance activities were conducted in strikingly similar ways during the First World War as during the Second World War.<sup>98</sup> States exerted their influence across cable networks that were prized geographical assets and legacies of empire. Companies like Cable & Wireless Ltd worked closely Whitehall in the much the same way as British Telecom has done in the current century. Radio masts and listening stations were established across the globe and the desire to intercept or manipulate these transmissions for reason of intelligence or propaganda has often inspired larger states to cling to small islands in obscure parts of the world in what appear to be time-warp remnants of empire.<sup>99</sup> These physical structures expanded and changed with the arrival of microwave telephone networks, mobile phone networks, telecommunications satellites and finally fibre optic cables. While the technology advanced, their critical importance to states did not waver.<sup>100</sup>

The increasing volumes of data intercepted by the intelligence agencies have indirectly driven the development many of the devices that now surround us. In particular, the vast increase in the volume of intercepted diplomatic traffic from third world countries by the 1960s drove the demand for high-speed computing from companies such as IBM and specialist contractors such as Cray Corporation. Directly or indirectly, by the 1980s, organisations like the NSA employed vast number of computing PhDs from universities and as one of the foremost historians of computing has observed, we have yet to tell the real story about the history of computing.<sup>101</sup> Moreover, the boundless volume of intercepted clear voice traffic grabbed by the signals intelligence agencies after 1960 also drove an entire field of advanced linguistic computer translation and computer voice recognition. Computing as a whole is perhaps ten years further advanced because of these defence-driven applications, moreover, devices such as Amazon Alexa or Google Mini now appearing in our homes, have their origins in research commissioned by NSA and GCHQ.<sup>102</sup>

While for many, the networks and ‘clouds’ that comprise cyberspace are unrelated to historic practices, they are intrinsically connected.<sup>103</sup> Incorporating these into a longitudinal analysis illustrates the ways cyberspace has been used by states as a central tool of statecraft. Indeed, it is probably worth

---

the classical theory of definition,’ *International Journal of Intelligence and CounterIntelligence*, 30:3 (2017), pp.557-82.

<sup>96</sup> David Lyon is one the few to observe that in the Snowden ‘revelations’ there ‘was little that was completely new’, David Lyon, ‘The Snowden stakes: challenges for understanding surveillance today,’ *Surveillance & Society*, 13:2 (2015). pp. 139-152.

<sup>97</sup> Tom Standage, *The Victorian Internet* (London: Phoenix, 1998).

<sup>98</sup> Dan Larsen. ‘Intelligence in the First World War: The State of the Field,’ *Intelligence and National Security*, 29:2 (2014), pp.282-302.

<sup>99</sup> Sarah Mainwaring and Richard J. Aldrich, ‘The Secret Empire of Signals Intelligence: GCHQ and the Persistence of the Colonial Presence’, *International History Review*, 2019.

<sup>100</sup> David Nickles, *Under the wire: How the telegraph changed diplomacy* (Cambridge: Harvard University Press, 2009); Simone M. Müller, *Wiring the world: the social and cultural creation of global telegraph networks* (New York: Columbia University Press, 2016).

<sup>101</sup> Paul E. Ceruzzi, ‘Are Historians Failing to Tell the Real Story about the History of Computing?’ *IEEE Annals of the History of Computing*, 36:3 (2014), 94-95

<sup>102</sup> Robert W. Seidel, “Crunching numbers” computers and physical research in the AEC laboratories,’ *History and Technology* 15:1-2 (1998), pp. 31-68; Jon Agar, ‘Putting the spooks back in? The UK secret state and the history of computing,’ *Information & Culture*, 51:1 (2016), pp. 102-124.

<sup>103</sup> Ronald Deibert and Rafal Rohozinski, ‘Liberation vs. control: The future of cyberspace,’ *Journal of Democracy*, 21:4 (2010), pp. 43-57.

remembering that the internet itself was an outgrowth of American military science research.<sup>104</sup> Established in the late 1960s by the National Science Foundation, ARPA quickly expanded on a global scale, enabling governments and military apparatuses to conduct a range of government business, including major nuclear and naval technology projects more efficiently. Although many argue that the ARPANET bears little resemblance to the cyberspace of today, we need to recognise that its foundations were laid by the Pentagon.<sup>105</sup> Super-computing and the internet both lack a single founding father because they emerged out of a myriad of advanced defence projects.<sup>106</sup>

With this comes boundaries, labels, designators and order. A compelling example is the little-known Domain Naming System (DNS), hierarchically allocating names and IP addresses to new 'entrants' of cyberspace. Viewed by many as a neutral, technical matter of limited political relevance, DeNardis has nevertheless explored the political underpinnings of this system, echoing Bratton's (and Foucault's) claim that an ability to address something means you can govern it.<sup>107</sup> Despite superficial impressions of trans-nationalism and unfettered freedom, every e-mail and website address is attached to and aligned with a physical territory. Allocated hierarchically, Domain names like '.fr' (France) and '.co.uk' (UK) connect a user or company with a territorial place. They connect them to a sovereign state. McDowell, Steinberg and Tomasello highlight the broader issue of Government's 'managing' of the Internet in these ways, showing how actors construct the 'infosphere' to 'achieve specific ends.'<sup>108</sup> While a determined user can certainly employ time-consuming techniques to mask their identity online, most websites and internet users are reliant upon these structures to engage with and use internet technologies. For the majority of communications and transactions the idea that the internet escapes a location is implausible.<sup>109</sup>

Thus, the history and geography of cyberspace cannot be properly understood without a reinterpretation of its connections to its material foundations and reliance upon sovereign states. Many social scientists and policymakers remain persuaded of the libertarian portrayal of cyberspace as weakening centralised power and control. Others have assumed that governments have only recently begun to re-assert control over what they assumed to be an anarchic space. This is perhaps understandable since so much of the history of surveillance and indeed computing generally contain missing elements that historians will be trying to unpick for decades to come.<sup>110</sup> But we now know enough to conclude that this technology probably reinforces traditional hierarchies, making the more powerful states like Russia, China and the United States yet stronger.<sup>111</sup>

## Conclusion

Cyberspace has consistently been used as a tool of statecraft. Although electronic 'space' has become increasingly important for a range of activities, from storage to communication, territorial 'place' remains prevalent. Temporality is equally important, not only in understanding the significance of the development of this physical infrastructure over time, but also in appreciating that many technical innovations were driven by the supreme efforts that security researchers exerted to stay ahead of the curve in this realm. The United States as an information hegemon, and more specifically the National Security Agency, has done more than many suspect to shape the current information environment. Meanwhile, smaller states have taken a little while to catch up and achieve purchase over new systems.

<sup>104</sup> Maryann Feldmann, 'The Internet revolution and the geography of innovation,' *International Social Science Journal*, 54:171 (2002), pp. 47-56.

<sup>105</sup> Tony Delamothe, 'The Once and Future Web: Worlds Woven by the Telegraph and Internet,' *British Medical Journal*, 324:7337 (2002), pp.620-21.

<sup>106</sup> Roy Rosenzweig, 'Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet,' *The American Historical Review*, 103:5 (1998), pp.1530-1552.

<sup>107</sup> Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

<sup>108</sup> Stephen McDowell, Phillip Steinberg and Tami Tomasello. *Managing the infosphere. Governance, Technology and Cultural Practice in Motion*. (Philadelphia: Temple University Press, 2008), p.23.

<sup>109</sup> Saskia Sassen, *Territory, Authority, Rights* (New York: Princeton University Press, 2008), p.331

<sup>110</sup> Lyria Bennett Moses, 'Recurring dilemmas: The law's race to keep up with technological change', *University of Illinois Journal of Law Technology & Policy*, 7:1 (2007), p.239.

<sup>111</sup> See for example Michael Adas, *Machines as the measure of men: Science, technology, and ideologies of Western dominance* (New York: Cornell University Press, 2015).

As the Arab Spring illustrates, this can wrong-foot regimes in the short term, but in the long term there is every sign that states are back in control.

What is most striking about the role of states and sovereignty in cyberspace is that often this interest is itself bounded. In striking contrast to our vision of cyberspace as global, governments appear to privilege *internal* control and authority, and so are less concerned with directly challenging the activity of other nations in cyberspace than with establishing control within national jurisdictions. Indian and Brazilian pursuit of 'data sovereignty' amongst the BRICS nations could be viewed accordingly, with new regulations promulgated that appear to challenge the globalisation of telecommunications. Even major cities like Los Angeles are paying higher fees to ensure that their data is stored locally and not in the cloud. The emerging 'splinternet' is a global phenomenon and not just about China, Russia or Iran.

The true rebels in cyberspace were figures like computer hacktivist Kevin Mitnick who devoted his life to evading the rules and believed that cyberspace provided a secret playground, but his eventual destination was a penitentiary. Hackers and cyber criminals enjoy sanctuary in locations such as North Korea and the Balkans, but even here their immunity depends on the world of states, either 'pariahs' or places with poor governance.<sup>112</sup> Social scientists might well devote more attention to the material, geographical underpinnings of cyberspace. While libertarian, anarchic representations are attractive, especially to politicians and policy-maker rolling out new regulation, they often overlook the role and significance of physical geography and sovereign power. More importantly, they underappreciate (if not misrepresent) the historic and enduring ability of sovereign entities to influence and manipulate this 'new' environment for their advantage.

While this analysis is on one level pessimistic, there remains room for optimism. Understood as the product of social relations, cyberspace has the potential to change. It is not that cyberspace has and will always be used as a tool for oppression, eradicating its usefulness for social movements and other liberating forces. It is, in the words of Doreen Massey, 'unfinished,' always being made and recreated. How this 'space' develops remains unknown and unconfirmed. Recognising the historic and underlying political relations that led up to its current existence is significant if we are to understand its future.

Perhaps the most compelling illustration of the connections between cyberspace and sovereignty were made not by political scientists, but by Trevor Paglen, an American artist whose work tackles mass surveillance and data collection. Using geography and satellite imagery, Paglen masterfully depicts the physical, material presence of the surveillance state. Doing so, he suggests that 'infrastructures of power always inhabit the surface of the earth somehow, or the skies above the earth. 'They're material things, always, and even though the metaphors we use to describe them are often immaterial - for example, we might describe the internet as the Cloud or cyber-space - those metaphors are wildly misleading.'<sup>113</sup> Building on the argument here and echoing the long-overlooked appeals of geographers, he shows how state secrecy and surveillance are produced through space.<sup>114</sup>

A more material approach also requires stronger attention to history and less emphasis on 'newness'. We might question approaches that emphasise the revolutionary impact of cyberspace that frequently results in overblown claims of transformation. Understood in connection to or with similar technologies of telephony and printing, the perennial nature of debates surrounding the relationship between 'place' and 'space' and the relationship between social transformation and technology emerges in a longer perspective. More importantly, a more measured approach allows us to reappraise the meaning of the Snowden revelations on surveillance and state hacking. Widely acclaimed as the high water-mark of Western surveillance, most discussions of current electronic spying practices are attended by hyperbole, being treated as exceptional or ahistorical. However, this article suggests the possibility that sovereign entities of all stripes have historically recognised the strategic value of exploiting cyberspace for their advantage all the way back to Bletchley Park. As James Bridle has

---

<sup>112</sup> Kevin Mitnick, *Ghost in the wires: My adventures as the world's most wanted hacker* (London: Little, Brown, 2011).

<sup>113</sup> Liz Jobey, 'Trevor Paglen: What lies beneath', *Financial Times*, 31 December 2015. Available at: <https://www.ft.com/content/beaf9936-a8ff-11e5-9700-2b669a5aeb83>. Accessed 12<sup>th</sup> January 2019.

<sup>114</sup> Trevor Paglen, 'Goatsucker: Toward a spatial theory of state secrecy,' *Environment and Planning D: Society and Space*, 28:5 (2010), pp.759-771.

shown, Snowden's so-called revelations were in fact on a continuum with other insights into surveillance over decades, if not centuries. States have always been in control of communications and there is less disorder in this space than we have been led to believe.<sup>115</sup> This absence of anarchy is either rather reassuring or rather worrying, depending on our point of view.

---

<sup>115</sup> James Bridle, *New Dark Age: Technology, Knowledge and the End of the Future* (London: Verso, 2018).