SOVEREIGNTY IN A DIGITAL ERA

A Report Commissioned by the Dialogue of Civilisations Research Institute Berlin
Sovereignty in a digital era

A report commissioned by the Dialogue of Civilizations Research Institute
Berlin

by

Kate Coyer and Richard Higgott¹

¹ Kate Coyer is Research Fellow in the School of Public Policy at the Central European University, Budapest and Richard Higgott is Emeritus Professor at the University of Warwick, now Professor with the Brussels School of Governance at the Vrije Universiteit Brussels. They wish to thank Simon Reich, Rutgers University; Vladimir Yakunin, Jean-Christophe Bas, Berthold Kuhn, and Jonathan Grayson of the Dialogue of Civilisations Research Institute; Elettra Bietti, Harvard University; Colin Bossen, Rice University; Yasodara Córdova, World Bank; and Bertrand de La Chapelle, Internet & Jurisdiction Policy Network for the helpful and insightful comments on earlier drafts of the Report.
### Table of contents

<table>
<thead>
<tr>
<th>Foreword</th>
<th>Jean-Christophe Bas</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Glossary</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>Digitalisation, sovereignty, and politics</td>
<td>10</td>
</tr>
</tbody>
</table>

- A digital spectrum for politics and international relations
- Hierarchy and the uses of strategic power
- Hybridity and techno-diplomacy
- This report: Analysing trends towards a digital future

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Sovereignty: A quick introduction</th>
<th>16</th>
</tr>
</thead>
</table>

- Then: Sovereignty as an evolving concept; 1648 and beyond
- And now: From globalisation to anti-globalism

<table>
<thead>
<tr>
<th>Part 2</th>
<th>Digital technology: An equally quick introduction</th>
<th>20</th>
</tr>
</thead>
</table>

- Digital sovereignty and data
- What’s at stake?
- Machine-learning and individual sovereignty
- Algorithmic decision-making and politics

<table>
<thead>
<tr>
<th>Part 3</th>
<th>Sovereignty and governance: The role of digital networks</th>
<th>26</th>
</tr>
</thead>
</table>

- Internet governance
- Elections, sovereignty and disinformation
- Internet intermediaries
- Intermediaries, state power and sovereignty
- Box 1: Russian internet legislation
- Box 2: Encryption—Apple versus the FBI
- Online extremism: National security and sovereignty
- Box 3: Codes of conduct and illegal online hate speech
- Social media platforms and content moderation
Part 4  Sovereignty and competing visions of the internet  43

International relations: 5G, the US-China contest on the new frontier of international power
The geopolitical ‘pecking order

Part 5  Digitalisation and political control  48

Citizens and the loss of privacy

Part 6  Digitalisation and pandemic: The impact of Covid-19 on sovereignty  52

Digitalisation and pandemic: A new pairing
Emergency powers tend to outlive their emergencies
An ‘infodemic’?
Platform power during a pandemic
Digitalisation and health surveillance: Freer or less free?
Spyware, the private sector and responsible surveillance
Decoupling and bipolarity in an age of pandemic
Exposing and amplifying existing inequalities
Where do we go from here?

Conclusion  Digitalisation and disillusion in the third digital decade  64

Historical hindsight: Digitalisation in perspective
The battle between democracy and authoritarianism: Tech power and public interest
Next steps: Beyond sovereignty

References  70
Foreword

The very culture of international relations is changing. Hierarchies of actors – states, civil society, corporate powers, social media influencers – their modes of behaviour, and their governing principles are being shuffled by the acceleration of the digital revolution. Meanwhile, the world experiences the more gradual epochal change, fast-forwarded by Covid-19, of the liberal world order giving way to a newly emerging multipolarity, with China the lead-challenger to US norms, and where digital frontiers are arguably the most fundamental terrain of contest.

In this context, how can we best understand the impact of digitalisation? What should we make of Facebook’s Marc Zuckerberg being a fixture at the prestigious Munich Security Conference, or Jack Ma of Alibaba’s A-list appearances at Western institutions spanning the West Point US military academy, the Clinton Global Initiative, and Davos? Far beyond the celebrity-like status of global tech entrepreneurs, digitalisation is actually reshaping the world order’s most foundational conceptual reality: sovereignty.

The initiative for this DOC project came via the observation that a broader array of agents than traditional state powers are key to shaping international policy, in most cases enabled by digital instruments. In numerous cases, corporate and digital actors have conducted business while ignoring laws and rules in their countries of operation. Facebook’s recent attempt to create its own currency; the increasing frequency of conflicts between state regulation and corporate policy around activities of a digital nature; and the way tech giants exempt themselves from taxation are just a few examples. What is striking here is that whilst shifts in world order are broadly acknowledged, the capability of states and the international community to master the dynamics and the agents of those changes is evidently missing. For a host of global actors grappling with the redundancy of multiple 20th-century institutions, being equipped with a working knowledge of digital actors and digital action is key, not least in order to mitigate the tensions between the cross-border nature of the internet and national jurisdictional expectations.

Our goal at the DOC Institute is to foster dialogue among all cultures and civilisations to forge shared worldviews on fundamental policy issues. Our culturally informed approach produces a multifaceted outlook, from the everyday level of human interaction to the global level of institutionalised power. This project, under the direction of Professor Richard Higgott, has been developed in this fashion.

This report, written by Higgott and his colleague Dr Kate Coyer, is the first of two instalments in this project. The report is circulated initially to provoke and facilitate debate. The digital players and ‘ecologies’ referenced throughout are diverse, evolving, and worthy of greater collaborative dialogue. In fall 2020, the DOC will convene a policy-focused working session featuring insights from multiple corners of the world and a spectrum of digital strategies. The gathering’s remit will be to produce a multilateral digital ‘playbook’, a much-enhanced elaboration of this first report, informed by the DOC’s commitment to a dialogical methodology that takes the presence of multiple civilisational perspectives as its point of departure.
We welcome comment and engagement and are looking forward to the project’s development in collaboration with our truly global network of experts – if you are new to the DOC and would like to participate in this dialogue, please get in touch.

Jean-Christophe Bas  
*CEO and Head of Executive Board, DOC Research Institute*
Executive summary

The aim of this report is to specify the impact of digitalisation on sovereignty. It is premised on the assumption that sovereignty, the dominant organising characteristic of social and political order for the last four centuries, has undergone profound change over the last half-century. Driven initially by technology-enabled globalisation, and then by anti-globalism, sovereignty has become an even more politically charged and contested concept as its significance has been re-enhanced by the rise of nationalism. The rapid emergence of digitalisation has been the agent that has powered a so-called ‘crisis of sovereignty’. This report analyses six aspects of the digitalisation-sovereignty relationship.

Firstly, the report looks at the concept of sovereignty as a determining factor of social and political life. It looks at how the nature of sovereignty – what it means for a state to be sovereign – has changed in recent years under the influences of globalisation, the drift towards anti-globalism, and, more broadly but closely connected, digitalisation.

The argument in short is that digitalisation fundamentally changes what it means for a state to call itself sovereign. That senior politicians and policymakers still think that the states they lead and manage can have absolute sovereignty – as many still do, rhetorically at least – beggars the imagination.

Secondly, it provides an introduction to digital technology, from its optimistic origins as a free, open, and transparent provider of information and communication, to now darker views of the internet’s role as a manipulative and manipulated agent of intrusion and socio-political control, driven by the monetisation of behavioural data captured by both a small group of tech giants and a fast-growing sector of small-to-medium sized digital companies. It identifies the significance and implications of machine-learning and algorithmic decision-making on socio-political life and asks what is further at stake in the development of digitalisation. In short, digital sovereignty asks us to rethink the nature of sovereignty itself.

Thirdly, it looks at the struggle between the tech sector and the state for control of digital governance. It focuses on the near ubiquitous presence of digital networks, and the complex and contested nature of internet governance and ‘internet intermediaries’ as interlocutors in the politically charged relationship between digital platforms and the state over content moderation and information access, as well as the relationship between digitalisation and electoral sovereignty.

Fourthly, it looks at visions of the internet and their implications for sovereignty. It identifies three competing visions: American, Chinese, and ‘other’, especially but not exclusively those of the EU as the principal alternative to US and Chinese attempts to build and maintain separate digital ecologies. These three visions reflect two struggles. Firstly, over regulatory primacy between private actors and states. Europe’s aims for a model urging a democratic regulatory response sets it apart from China and the US. Europe is shown to be resisting not only Chinese and US political pressure but also the power of major US tech corporations. Secondly, the report looks at the contest over the shape of a post-liberal American led world order as the US and China battle for international ascendancy over digital technologies. The report offers a short study of the US-China relationship over the role of Huawei in the development of 5G technology to illustrate the manner in which the governance and control of digital technology – and especially a trend toward decoupling in the digital sector – is becoming one of the major international relations agenda items of our age.
Fifthly, the report looks at the fraught relationship between digitalisation and political control and particularly the juxtaposition of the internet’s conflicting and contradictory positions as an agent of empowerment, openness, transparency, and potential democratisation on the one hand and as an agent of control, repression, and political authoritarianism on the other.

Sixthly, the report was drafted only as the implications of Covid-19 were beginning to emerge. Just as digitalisation affects socio-political and economic life both domestically and internationally, the coronavirus is also exacerbating change in these domains. The report’s judgments reached in parts 1-5 are both complicated yet reinforced by Covid-19. Both the theory and practice of sovereignty, and our understanding of global world order, will be dramatically affected by it. The report offers some inevitably preliminary implications of Covid-19’s impact on the sovereignty-digitalisation dynamic.

The report concludes that:

(i) The optimism of the early ‘digital utopians’ is giving way to disillusionment as the impact of the under-regulated power of the private sector is operationalised.
(ii) The concept of absolute sovereignty is a polite fiction in an era of globalisation and has become even more so in an era of digitalisation. But digitalisation affects sovereignty in different ways for different kinds of states.
(iii) Excited by its potential but fearful of its darker side, the key issues are how both states and tech companies respond to the challenges of digitalisation and the impact of civil society’s longstanding work in fighting bad laws and practice.
(iv) The extant challenges are further exacerbated by the Covid-19 global pandemic.
(v) It is time to recognise sovereignty as fungible, rather than absolute. It is more a process of bargaining in an increasingly hybrid international, globally networked context of digitalisation for which neither history nor a reliance on unregulated private actors mediating for states have any real lessons.

These conclusions carry four major implications:

(i) Over the short-to-medium term, the world will likely become less prosperous, less open, and less free as states, confusing resilience and policy autonomy with sovereignty, turn in on themselves in enhanced nationalist fashion.
(ii) Bipolarity will be reinforced. What started out as a US desire to decouple its economy from China’s, especially in the domains of artificial intelligence (AI) and digitalisation, is now reciprocated by China. The degree to which this process drives a ‘new Cold War’ is yet to be determined.
(iii) Assumptions of the sovereign control of digital communication are becoming mere exercises in wish-fulfilment rather than realistic aspirations. A successful resolution of the current impasse will not come just from great power geopolitical games reasserting the absolute sovereignty of the state.
(iv) It is clear on the basis of observed behaviour that, like it or not, states and regions, such as Europe are likely to search for a role in this sub-optimal bipolar battle for digital governance rather than search for multilateral solutions.

But the report also offers an alternative, more positive, scenario. It advances an argument that in a world of digital communication, there is a limit to the degree of global decoupling that can actually occur. The digitalisation genie will not easily be put back into the bottle. Technology
is now global not only in its distributive effects but also in its consequences. Viruses, both human and digital, are trans-sovereign in their impact. They do not need passports. In the current digital era, the pursuit of nationalist, transactional international relations run counter to the many network processes and indeed habits of cooperative behaviour that digitalisation has created and which, if developed and used responsibly, can further foster these processes. That this is not happening is a current tragedy with short, medium, and if nothing is done, longer term negative connotations for states and the societies for whom they purport to speak and act.

The internet continues to play vital roles in pro-democracy movements, in the delivery of vital independent journalism, and as a mode of communication on which civil society relies. Decentralised models offer alternative visions of infrastructure and governance. But choices must be made and regulations must be appropriately enacted if we are to secure a long-term, open internet.

Maybe when nationalist endeavours, driven by a greater desire for the mythical beast called sovereignty, fail to solve our problems, as they almost certainly will, collective action through reformed – but harder-headed – multilateral cooperation, operationalised in a digitally networked manner, may just prove increasingly relevant, desirable, and inevitable. Covid-19 and the manner in which it is addressed may well prove, one way or the other, to be a turning point in this process.
Glossary

ACLU | American Civil Liberties Union
----|----------------------------------
BBC | British Broadcasting Corporation
BRICS | Brazil, Russia, India, China, South Africa
CDA | Communications Decency Act
DNS | Domain Names System
DS | Digital Sovereignty
FAANG | Facebook, Amazon, Apple, Netflix, Google
GAFAM | Google, Apple, Facebook, Amazon, Microsoft
GDPR | General Data Protection Regulation
HHS | Health and Human Services (USA)
ICANN | Internet Corporation for Assigned Names and Numbers
IETF | Internet Engineering Task Force
ITU | International Telegraph Union
NHS | National Health Service (UK)
NWICO | New World Information and Communication Order
OECD | Organisation for Economic Cooperation and Development
RIRs | Regional Internet Registry
SITDA | Sovereignty in the Digital Age
UNESCO | United Nations Economic, Social and Cultural Organisation
UN-WGIG | United Nations-Working Group on Internet Governance
W3C | The World Wide Web Consortium
WEF | World Economic Forum
WSIS | World Summit on the Information Society
Introduction: Digitalisation, sovereignty, and politics

We live in the third digital decade, or what the World Economic Forum (2019) calls the “Fourth Industrial Revolution”. It is a time without precedent. After the high watermark of globalisation – replete with visions of the “end of history” (Fukayama, 1992), increasing international economic integration, and the “borderless world” (Ohmae, 1990) – sovereignty is back in fashion. As we once again understand, there is no end of history, and like all fashions that are never quite the same when they return, sovereignty is not what is was, or was believed to be at its height in the 19th century. It has changed and continues to change. The aim of this report is as follows:

(i) To examine the nature of the re-assertion of sovereignty as a central concept in the modern lexicon of international relations scholarship and practice following its years as a seemingly redundant category in the lexicon of globalisation.

(ii) To examine sovereignty’s relationship to that core factor that has come to fundamentally reshape it in the modern age: digital technology.²

Digitalisation disrupts national sovereignty. In an era when more than five billion people – nearly two-thirds of the global population – have mobile phones, states are increasingly deploying legal, and at times extra-legal, regulatory responses to attempt to regain control, for better and worse, over both their national and international informational flows. Digital technology casts shadows over what it means to be free and equal in an age when both private actors and states have more instruments of control.

Moreover, there is as yet no established positive correlation between technological progress and human moral progress. Thus, normative conclusions – negative or positive – about the future impact of digital technology cannot be simply assumed. Rather, we must unpack key aspects of digital technology and account for the manner in which it affects contemporary sovereignty before we can conclude with some normative propositions about what must be done to ensure that the beneficial nature of digitalisation prevails over its negative and darker effects and practices.

The internet was supposed to open up new spaces to allow for more horizontal flows of information and communication. Yet, increasingly, the internet and digital technologies have become a battleground between states and private companies – with civil society as an active but struggling third player. New tensions over sovereignty and jurisdiction compete with freedom and openness. The quantity of information online can often overwhelm quality and private gatekeepers further complicate the way forward. Digital information not only reshapes reality; in some contexts, it is replacing it.

Importantly, digital communication is now fundamental to political life. Still in its infancy but growing exponentially, we define it as the ways in which contemporary social, political, and economic life are restructured around digital communication and media infrastructures. We ask to what degree digitalisation is setting parameters on individual and collective liberty, the philosophical underpinnings of political community, and indeed the theory and practice of politics generally. Specifically, we ask to what extent these processes can and do enhance or limit two principal political and social constructs and practices: sovereignty and democracy.

² The report deals only with digital technology, not technology more generally or cyber warfare specifically.
A digital spectrum for politics and international relations

We need to rethink the concept of sovereignty and the behaviour of states in an era characterised by the return of nationalism and the changing nature of sovereignty across the spectrum of the digitalisation of politics and international relations. The analysis of digitalisation must traverse the spectrum from the soft edges of culture, cultural relations, and diplomacy through to the hard edges of the new (cyber) warfare. We must see digitalisation as both a cause and an instrument of change. On the way the analysis must address issues as far-reaching but interconnected as e-commerce and experimentations in non-state currencies, the ‘datafication’ of society, hate speech, online extremism, misinformation and disinformation, internet governance and jurisdiction, and the future of free expression in a digital world characterised by both hierarchy and hybridity of digital actors in global relations.

Hierarchy and the uses of strategic power

By hierarchy, we mean the behaviour of the digital ‘superpowers’ – the US and China, whose power is seen by the economic weight of their digital companies – and the aspiring great powers, notably the EU collectively, Russia, India, and Brazil, through middle powers such as the bigger Nordics, Australia, Canada, South Korea, and smaller states and regions. The digital strategies of these varying powers are driven respectively and differently by their individual and changing conceptions of contemporary sovereignty and the degrees to which these conceptions affect policy as they seek to position themselves in the emerging digital order. Specifically:

- What it means to be a digital global player and what this is doing to our understanding of sovereignty.
- Whether states are on the offensive as sovereignty enhancers or on their back heels and in reactive mode as sovereignty defenders.
- What is, or should be, the balance in the relationship between information and communication as socio-political practice on one hand and technology, especially the internet, as the instrument of their delivery on the other.
- The fact the internet is an instrument of domestic consolidation via domestic surveillance and control and at the same time the modern-day driver of state strategies for the projection of international influence.
- At the same time, control over the internet and digital sovereignty is a global effort by states as they try to assert their sovereignty over internet regimes or tech companies often outside their direct control.

Hybridity and techno-diplomacy

By hybridity, we mean the presence and role of the principal non-state players in the digital era; what we might call the non-state ‘powers’, some exhibiting state-like properties, which have driven digitalisation in the 21st century: notably Google, Apple, Facebook, Amazon, and Microsoft in the US and Tencent, Huawei, Baidu, Alibaba, and Weibo in China. The battle to secure ascendancy is no longer simply between sovereign states butting heads with each other across a spectrum from diplomacy to war, the traditional material of international relations.

Rather, the major states are now harnessing privately developed technological platforms of power to enhance the rhetoric of nationalism as a tool in the battle to assert their sovereignty
and domestic power. In its recent appointment of an ambassador to Silicon Valley, the Danish government’s thinking was quite straightforward: the economic strength and impact that major tech companies have on the lives of Danish citizens is greater than the many other places where they have traditional embassies. This is a telling move towards a future of ‘techno-diplomacy’.

The evolution of a global communications order is defined not only by shifting relationships between states but also by private actors wielding significant power to challenge national sovereignties via the privatisation of public spaces that digitalisation has wrought and also the state surveillance practices it has enabled. Private actors are also keen to consolidate their positions. Companies like Facebook and Google operate in a predatory manner towards would-be competitors. Using their substantial buying power, they practice ‘buy-and-kill’ tactics towards fledgling companies before the smaller companies can gain competitive momentum. This tactic is well established (Waters, 2020) and reflects big player market dominance. Three of the five top companies on the Forbes Rich List are tech titans and the five biggest companies in the world by market value are Californian tech firms. The scale of their oligopolistic power is unprecedented, surpassing even that of ‘big pharma’ and oil (see Bartlett, 2018). If we look at Facebook and Google in social messaging and online advertising and Amazon in online selling, then they account for 60% of total digital advertising. 83% of total social media advertising spending is made on Facebook.

Moreover, the tech giants are appearing to operate like sovereign states. In 2017, Mark Zuckerberg stated, in a comment he has no doubt come to regret, “Facebook is more like a government than a traditional company”. Bertrand de la Chappelle, in a nice analogy, compares Facebook’s terms of service to legislative power; their senior staff are the Executive and Facebook’s Oversight Board is the judiciary. Private internet companies and social media platforms hold unprecedented control over how and what we access online; acting sometimes too often as gatekeepers and other times not often enough, they do not always exhibit sufficient levels of ‘rights-respecting’ transparency. But as we see on an almost daily basis, the regulation of speech has been transferred from states to private actors, raising unanswered questions about the longer term future of freedom of expression.

Also central to contemporary activity is the concept of information sovereignty – basically the struggle over the degree to which states have a legitimate right to control information flows within their territories. Information sovereignty is a double-edged political sword. While new technologies can lower barriers to access and enable a global and transnational commons to help counter state-specific authoritarianism, they also make it easier for states and domestic surveillance regimes to monitor and control information, thus contributing to authoritarianism.

The internet was designed as a decentralised architecture/infrastructure but there have always been competing models of what the digital terrain should look like. Current tensions over design, governance, and jurisdiction reflect broader global fissures. In the contemporary era, the US and China are creating two sharply defined technological and online systems – what we might call separate digital ecologies. The American model is still primarily private-sector driven while China’s is state driven. But both systems envelope the development of AI, big data, 5G, and instruments of cyber warfare within their wider national strategies vis-à-vis each other.

Other players – notably India and Russia – are also interested in creating their own ecological systems where national sovereign control is their primary driver. The EU is engaging in its own regulatory efforts and financial penalties to push back on the power of corporate internet actors.
But will they succeed? And what of other emerging players such as South Korea and Brazil? At the global level, pressure to align with the United States will be strong for all its allies – especially vis-à-vis Chinese giants in 5G technology such as Huawei. Is this alignment going to be the outcome for Europe and maybe even Japan? Will the struggle to prevent national fragmentation of decision-making within Europe prevail? Will the EU offer a viable model of regulatory standards to keep the power of global digital technologies in check? These sovereignty-driven questions are exacerbating by the day, especially since the onset of the Covid-19 pandemic.

But state-to-state struggles are not the only questions. Equally significant is the question of whether the balance in data gathering and data holding between states and private actors can be rationally regulated and reasonably symmetrical. What role and impact civil society might have in these contests over fundamental rights such as privacy is also a core question. This is especially the case in the US and Europe, where the relationship between government and the GAFAM (Google, Apple, Facebook, Amazon, Microsoft) or FAANG (Facebook, Amazon, Apple, Netflix, and Google) companies is a work in progress. If the growing nationalist and isolationist sentiments of governments in recent years cannot be contained, then state assertions of the primacy of “security concerns” will lead to what Ian Bremmer (2020) calls a “tech-based military industrial complex”.

This report: Analysing trends in our digital future

Questions surrounding information sovereignty aren’t new. They have been driven by countries in the Global South and sparked major international debates at venues such as UNESCO and the International Telecommunications Union (ITU) over the second half of the 20th century, leading to calls for a New World Information and Communication Order (NWICO) from Global South countries and the Non-Aligned Movement, as part of broader efforts to redress global economic inequality and the legacy of imperialism, and to address imbalances in global communication flows and a lack of ownership and control over crucial telecommunications infrastructure. The UN’s Internet Governance Forums, emerging from the 2003-05 World Summit on the Information Society (WSIS), serve as annual forums for cooperation. The UN also established a High-Level Panel on Digital Cooperation in 2019 and there are a range of other efforts to develop meaningful multi-stakeholder approaches to internet governance.

But the rapid rise of digital communication technologies and global communications infrastructure have changed both state desires and state capacities to govern information flows, challenging effective multi-stakeholder cooperation. A recent report from the Internet & Jurisdiction Policy Network (2019) laid out the urgent case for coordination, arguing that public and private initiatives developing in an uncoordinated manner will have detrimental consequences for both parties and global stability overall.

Will the complex state of affairs identified above inevitably lead to the fragmentation of the internet and the creation of what the BBC (Adee, 2019) has called a “digital Westphalian system” akin to a Westphalian system of sovereignty? Or will the internet remain open and accessible, albeit controlled by globally applied US law captured in the terms of service of

---

3 See UNESCO’s McBride Commission report, ‘Many Voices, One World’ for a set of recommendations to make global media ownership and representation more equitable. Though prepared in 1980, it is telling that many of the problems articulated and recommendations proposed remain germane today.
various private companies? A once utopian narrative associated with the digital revolution has been replaced by more alarmist narratives. Will a ‘third way’ emerge? If so, to what extent can it be led by the public interest and the regulatory responses of European and other like-minded states in the face of growing pressure from China, and increasingly the US, to bifurcate the digital world?

The answers to these questions cast massive domestic and international policy shadows over both near and long-term futures. While these answers are not yet known, assumptions can be made from drawing together existing analysis of the attitudes, policies, and evolving practices of the key players to provide as much of an indication of the future direction of travel as possible. Moving away from this false dichotomy is the key prerequisite for identifying a solution, which is not limited to a stark binary choice between re-imposing strict territorial frontiers or a globally unified regulatory environment. The aspiration of this report is to do precisely that.

Part one of the report offers a quick introduction to the concept of sovereignty as the determining factor in social and political life for the last four centuries. While recognising the contested nature of the concept, it looks at how the nature of sovereignty – what it means for a state to be sovereign – has changed under the influences of globalisation, the drift towards anti-globalism, and now the rise of digitalisation over the last three decades.

Part two provides an equally quick and non-technical introduction to what we mean by digitalisation, focussing specifically on the nature and implications of machine-learning and algorithmic decision-making and asking what is at stake in the continued development of digitalisation.

Part three looks at the relationship between sovereignty and digital governance. It focuses on the now near ubiquitous presence of digital networks, the complex and contested nature of internet governance, and the role of ‘internet intermediaries’ as interlocutors in the politically charged relationship between digital platforms and the state over the neutral-sounding but highly contentious issue of ‘content moderation’.

Part four looks at the major competing visions of the development of the internet and their implications for sovereignty. Far from a consensus, this section identifies three visions that can be simplified as American, Chinese, and an ‘other’ – largely European – model. The European view is formed around a struggle for regulatory primacy between states, the tech giants, and the public/state users of the internet. Part four also has a short case study on the relationship between the US and China over the issue of Huawei’s role in the development of 5G technology.

Part five looks at the contentious relationship between digitalisation and political control and particularly the Janus-faced nature of the internet as an agent of empowerment, openness, and the potential enhancement of democratisation on the one hand and as an agent control, repression, and authoritarianism on the other.

By way of conclusion, the report considers how and why the sense of optimism that accompanied early digitalisation appears to be giving way to a growing sense of disillusion, even amidst the many examples of technology operating in the service of social change.
1. Sovereignty? A quick introduction

Then: Sovereignty as an evolving concept

Since the time of the Treaty of Westphalia (1648), the sovereign state has been the primary subject of modern international relations. Its extensive philosophical antecedents lie in the work of the Frenchman Jean Bodin and the Englishman Thomas Hobbes. Unlike most concepts in politics, sovereignty’s roots are not traced back to the Greeks and the Romans. The concept’s history need not be our concern here, save to note that for both Bodin and Hobbes, the historical context of the religious wars of the century prior to the peace of Westphalia conditioned them to see the need for something, which came to be called sovereignty, to act as a form of supreme political authority necessary to restore social order. For them it was an intensely practical, not theoretical concept. Power was absolute, permanent, and indivisible; control over the citizenry was located in the hands of a sovereign answerable only to God (for a discussion see Herzog, 2020).

Over the centuries, sovereignty morphed from the power of a single individual, invariably a monarch of some description, through various political reforms, until it came to be seen as we think of it today: a system of authority based on the relationship between territory and autonomy and embodied in the state as the highest point of decision-making and authority. The sovereign form of the state became hegemonic by a process of eliminating alternative forms of governance (Spruyt, 1994), determining that political life is, or ought to be, governed according to the principle of sovereignty. The concept of sovereignty focuses socio-political and economic life around a single site of governance: the state.

In the influential Hobbesian view of the world, the political purpose of the sovereign state was the establishment of order, based on mutual relations of protection and obedience (Hobbes, 1968). The sovereign acted as the provider of security. In return, the citizen offered allegiance and obedience. Sovereignty became the centre of authority, the origin of law, and the source of individual and collective security. Citizens were bound together by a common ruler (as in Hobbes’ famous Leviathan [1651]) and a common law. This basic structure of governance forged a social bond among citizens and between citizens and the state. Moreover, sovereignty gave rise to a sharp distinction between the domesticated interior and the anarchical exterior of the sovereign state.

In general terms, inside and outside came to stand for a series of binary oppositions that defined the limits of political possibility. The inside came to embody the possibility of peace, order, security, and justice. The international outside came to represent the absence of what is achieved internally: war, anarchy, insecurity, and injustice. Where sovereignty was present, governance was possible; where absent, governance was limited. Modern political life was thus predicated on an exclusionary political space. As democracy developed, sovereignty became understood as a political practice defining the social bond between the state and its citizens in terms of unity, exclusivity, and boundedness (for a discussion see Devetak and Higgott, 1999).

The other crucial function traditionally performed by the sovereign state has been the management of the national economy. Historically, there have been competing accounts of how states should govern their economies, especially over the manner and extent to which governments should intervene in and regulate economic activity. Within the dominant liberal tradition, national economies were treated largely as self-contained, self-regulating systems of
production and exchange delimited by the state’s territorial boundaries. This view was as true for economic liberals such as Adam Smith and David Ricardo as it was for economic nationalists and mercantilists such as Friedrich Liszt and Alexander Hamilton. This is not to suggest that these thinkers were blind to the fact that economic activity commonly spilled over national frontiers, but that they treated national economies as self-contained units in the international market. That states monopolised the right to tax within their boundaries further enhanced the correlation of the economy with the state.

In short, the modern state drew together several key functions under the principle and institution of sovereignty. The purpose of the sovereign state in modern political life was thus to stabilise the social bond between the state and the citizen. This was achieved by resolving questions of governance around the principle of sovereignty, which meant, as a corollary, establishing structures and practices of governance in terms of the direct correspondence between authority, territory, community, and economy – all embodied in the sovereign state. These parsimonious and elegant assumptions have dominated our understanding of sovereignty – or so the theory would have it.

But as Stephen Krasner has noted, a historical reading of the Westphalian theory of sovereignty has always underestimated how basic principles have always been transgressed or mitigated in one form or another. The golden age of absolute sovereignty that modern-day leaders make appeal to can only be political posturing at best and a political fiction at worst. All states are not, of course, the same, and one actor’s ideal type of sovereignty can be diluted by the behaviour of other actors in any of four ways: conventions, contracting, coercion, and imposition (Krasner, 1995-6, pp. 116 and 123-139). We need to recognise how fragile and how fungible the concept of sovereignty articulated in the Westphalian model really is. It has always been a negotiated state of being for states and their governments in the international system. For Krasner,

“… [the] … Westphalian model is better conceptualized as a convention or reference point that might or might not determine the behavior of policymakers who are also motivated by material interests, security, and national ideals, and whose ability to influence outcomes depends upon their power” (Krasner, 1995-6, p. 117).

Moreover, sovereignty has always been a Eurocentric, and later Western discourse (see Hobson, 2014). And the legacy of colonialism enacted by Europe on Asia and Africa has informed the development and practice of sovereignty. For the post-colonial or developing world, the presence or absence of sovereignty became synonymous with inferiority and difference by virtue of a Western intellectual tradition that defined access to sovereignty by a spectrum of dichotomies: developed–undeveloped, civilised–uncivilised, modern–traditional, democratic–undemocratic. Aspirations to sovereign statehood becomes conditional on moving toward the Western end of these spectrums. This facet of sovereignty is not without relevance for our discussion of digitalisation. If the 20th century was what Pourmokhtari (2013) describes as the “age of national imperialism” then it is not too far-fetched, as we will demonstrate, to see patterns of digital imperialism emerging in the 21st century.

It is in these theoretical and historical contexts that we must locate the modern-day discussion of sovereignty. The idea of states as discrete, unitary, rational, and self-contained policy actors has always been a fiction. The Westphalian model of sovereignty is frequently compromised, even for the most powerful of states. The international system does not consist of identical state
actors enjoying comparable levels of autonomous authority within state boundaries. Nor is it new to suggest that sovereignty is in a state of atrophy. Change has been a permanent feature of our understanding of sovereignty for more than 350 years. The next section identifies the current drivers of change in that system.

And sovereignty now: From globalisation to anti-globalism

The broad understanding of sovereignty described above continues to evolve. In short, two phenomena – globalisation and now digitalisation – have begun to unravel the distinctive historical resolutions of sovereignty and the sovereign state identified in the previous section.

With the passage of time and the changed milieu in which states exist, it has become increasingly apparent that the sovereign state is no longer adequate as a means of comprehensive organisation of modern political life and the provision of public goods normally associated with states. Increasingly, the sovereign state is seen as out-of-kilter with the times as first globalisation, and then digitalisation, transforms time-space relations and the forms of interaction of social and political life.

For definitional purposes we see globalisation as it developed in the last quarter of the 20th century as the stretching, deepening, and intensifying of global socio-economic relations driven by the changing nature of market capitalism, technology, and culture. The reconfiguration of power and authority under pressure of economic globalisation has progressively tested the capacity of the state to deliver welfare provisions and, in turn, has transformed the social bond between states and their citizens. The advent of new technologies, initially in transportation and then information and communication as the core elements of economic globalisation, has given rise to the compression of time and space at local, national, regional, and international levels.

The success of economic globalisation as a dramatic generator of aggregate global wealth caused many to miss – or perhaps more accurately to ignore – its unequal distributional effects and deepening inequalities. What did not go unnoticed was the progressive effects of economic globalisation on large sections of the lowest income people in the developing world, especially East Asia, as over a billion people climbed out of poverty in the last quarter of the 20th century. But it is now also well understood how globalisation has altered labour and employment relationships the world over, especially through the creation of greater job insecurity, increased unemployment, and growing income and social inequality in the manufacturing communities of the states that led and benefitted from the industrial revolution. The substitution of work forces in one part of the world for those in other parts in an era of increasing mobility of capital and technology is now easier. Economic globalisation privileged the skilled, the cheap, and the mobile at the expense of the semi-skilled, unskilled, and immobile.

This trend has put immense pressure on our understanding of state sovereignty. As domestic and foreign economic policy issues increasingly blur into one another, as the domestic economy becomes increasingly internationalised and detached from the sovereign nation-state, and as economic de-regulation and de-nationalisation continue, it has become, and continues to become, more difficult for states to manage the domestic-international trade-off. In short, the sovereign policy-autonomy of states has diminished in the face of globalisation. It becomes harder for governments to provide the compensatory mechanisms to underwrite social cohesion in the face of changing – often collapsing – domestic economic structures. Further, the increased mobility of finance makes it more difficult for governments to tax; thus the burden
of providing services falls increasingly on labour, making it difficult to run welfare states and fuelling the rise of the populist politics of resentment and nationalist objections to globalisation.

As we have seen since the closing days of the C20 and especially since the financial crisis of 2007-08, the internationalisation of trade and finance has ceased to be simply an issue of sound economic theory. It is also contentious political practice. When pursued in combination, free markets and the reduction of compensatory domestic welfare elements for those adversely affected by globalisation have proved to be a potent populist cocktail that heightens the demand for stronger sovereign behaviour on the part of the state at the very time that its ability to assert its sovereign autonomy is more challenged.

To recap, globalisation, in contrast to what many anticipated, has not led to the establishment of a single, integrated socio-economic space, but rather a disparate set of information-driven global networks that can function in part or as wholes, across global spaces. This goes some way toward explaining the unevenness in globalisation’s impact and the intensity of the reaction to it in recent years, reflected in the rise of populism and nationalism. What is important for this report is the degree to which the trend has been facilitated and accelerated by the tools provided for it by networked digitalisation in recent years.
2. Digital technology: A non-technical introduction

Let’s begin by restating the obvious: digital tools and services are essential elements of modern communication. Digital tools are increasingly fundamental for a range of uses like news consumption, education, entertainment, commercial activity, political communication, public diplomacy, communication between governments and citizens, the delivery of public services, financial services and transactions, and a range of other everyday activities. Digital technologies are increasingly present in our daily lives and can be instrumental in strengthening individual autonomy and self-determination. But this is not an axiomatic outcome of this activity.

An unprecedented amount of data is being created and collected with ever-increasing scale and speed. Much of this delivers considerable social value. Imagine life without a powerful search engine such as Google and the social benefits of free global maps, itinerary planners, and so on that are used by billions of users many times a day. But this does not diminish the challenges of data collection, which requires us to disclose vast amounts of increasingly personal information, both voluntarily and involuntarily. This data is becoming progressively monetised in largely non-consensual and non-transparent ways, including through third-party sales, for comparatively small amounts of personal convenience when matched against the economic benefits realised by a small number of companies. General public awareness of the scope and breadth of data collected at virtually every level of digital activity remains troublingly low. Especially as it is not just that data is collected but that information is retained, repackaged, and resold to countless companies with virtually no transparency or accountability. These processes remain opaque to almost everyone and indeed even most legislators do not understand.

In an environment of unprecedented interconnectedness and interdependencies, hard-fought fundamental rights that are valued offline must now be, but are failing to be, upheld online. How are these issues tied together? For example, how will commitments to the rule of law, informed decision-making, and human rights be honoured amidst the ongoing processes of digitalisation and the related social, political, and economic transformations fuelled by technological advancements? Negotiating what we might call competing sovereignties – state, economic, electoral, and individual – is one of the great challenges of our time.

While technology was supposed to enable the free flow of information with unprecedented speed, irrespective of national boundaries, this vision has been displaced, or is at least in contention with governments seeking to reign in this technological freedom. But was technology ever without unfettered regulation from the state? States have long exerted control over their media and informational landscape. There are of course necessary regulatory functions the state has over things like spectrum allocation and broadcast licensing, but even these are subject to abuse by states such as in Hungary, for example, which has weaponised these powers against a free press in favour of the Orbán regime. These controls also run the spectrum from direct censorship to criminal penalties and sedition and blasphemy laws, but also includes efforts to assert sovereignty over the technology and infrastructure of the time.

In the 18th and 19th centuries for example, British governments enacted taxes and duties on newspapers, including a stamp duty that made the publication of pamphlets or papers that failed to pay up illegal. Critics called these ‘taxes on knowledge’ to limit the growing independence of the press. In the 1960s, Western European governments seeking to stop popular offshore pirate radio stations from broadcasting in international waters, over which they had no
jurisdiction – perhaps most famously Radio Caroline – elected to make it illegal for domestic companies to advertise on their airwaves as a way to force stations off the air by going after their primary source of revenue. The Soviet Union, as part of its multi-pronged efforts to control information and media production, tightly restricted the ownership and use of photocopiers to try and prevent the distribution of underground Samizdat (self-publishing) literature. Transnational satellite broadcasting has even served as a disruptive technology, threatening state media monopolies by allowing voices to break through closed environments. Such was the case in Iran where the government – technically and jurisdictionally incapable of blocking satellite broadcasters operating from outside the country – passed a law, albeit unevenly enforced, prohibiting ownership of satellite dishes. The government undertook a major crackdown in 2016, even though approximately 70% of Iranians rely on satellites for television, and it should be added, to bypass state censorship of the internet.

The lesson here is that states looking to exert control over their media environments can find quite creative ways of cracking down on the free flow of information, and often do so by seeking to curb access to the latest disruptive technologies, whether this is by restricting internet access or by taxing the actual ink newspapers are printed with.

**Digital sovereignty and data**

Digital sovereignty implies that states must have the capacity to regulate digital activities and to enforce regulations. For civil society and individuals, this means being in control of one’s own digital data. This includes, but it is not limited to, how data and digital assets are treated and extends through to an individual’s right to privacy. The concept has also more recently become closely tied with opposition to the hegemony of the US and US-based FAANG.

The European Union is the most active pursuer of measures to reframe internet governance around an international framework of state sovereignties rooted in privacy and data protection, as guaranteed in the EU’s Charter of Fundamental Rights. Calls for digital sovereignty helped initiate the EU’s General Data Protection Regulation (GDPR), which overhauled how companies operating in Europe process and handle data.

GDPR went into force in 2018 and is now the strongest set of data protection rules in the world. While not without its flaws and critics, GDPR nevertheless creates stronger accountability and compliance mechanisms, harmonises rules across EU member states, and most profoundly, it grants far greater protections to the public, including allowing people better access to the data that companies hold about them. It also adopts clearer requirements for organisations and companies to obtain consent from the people about whom they collect data. There are stiff financial penalties for failure to comply.

Digital sovereignty has also come to frame the broad set of concerns in Europe about the ever-increasing dominance of primarily US-based tech companies, including the low tax or non-existent rates paid by American companies. The EU’s Commissioner for Competition is investigating Amazon for its use of consumer and sales data to gain an unfair market advantage over smaller companies. Angela Merkel and Emmanuel Macron have been outspoken in their desires to build European competition in digital and cloud services and artificial intelligence, for reasons of economics and security, and to reduce dependencies on American tech companies like Google and Microsoft for data storage and management. Macron (RFI, 2019) has gone so far as to say “the battle we’re fighting is one of sovereignty… If we don’t build
our own champions in all areas—digital, artificial intelligence—our choices will be dictated by others.”

GDPR can be read as one way of reasserting European sovereignty over the tech space. It also strongly asserts a right to privacy. It is reasonable to assume that it is pressures such as these that have seen Google move the data of UK users from its current headquarters in Ireland to the US, prompted by a lack of certainty that post-Brexit UK data laws will be robust enough. Microsoft lost German contracts after a state data protection authority objected to its use of Office software in a local school district, arguing the company could use student data for its own purposes. A Swedish court raised jurisdictional concerns in the deciding of the 2018 US CLOUD Act, which requires an internet platform with a US presence to provide customer data for use in a US criminal case even if that data is being held on a foreign server.

In 2011 the WEF, among others, suggested that personal data would be the new “oil” (WEF with Bain & Company, 2011). If so, then the leaders of the digital industries, the US FAANG corporations (Facebook, Apple, Amazon, Netflix, and Google) occupy a role in the high-tech sector akin to that of the ‘Seven Sisters’ in the 20th-century oil industry (Sampson, 2019); they are global, innovative, breakthrough organisations with a tendency towards monopolisation and a view of themselves as being largely beyond the control of the state.

However, data – unlike oil – is not a naturally occurring material sitting inertly in the ground awaiting extraction for its financial value to be realised. The analogy obscures the ways in which data is generated, appropriated, and sold, often with troubling accompanying implications. Nick Couldry and Ulises Mejias (2019) go as far as to suggest the new data relations represent a form of “data colonialism” – hence the allusion in our discussion of sovereignty to a new 21st-century imperialism. More than 95% of global cell phones and desktop operating systems are run by Apple, Google, and Microsoft.

What’s at stake?

If Facebook were a country, in population terms it would be the world’s largest, with over two billion citizens (i.e., ‘people on its site’). It would also, as Cynthia Wong (2018) argues, “be ruled by an opaque, unaccountable, and undemocratic regime”. As far back as 1980, Langdon Winner argued that technologies themselves have political power and embody social relations. In ‘Do Artifacts Have Politics?’, he concluded that “the very process of technical development is so thoroughly biased in a particular direction that it regularly produces results heralded as wonderful breakthroughs by some social interests and crushing setbacks by others”.

Early optimism for the internet and its potential is reflected in the mission statements of the social media companies who like(d) to see themselves not ‘just’ as tech companies but as community builders, with mottos like Google’s now retired ‘Don’t be evil’. Indeed, first movers in the development of digitalisation – who Rana Foroohar of the Financial Times (2019) calls the “digital utopians” – were convinced that the internet would be a force for good. The free flow of information in a decentralised digital ecosystem would be a democratising force spreading trust and transparency and breaking down communicative borders. Over time, this utopian hope has been challenged in response to changing realities.

We recognise that technology and social networks can be vital tools for journalists, human rights defenders, and social movements in their work to hold power to account, as well as
models of cooperative platforms and innovation offering alternatives. Jonathan Zittrain argues in *The Future of the Internet and How to Stop It* (2008) that the trajectory of the internet has been one of lost opportunity and new forms of control, but its salvation might just lie in the hands of users, or, so-called netizens. Generative technology projects like Wikipedia, he argues, offer open models of networked collaboration.

While there is absolutely opportunity for a different way forward, the darker and commercial aspects of online behaviour and surveillance regimes are currently overshadowing these hopes. The most apocalyptic of contemporary visions of the internet now see it as the major threat to democracy (see Bartlett, 2018). As Foroohar notes, the opportunities and pressures to monetise data – through a “business model based largely on keeping people online” (Foroohar, 2019, p. xvi) – have superseded the utilities of freedom with attendant implications for the relationship between the digital industries, power, and politics. Such conflicting visions and realities have resulted in an uneven, fractured, and contentious operationalisation of internet governance. It has also given rise to more fundamental questions about how social media works simultaneously for and against people. In his book, *The Googligization of Everything*, Siva Vaidhyanathan (2011) warns that companies like Google generate a blind faith and dependency towards “techno-fundamentalism”. As he says, “We google, we don’t search”. We ignore, or more precisely, simply do not know how their internal decisions and algorithms affect our lives in ways we do not think about and do not see.

**Algorithmic decision-making and individual sovereignty**

Data-driven systems and technologies are designed to achieve optimum solutions based on the parameters *set by their developers*. When operating at scale, these programmed processes inevitably prioritise certain values over others, with profound implication for how we process content, access information, and make decisions. Machine-learning relies on the breadth of user data to prioritise results in search, shape and predict personal preferences and recommendations, and alter flows of information. The increasing use of algorithms and machine-learning make it possible to infer intimate and detailed information about individuals.

This encourages and enables micro-targeting of individuals as they are sorted into categories that reinforce social, economic, cultural, and gendered segregation and possible discrimination. A 2016 ProPublica investigation (Angwin and Parris Jr., 2016) found that Facebook was allowing advertisers to target housing ads in a discriminatory fashion. Facebook’s advertising sales programme allowed advertisers to screen out users based on race, gender, family status, and other categories explicitly protected by fair housing law. Facebook claims to have removed these discriminatory targeting options, but a 2019 lawsuit filed against the company by the US Department of Housing and Urban Development claims otherwise.

Personalised, fine-grained layers of algorithmic persuasion can have real impact on individual autonomy and people’s ability to form opinions and take decisions independent of automated influences. The effects of the vastly expanding targeted use of aggregated data require responses that go beyond data protection. They require us to ask fundamental questions about the ‘datafication of society’. Machine-learning tools already have the capacity to predict choices, but also the power to influence emotions and thoughts, even at the subliminal level. The societal risks are real, but little understood. Algorithmic tools are widely used for commercial purposes, but also increasingly for political gains within democratic countries and to promote the ambitions of authoritarian or anti-democratic regimes wishing to inflict targeted
harm and electoral interference. Significant power is thus conferred on those who control such algorithmic tools, be they companies or governments.

Algorithms are increasingly used to make decisions on all manner of information accessibility. The word ‘algorithm’ refers to computer code that carries out a set of instructions, or a series of steps, like in a recipe. They are essential for computers to process and calculate how to use data. What articles and whose posts appear in your Facebook newsfeed are examples of algorithmic decision-making. Algorithms are essentially built to approximate the world and accommodate the architect rather than internet users (Wagner, 2019).

Human bias is of course embedded into algorithms. Individuals train the machines and write the code that makes decisions about content. People also form the backbone of the manual, content-moderation teams. So, rather than positing the debate as a dichotomy of humans versus machines, the focus should be on reframing the question to ask what machines are being trained to look for what, and what they do with what they find.

These biases are not insignificant concerns. Speaking at the 2019 World Economic Forum, MIT researcher Joy Buolamwini described what she calls “the coded gaze” as a “reflection of the priorities, the preferences, and also sometimes the prejudices of those who have the power to shape technology” (Feloni, 2019). Just this spring, IBM and Microsoft announced plans for a moratorium on their facial recognition software technologies, citing concerns of bias and their use by law enforcement in ways that have demonstrated harm and bias against black Americans. That these announcements came in the wake of public outrage and protest over police brutality and surveillance in America is not without relevance here.

Zeynep Tufekci (2019) argues that while social media speech might feel public, the reality is we each experience content differently, since companies target and deliver posts to each user in a highly fragmented manner depending on complicated and non-transparent algorithms geared to maximising advertising revenues and corporate profit. Search engines and social networks manipulate what we find and who we interact with online in ways that maximise value to advertisers but limit the range of what people are exposed to. In effect, users can succumb to behavioural persuasion emanating from digital companies.

This is evident in how information is privileged through the algorithms of newsfeeds and search results. Even something like Facebook’s Free Basics programme, which is marketed as an ‘on ramp’ to internet access for people in the Global South, only creates access to a very narrow window of the internet by offering ‘free’ access to a limited number of specific applications, such as Facebook and other content providers, to the users they have contracted with or that governments allow (Biddle, 2017). Mobile carriers entice users by offering similar ‘zero rating’ plans. Few African countries, for example, have data protection or net neutrality requirements for internet providers to treat all digital content equally, without favouring specific apps. Lax government oversight means that people may never be informed that they pay for these ‘free’ apps by exposing their personal information to data mining by private companies. While some would argue a limited internet is better than no internet at all, these examples help underscore the evolving, indeed compromised, nature of digital sovereignty, and the different kinds of internet, or intranets, people are experiencing based not only on state controls, but through the mechanisms of privatised infrastructure.
Unsustainable asymmetries

The wider political impact of digitalisation changes as the interests of the owners of these most powerful economic forces on the one hand and consumers on the other become excessively asymmetrical. For sure, information asymmetries have always existed in society. There is a whole subfield of economics and media studies built around it. Indeed, most successful polities and societies exhibit economic and political inequalities and asymmetries. The problem occurs when these inequalities and asymmetries become so exacerbated as to be unsustainable. A question to be explored is whether we have reached the level of unsustainability in the power relationship between digitalisation and politics and its effects on the sovereignty of states, their governance structures, democratic or otherwise, and their international relations. This all begs the question of who governs the internet, and in whose name or benefit.
3. Sovereignty and governance: The role of digital networks

Internet governance and the changing balance of power

Who runs the internet? This is a question with no clear answer, but rather many answers – there is no singular entity ‘in charge’. According to the UN Working Group on Internet Governance (UN-WGIG, 2005) internet governance is the “… development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, and decision-making procedures that shape the evolution and utilization of the internet”. Internet governance is not the product of a singular institutional hierarchy but has rather emerged from the decentralised and bottom-up coordination of tens of thousands of primarily private companies around the globe, from internet service providers, to server operators, standards organisations, and domain name registrars (Masters, 2014). Bertrand de La Chapelle reminds us to distinguish between governance of the internet – the protocols and identifiers – and governance on the internet – the way it is used, the application layer, and more. The former has a progressively evolved ecosystem of institutions – IETF, W3C, RIRs, DNS operators, ICANN and more – while very little exists for the latter.

Of all those who use and take the internet for granted in the current era, only a small proportion really know how it works. The aggressive extraction, personalisation, customisation, manipulation, and continuous experimentation with data from the internet (see Tufekci, 2019; and Zuboff, 2015 and 2019) has become inseparable from internet use, often in ways little understood by anyone other than those with the expertise at the core of the new technology. Its effects on politics have been profound. Outside China and Russia, US-based companies dominate. This is leading to tensions and contests, especially (i) between states and corporations as they vie for regulatory control of the tech industries and (ii) between nation-states as they strive to control their own international and regional spheres of digital influence. So, how do we govern the internet?

Internet governance itself needs to be understood in relation to the changing role of both the private sector and the state, and the interplay between them. Most intermediaries operate across multiple state jurisdictions and technical arrangements are themselves a form of order. Of course, maintaining openness of networks and interoperability across the multitude of platforms requires cooperation among a wide range of actors, from states and international organisations to developers, internet service providers, network operators, internet users, and digital rights defenders. For example, ICANN, the operating body managing the global Domain Name System (DNS), a non-transparent organisation with tremendous powers over the internet, nevertheless represents what Milton Mueller (2010) calls a “revolutionary departure from traditional approaches to global governance” in its reduction of the powers of national governments and existing intergovernmental organisations.

As the internet has evolved, and contentious policy issues have come to the fore, the idea of internet governance has resulted in the conflation of technical resource management with the governing and policymaking around how the internet is actually used and experienced. This once decentralised, open model of the internet has been displaced by new gatekeepers in the hands of both states and private enterprises. The ‘old’ internet, as David Kaye points out, was hard to police (2018).
Lawrence Lessig argued in *Code version 2.0* (2006), software and technical standards are for all practical purposes a new form of law because, like laws, they shape what people can and cannot do. He reasoned that technical standards programmed into software, social media platforms, search engines, and algorithms – determined by private corporations – now have the power to shape how we organise and disseminate information. To the extent that sovereignty is exercised by the adoption and enforcement of laws, digitalisation is giving birth to a new form of sovereign control.

Our standard assumption is that it is the governments of sovereign states that hold responsibility for determining the boundaries and codes governing what people do in the physical world, backed by their authority and might. This assumption is constantly being tested online. New forms of power are held by those who write the code and programme the machines for what code should be written. Governments try to use the weight of their influence and force of their laws to reign in control of the internet when they see their sovereignty under threat, either from the unchecked power of corporations, or from individual autonomy and the freedom of social movements or political opposition. Yet, such is the pace of technological change, when states attempt to exercise control over the virtual world they are often fighting the last war rather than the next one.

The FAANG corporations are now the biggest, richest, and most powerful companies in the world. Their collective market capitalisation is greater than all states with the exception of the US, Japan, China, Germany, and the UK. But drawing up ‘national balance sheets’ hides the significant complexity and real depth of the global interconnectedness of these industries. For example, it hides the depth of the global supply chain relationships between these US companies and their Chinese interlocutors and other partners as indispensable providers of the integral component parts for their products. And size matters politically, both domestically and internationally. It has implications for our two core questions concerning: (i) sovereignty and the manner in which it is affected by the growth of digitalisation; and (ii) what it means for the governance and politics – both domestic and international – of the internet.

At the domestic political level, there are clearly correlations in the major states between: (i) the growing ability of government, through the use of the internet, to survey and manipulate the political thinking and behaviour of citizens (maybe both individually and collectively) and the attendant political implications discussed above; and (ii) In a manner analogous to what happened with the industrial revolution that displaced agricultural and artisanal labour through mechanisation, the massive and growing presence of the digital industries in the economies of the major states must be set against the decline of other once powerful industrial and manufacturing sectors and the labour forces they employed.

These two correlations are reflected in: (i) the growing political attraction and influence of populism and ‘illiberal democracy’ at the expense of liberal democracy; and (ii) the growing nationalist resistance to ‘globalism’ – basically international trade and cultural cosmopolitanism. Both correlations have major implications for traditional understandings of sovereignty.

At the international level, the effects of digitalisation are also broad and deep. They go well beyond the now widely acknowledged use of social media and hacking activities by motivated international actors such as Russia to interfere in and manipulate the electoral politics of other
countries, such as the interventions in US elections. The race for digital hegemony is also changing the international balance of power. It is at the heart of the contemporary contest between the US and China. It has spurred a return to geopolitical and bipolar thinking after a brief, cooperative post-Cold War honeymoon. The effects of such thinking could be self-reinforcing.

Even the European Union, still in theory the principal champion of multilateral, international institutional collective action problem-solving, now asserts that it has for too long been “too soft”, as President von der Leyen said at Davos in January 2020. She, and her High Representative for Foreign and Security Policy, Josep Borrell, talk about the need for the current EU Commission to become a “Geopolitics Commission” and, à la President Macron, they talk of the need to secure national “digital sovereignty” (DS) as a priority across the major European states (for a discussion see Higgott and Langenhove, 2020). Here, the distinction between ‘digital sovereignty’ and ‘sovereignty in the digital age’ (SITDA; i.e., its redefinition) is important. DS, reaffirming a traditional competitive mindset, is a rallying cry for the expression self-interest. SITDA, by contrast, also relates to the responsible exercise of national sovereignty in shared online spaces where the jurisdictions of several countries can overlap. SITDA does not negate competition but also reflects the challenges of coordination and cooperation.

Digitalisation changes the nature of state power, international relations, and diplomatic practice. Digital networked communication changes approaches to international bargaining and strategy from the pre-digital age. So, if we are thinking about the changing nature of the autonomy of states, we need more precisely defined minimal conditions for multilateral cooperation that recognise: (i) that digitalised network activity in combination with centralised corporate power change the nature of connections in global governance; (ii) that networks do not require government sanction. Indeed, networks – unlike the more traditional institutional hierarchies of the second half of the 20th century – encourage self-organisation; (iii) that the governance dilemma is no longer simply democracy versus autocracy, although that dilemma remains; but in addition, it is also a question of open governance versus closed governance (see Slaughter, 2017) and, we should add, open versus closed digital spaces in competing centralised versus decentralised systems.

What would the governing principles of an open digital world order look like? Some traditional liberal values will presumably remain salient. There would still be a place for democracy of many variants, freedom of thought and expression, rule of law, and human rights. But how would these values be enabled and/or coexist within a context of the greater influence of national and “civilisational” values (see Higgott, 2020), especially when experienced through devices, networks, and technologies owned by private companies largely based in the US? But what happens when governments demand tech companies bend their products to fit their restrictions and cultural norms? In an open, networked, decentralised digital order we should also expect power to be distributed more horizontally – both publicly and privately, with fewer hierarchical control mechanisms and with flatter, reciprocal structures – than in the past.

Calls for privacy by design – that is, building public-interest and trust mechanisms into digital devices and tools – will mount. Sasha Costanza-Chock (2020) argues design justice, or ways in which design might be led to help marginalised communities dismantle, or at least mitigate,

---

4 See the empirical evidence in the ‘Mueller Report’ (US Department of Justice, 2019) and the Senate Intelligence Committee inquiry into Russian interference (Ratnam, 2020).
structural inequalities, can be expected to grow. An open order will work with more nebulous terms such as ‘community’ and ‘civilisation’ in which we will inevitably see, indeed are seeing, digital spheres of influence, albeit with fuzzy and fractal borders, consolidate around the superpowers at the same time as new sites of resistance emerge. Indeed, they are already developing as the role of the so-called “civilisation state”, traditionally resistant of Westphalian notions of sovereignty, becomes more prominent in international relations (see DOC Research Institute, 2019; and Higgott, 2020).

Intermediaries, state power, and sovereignty

The primary function of international economic legal organisations under what we might call the traditional conditions of sovereignty was always, in the last instance, to preserve the power of the nation-state to regulate its own markets. National markets, pre-globalisation, were constrained by borders. The state also determined the market for media in the pre-digitalisation era, since media was a predominantly national enterprise. The state would act as regulator in its own domestic spaces. It did so not only to protect national broadcasters but also national identity. States were and often are responsive to other states. In 2016, French satellite television provider Eutelsat dropped the broadcast of a Kurdish channel at the request of the Turkish government, saying it broadcast propaganda from the Kurdistan Worker’s Party (the PKK). In the late 1990s, the German government expressed anxiety over the number of Turkish satellite television channels in the country. If people were watching Turkish television, the government argued, they weren’t assimilating with German culture. Turkish people, on the other hand, rightly argued that they carry multiple identities.

Laura DeNardis (2014) argues that state control of internet governance functions via private intermediaries and has “equipped states with new forms of sometimes unaccountable and non-transparent power over information flows”. This includes the adoption of laws that hold these companies responsible, often with stiff financial penalties, if they fail to block or remove content within a specific jurisdiction in which the company might operate, such as Germany’s NetzDG law. As a result, these intermediaries often censor content on behalf of governments without adequate safeguards for freedom of expression and privacy, or without transparency and accountability mechanisms. Holding internet intermediaries liable can shift some state activities – especially law enforcement and responsibilities such as copyright enforcement – on to ISPs. In Thailand, a journalist and blog editor was convicted in a criminal court, under Thailand’s lèse-majesté law, for failing to remove a user comment on her blog (BBC News, 2017, ‘Lese-majeste explained’).

Internet intermediaries – the services, infrastructure, and devices that allow people to connect to the internet and transmit content, such as ISPs, web hosting providers, social media platforms, and search engines – also need to be understood in the changing context of state power. They can act as control agents between sovereign governments and citizens, as governments around the world increasingly press intermediaries to block certain kinds of online content deemed inappropriate; for example, hate speech, privacy violations, and the like. Pressures, emanating largely from governments, are growing to make social network intermediaries legally responsible for what their users do and say. Most intermediaries operate across multiple state jurisdictions and technical arrangements are themselves a form of order. Of course, maintaining openness of networks and interoperability across the multitude of platforms requires cooperation among a wide range of actors, from states and international
organisations to developers, internet service providers, network operators, internet users, and digital rights defenders.

Informal modes of cooperation that transfer decision-making from states, that are legally obliged to protect and respect human rights, to private entities, that do not have the same obligations, carry important implications for human rights if the necessary safeguards are not put in place. The UN and the Council of Europe have been clear in advocating against ad hoc relationships between states and companies that bypass human rights obligations. The Council of Europe’s Commissioner for Human Rights concluded:

“rule of law obligations…may not be circumvented through ad hoc arrangements with private actors who control the internet and the wider digital environment…Member states should stop relying on private companies that control the internet and the wider digital environment to impose restrictions that are in violation of the state’s human rights obligations” (Council of Europe, 2014).

Most intermediaries operate across multiple jurisdictions and must comply with national laws in both their home and host countries. Within the EU, internet companies must also comply with other legislation such as the GDPR, the E-Commerce Directive, and competition law, among others. The OECD has recommended limiting intermediary liability as one of its 14 recommended Principles for Internet Policy Making (2014) to “promote and protect the global free flow of information”, principles that also include transparency, due process, accountability, and multi-stakeholder policymaking. In the US, the Communications Decency Act of 1996 (CDA) (47 USC § 230) removes liability from internet companies for content generated by users, which has made the US an attractive home for tech companies. Proposals to revise Section 230 in the US and the expected EU Digital Services Act might, however, change this.

Sandra Braman (2006) has argued that the “informational state” is replacing the control of the bureaucratic welfare state over information creation. Its ability to process flows and uses of information becomes a more effective form of power. As the informational state comes to know more and more about individuals, individuals come to know less and less about the state. Any model of representative democracy requires a two-way process in which individuals have a basic knowledge of the activities and practices of government and the government has sufficient knowledge about citizens to apportion representation and resources. There are things states legitimately need to know about us. With the informational state, however, the capacity of the state to gather and process information about its citizens and about the resources and activities within its space has grown and continues to grow exponentially. At the same time, the ability of citizens to learn about what the government is doing is declining at a similar rate.

Rebecca McKinnon (2013) describes what she calls “networked authoritarianism” to describe the ways in which corporate networks are turned into opaque and subtle yet invasive extensions of state power. She argues that both the corporations and governments that build, operate, and govern cyberspace are not being held accountable for their exercise of power over all who use these networks. She claims that governments are exercising power over people beyond

---

5 General resolutions as part of the EU’s Digital Single Market emphasise that the limited liability of intermediaries is essential to protecting the openness of the internet, fundamental rights, and legal certainty and innovation. Yet the E-Commerce Directive encourages intermediaries to remove content on the basis of third-party or law enforcement requests without judicial determination of the legality of the content at issue. Thus, there exist contradictions even within EU directives.
their jurisdiction and without the consent of the networked. For all governments, especially, but not only, at the authoritarian end of the spectrum, control and the question of where and how data is stored matters.

The battle in the “market for loyalties” (Price, 2002) sees states in a shuffle for allegiances wherein they often use communications regulation to organise a cartel of mythologies and identity among themselves. Under the increasingly authoritarian regime of Hungary’s Victor Orbán, in a wholesale undertaking to control the narrative through state capture of the media and cultural institutions – including a complete redrawing of its media laws and the introduction of a wide range of measures to control news and information – the government has seized direct control of communications regulation. It eliminates most mainstream press unfavourable to the regime through a variety of formal and informal measures. Orbán’s media constitution has also sought to establish regulatory jurisdiction over the internet by seeking to require blogs of a certain size to register with the state, and seeking to regulate virtually all online content in the Hungarian language, produced by Hungarians, or aimed at a Hungarian audience, whether the producers were based within the sovereign borders of the country or not (Dunai, 2014). Whether this can ever be enforced is questionable but its intent is noteworthy. At the very least, it is an attempt to create a virtual border around a Hungarian sovereign cyberspace of its own imaginary.

In 2018, an investigative report from Bloomberg (Robertson and Riley, 2018) revealed that China inserted microchips into computer servers used by almost 30 US companies, including Amazon and Apple, which granted China unprecedented backdoor access to data and computers. This has serious potential economic and national security implications given the global trade model relies on outsourcing parts, especially with so much technology manufactured in China. Russia now requires public employees to use mobile phones that are locally produced and that run on locally produced software. India, as well as Russia, wants foreign tech and electronic payment companies to store data on local servers. Data localisation poses a range of challenges because it opens up the possibilities for state surveillance but ostensibly also allows countries to sustain greater technological sovereignty.
There are numerous examples of governments pressuring companies to do the work of law enforcement for them. David Kaye argued, “[i]t is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone’s security online” (Kaye, 2015). For example, the Turkish government, following the failed coup in July 2016, came down heavily on dissent and opposition voices online. The Ministry of the Interior reports that from August 2016 to January 2017 alone, 10,000 people were under suspicion and 1,656 social media users were arrested on suspicion of spreading terrorist propaganda and insulting state officials. President Erdoğan has regularly blocked access to social media platforms and communication apps in the name of ‘public safety’.

**BOX 1**

**Russian internet legislation**

In Russia, a series of anti-extremism and internet laws introduced since 2011 have given the state far-reaching powers to control online communication and curb political speech. 2011 was a turning point in Russian internet policy, perhaps not coincidentally commencing in the midst of the Arab Spring and as Russian civil society actively began using social media to organise protests. Laws including the ‘Yarovaya Law’ require any personal data of Russian citizens to be stored on servers within Russia. This means that any website or mobile application available in Russia is required to be hosted on Russian servers. LinkedIn has been blocked from operating in the country for noncompliance with this law; however, more significant companies such as Facebook and Google do not store data on Russian servers but have yet to be penalised. Telecom operators must store phone conversations, text messages, and internet traffic of users for six months. Operators of free Wi-Fi hotspots like those in cafes or libraries must collect and store personal data on all users.

In 2019, Russian lawmakers passed ‘sovereign internet’ legislation to further centralise control by allowing Russia to create its own autonomous internet under the guise of national security protection in the event of a cyberattack.

Other laws grant Russian authorities access to user data, including requirements for internet and telecommunications companies to turn over data to the FSB upon request, without a court order or justification. This law applies to all data, and to sites located anywhere in the world with a reader in Russia. The law also makes it a criminal offense to not warn the authorities of ‘reliable’ information about planned terrorist attacks and several other crimes. Other Russian laws grant authorities the power to blacklist and force a broader array of websites offline, without court orders. The ‘bloggers law’ requires blog owners and social networks with over 3,000 readers to register with state authorities. Authorities blocked access to Telegram, an encrypted messaging app, and promulgated laws criminalising the spread of ‘fake news’.
Elections, sovereignty, and disinformation

One core element of any country’s ability to define itself as sovereign is it to be found in its ability to conduct and control its own elections. In democracies, this means that elections must be, to use the popular cliché, ‘free and fair’. Modern communication technologies and social networks should be powerful spaces for people to engage in open and pluralistic debate, and in many basic and highly creative ways, they are. But the possibilities for the manipulation of elections, and their being targets of foreign interference, are real when the vast majority of users congregate on just a few centralised digital information channels. When this coincides, as in the US and Europe, with the ongoing decline in newspaper circulation, social media – especially with its dramatic rise in concentrated online advertising – is not fulfilling the democracy enhancing-role that the early utopians had envisaged.

This mix of centralised and privatised social media platforms, targeted advertising, data monetisation, the decline of newspapers, and the decline in trust, has generated an informational disorder ripe for exploitation. Political consulting firm Cambridge Analytica improperly misappropriated the personal data of a reported 87 million Facebook users without their consent, data they had they had inappropriately obtained, which was then used by Donald Trump’s 2016 presidential campaign.6

How democracy is to persist in the face of this onslaught in the digital era, especially in the hands of the unscrupulous, is now a major issue. Disinformation campaigns intended to create harm have become tools of information warfare in ways that question national sovereignty and

---

pose new challenges for a state’s international relations. Exogenously generated cyberattacks intended to disrupt elections are an act of international harm. Such attacks include not only disinformation campaigns but also unlawful hacking of information systems, the use of sensitive information on candidates to sway public opinion, the manipulation of election results, and the issuing of denial-of-service attacks.

Why are disinformation campaigns so pervasive? Are they the dark side of digital diplomacy? They clearly create distrust but are they changing hearts and minds? If citizen response is any guide, then the answer is on a spectrum from ‘probably to certainly’. In an era of digitalisation, ‘echo chamber’ politics is reinforced by what Eli Pariser has called “filter bubbles” (2012). Much of what most people see online is determined by algorithms programmed to give back more of what we are already interested in based on automated data capture of what they have fed into the system in the first place. Algorithms draw on search histories, physical locations, click behaviour, and much more to determine the information we receive in our social media newsfeeds and elsewhere online. We are thus our own unwitting filters.

Of course, neither propaganda nor electoral interference among states is new. The traditional ‘informational war’ still remains among state broadcasting platforms – with all its ideological and cultural baggage – with Russia’s contemporary equivalents Russia Today (RT) and Sputnik, and Voice of America (VOA), an American Cold War holdover in the midst of dramatic and concerning changes. This comes alongside a new Cold War involving micro-targeting that is hard to detect and counter, unlike the state broadcasting of VOA or Radio Free Europe, such as those of the St. Petersburg-based Internet Research Agency, which has sought to influence recent US elections through computer hacking and extensive social media disinformation campaigns. Congressional and voter fears, if not presidential ones, are running high in the current US election cycle in the face of evidence of continued Russian efforts to foment chaos and distrust. Similarly, German intelligence officials cite evidence of Russian support for Eurosceptic and anti-immigrant parties across the EU, as well as in the Brexit vote. Even more invasive campaigns are undertaken by Russia against its immediate regional neighbours.

Conversely, authoritarian states, in the name of sovereignty, justify their own global internet policy agenda in which censorship and surveillance are rationalised in the global conflict of freedom of expression. Russia, for example, sees arguments for unfettered freedom of expression as an imposition from the West. 2020 is a far cry from 1989, when the ideals of a borderless world captured in the Western grand narrative – that liberal values of democracy, freedom of speech, and human rights would flourish – briefly prevailed: “… [t]he ‘information war’ world view is now used to argue for a ‘multipolar’ world where there are no universal norms, just zones of influence” (for a discussion see Pomerantsev, 2019). The Russian Parliament has gone so far as charging Deutsche Welle with interference in Russian internal affairs for its coverage of anti-Putin protests in Moscow. Legitimate reporting has been equated with disinformation and propaganda.

Yet this is not just a Russia vs the West phenomenon. The US has also had a long history of its own brand of cultural intrusion into other societies and its own conspiratorial narratives, including those promulgated by the current president, who tweets regularly about vast domestic

---

7 In June, 2020 President Trump appointed a new CEO for Voice of America whose controversial first moves in office prompted a bipartisan group of Senators to raise concerns that the VOA and its subsidiaries Radio Free Europe/Radio Liberty would become pro-Trump propaganda outlets, raising questions about the future quality of reporting, and certainly harkening back to the Cold War era operation.
media plots against him and gets his daily briefings from Fox News, which itself dismissed the coronavirus as a hoax and spread false information and conspiracy theories in the early days of the pandemic (Swisher, 2020).

Similarly, domestic disinformation campaigns provoke distrust and undermine shared realities in China, Poland, Iran, and indeed around the globe. During recent elections in India and Brazil, the messaging platform WhatsApp became a popular site for targeted disinformation campaigns to benefit the eventual victors Premier Modi and President Bolsonaro. This platform is used by over 200 million people in India alone, and by nearly half of Brazil’s 210 million citizens. The proliferation of disinformation and misinformation in private message groups poses a particular challenge. Fact-checking initiatives also have difficulty tracking content on the app. Calls for Facebook to do more to intervene are strong but also mixed with concerns of the company not only acting on its own political agenda or biases but also serving as a tool for state surveillance.

Not all disinformation campaigns are connected with elections. There is emerging evidence, according to the US State Department, of Russia-linked disinformation campaigns to spread conspiracy theories against vaccines in the US (Kirk, 2019) and alarm about the coronavirus pandemic (Glenza, 2020). When Saudi Arabian journalist Jamal Khashoggi first disappeared, Twitter suspended a network of bots promoting Saudi government talking points. Research from Brown University has shown that approximately 25% of all tweets on climate issues, over a third of which referred to fake science, are generated by bots – software masked as a human that can be programmed to tweet, like, direct message, or retweet. Responding to disinformation and misinformation online, Facebook, YouTube, and Twitter have disabled hundreds of thousands of accounts and bot accounts for violation of terms of service, but such accounts are easily mirrored or reproduced elsewhere.

Facebook has also been subject to legitimate, serious criticism for its decision to continue running paid political ads. While Twitter elected to stop accepting political ads, Facebook reaffirmed its policy of allowing political ads, and allowing those ads to go unreviewed by fact checkers, thus allowing campaigns and candidates to spread lies and mistruths. Facebook’s solution, after months of pressure, has been to offer users a bit of choice over the ads they see. But this has done little to assuage fears. In aiming for neutrality, the company’s policies effectively elevate politicians’ words above consequence and obscures the current state of political discourse and platform power.

So, is digital sovereignty at odds with the basic tenets of electoral integrity? And whose digital sovereignty are we talking about – that of states, the tech companies, or citizens? If in posing this question, we are talking about a new version of self-determination and the capacity to make rules, then we are talking about sovereignty in a heretofore unprecedented manner. Further, if the state chooses to take a techno-libertarian approach – or as some leaders do, a personalised approach – not to intervene or go so far as to encourage intervention, even when its core democratic functions are under challenge, how can electoral integrity be safeguarded? A recent study from Pew Research Center (Gilberstadt, 2020) found that in the US, a nearly identical percentage of both Republicans (76%) and Democrats (74%) have little confidence that tech companies can or will prevent the misuse of their platforms in the 2020 elections.

Threats to elections as an attack on national sovereignty are, Evgeny Morozov (2018) argues, one factor causing states to take a more interventionist approach towards the tech sector. France recently passed a controversial law granting judges the power to order the removal of content from social media and to block sites that publish such content during elections if it is deemed
to be manipulating information with the aim of influencing a vote. The legislation was opposed by some, who saw it giving too great a power to the state to determine the boundaries of political speech. The legislation also requires tech platforms to publish the purchaser and price paid for sponsored content as a requirement to enhance transparency. There is a long history to this challenge. It builds upon a law from 1881 outlawing the dissemination of false news. Interestingly, Singapore passed similar legislation last year. The EU and NATO have enhanced their capabilities to identify and track misinformation. Some countries have banned Russian-language television broadcasters on the grounds that they have incited hate and spread disinformation. In 2015, the EU’s StratCom Task Force created a dedicated project to respond to disinformation from Russia, particularly that which targeted Ukraine.

Online extremism, national security, and sovereignty

The past decade has brought deep concerns over the impact of extremism online. Governments, law enforcement, and security agencies are increasingly pressed to do more in order to combat the spread and prevalence of extremist and hate speech. Many governments have responded by creating their own internet monitoring and surveillance regimes, seeking to grant themselves greater powers to control internet activity, and by asking or requiring internet companies to remove or block such material. As a result, there is a need to properly distinguish between extremism as a threat to individuals and extremism as a threat to the state, and when developing and implementing policies, to consider what we are trying to secure, for whom, and at what cost.

What makes this area especially complicated is that some uses of the internet for terrorist or extremist purposes are of course often indistinguishable from regular everyday use by average citizens, making it especially difficult to find optimal solutions. Private companies are defining ‘extremism’ and ‘violent extremism’ in an environment where no legal or international (UN-level) definitions have been agreed. This has implications for the safeguarding of human rights as state approaches sit at the intersection of national security, human rights law, internet jurisdiction, and digital democracy. French telecommunications company Orange shut down Google and Wikipedia for one morning in France because both had been added to the terror watch list – people trying to access the sites were redirected to a website of the Interior Ministry and had their IP addresses flagged (Nielson, 2016).

While much of the focus and response by Western states and tech companies has been countering Islamic extremism, white supremacist and far-right nationalism has experienced a 600% growth on Twitter since 2012, reinforcing the claim that internet policy responses to extremism have been fuelled by government interests and not always where the greatest threats to safety and security may lie. The Department of Homeland Security under Donald Trump eliminated grant funding to a number of organisations involved in countering far-right extremism that had been awarded funds under President Obama (Beinart, 2018). The US State Department has also threatened the existence of the Open Technology Fund, which has supported many circumvention tools and encryption technologies to journalists and activists operating under repressive regimes, including popular messaging app Signal, used worldwide by a range of users.

Responses to violent extremism demonstrate tensions over a state’s right to exercise its sovereignty. National security, like sovereignty, is a common rationale states invoke when seeking to exert and enhance regulatory control in a given area. And there is grounding for it
in human rights law at both the international and European levels, for example. However, national security is a broad and flexible catch-all reference often used as justification for state surveillance and communication regulation that undermines, implicitly and often explicitly, human rights. Turkey has a history of throttling access to social media in the name of national security when the effect is clearly to curb government critics.

Anti-extremism laws are used to enhance far-reaching state authority over online communication under the guise of counter terrorism. Four brief examples illustrate this: (i) In Russia, Andrei Bubeyev was sentenced to ten months in prison for re-posting to his VKontakte profile an image captioned “Crimea is Ukraine” and a video “that referred to Russia as a ‘fascist aggressor’” (The Moscow Times, 2017; and Ennis, 2016); (ii) Anti-terrorism laws in Jordan were amended to include prison sentences for “disturbing relations with a foreign state”; (iii) Charges were quickly brought against a supporter of the Muslim Brotherhood who posted comments criticising the United Arab Emirates (UAE), a major donor to Jordan; (iv) Likewise, both Bahrain and Saudi Arabia have levelled terrorism charges against journalists who have criticised the government; Bahrain stripped several journalists of their citizenship on charges related to terrorism.  

There are countless other examples of states blocking select platforms in-country: Iran has blocked Twitter for over five years; LinkedIn remains blocked in Russia for non-compliance with data localisation laws that Google and others have yet to comply with, but LinkedIn seems to be the test case there; Turkey has blocked YouTube and other platforms on several occasions over the past decade, including a year-long ban on Wikipedia in 2017 until Turkey’s high court ruled it unconstitutional. China has blocked popular messaging apps over claims they could be used by terrorists.

These restrictions reveal themselves more overtly in less open and authoritarian regimes but trends across the European Union demonstrate a similar range of governmental efforts to seize far-reaching powers with troubling implications for civil liberties and free expression online (Coyer, 2017). For example, just one month after the terror attacks at Charlie Hebdo, the French government issued a decree granting the state powers, without a court order, to block websites accused of promoting terrorism. Since then, state orders for content removal have doubled in France. In 2018, the French government also passed a law criminalising visits to “terrorist websites”. This legislation has been criticised for a seemingly automatic presumption of intent. At the same time, hate crimes targeting Muslims rose following the Charlie Hebdo attack and other terrorist incidents (Travis, 2015). Asylum seekers and migrants face an increase in violence and harassment across the EU, while anti-Semitic crimes are also on the rise.

In the UK, the 2016-18 Investigatory Powers Acts extended state surveillance over online communications by unprecedented measures, granting government expansive powers without judicial oversight in the name of national security. Despite past and ongoing legal challenges – from Privacy International, Liberty and other civil liberties groups – the Acts authorise bulk data collection and give law enforcement broad access to that data. Of course, privacy and security should not be viewed as mutually exclusive propositions. As former OSCE Representative on Freedom of the Media and now Council of Europe Commissioner for Human Rights, Dunja Mijatović (OSCE, 2016) argues, “Free expression and new technologies should be looked upon as tools to counter terrorism and not as a restraint in the fight against it”.

---

8 See Courtney Radsch’s (2016) report for further discussion of such events.
Indicative of the uneasy tension around platform power, states are relying heavily on internet companies to do this work for them. As a result, private companies are defining what is terrorist and extremist content and are making these decisions largely without common international definitions, judicial oversight, real transparency, or sufficient input from civil society. Twitter has removed or suspended hundreds of thousands of accounts for violations related to the promotion of terrorism since mid-2015, while Facebook announced it will rely more on AI to identify extremist content. Despite more recent disclosures, little is known of social media companies’ actual internal policies and processes of content moderation and removal. Tools, platforms, and technologies used by extremists or terrorist organisations can be the same as those used by pro-democracy movements, non-governmental organisations, journalists, and vulnerable social groups.

The companies also have an inconsistent track record of decision-making around extremism. In 2017, YouTube removed hundreds of videos related to the Syrian war, but caught up in the sweep was content that provided some of the only independent coverage of the region and footage that could be used to document human rights violations, or even war crimes, by ISIS and other actors. Facebook users reporting on, or documenting, what the UN has termed a “textbook case of ethnic cleansing” of the Muslim-minority Rohingya population in Myanmar were removed (Cumming-Bruce, 2018). On the other side, a Reuters investigation also found rampant examples of posts attacking the Rohingya and other Muslims in Myanmar on Facebook in local languages. Researchers and activists warned Facebook this content contributed to acts of genocide against the Rohingya. Moreover, its failure to hire content moderators who spoke the language amidst warnings of the harm the content was creating exacerbated this situation.

What happens when the decision over content takes place at the infrastructure level? How does this impact digital sovereignty? Cloudflare is a content delivery network that provides technical support to help websites load quickly and protect them against things like distributed denial-of-service (DDoS) attacks designed to knock websites offline. Cloudflare is not a household company, but it provides critical backend support for websites to be able to function. The company is significant, with over six million websites using its products, and handling around 10% of total internet requests. The company has a policy against censorship and has in the past been criticised for allowing its services to be used by terrorists, hackers, and scammers. But it has also protected pro-democracy websites in Hong Kong under attacks presumed to be from the Chinese government. However, following the 2018 ‘alt-right’-led march in Charlottesville, North Carolina, Cloudflare’s CEO Matthew Prince decided to remove white supremacist website The Daily Stormer from its services. Google soon followed suit. While standing by his decision, Prince reflected on his own actions, noting a failure on the company’s own behalf to not manage censorship decisions with consistency and objectivity, and arguing that no one individual should have the power that he himself had just exercised. Whether or not the company was correct in its actions is moot. But it raises questions about who has the right to determine access to the internet, with attendant implications for digital sovereignty.

Notably, in an era of nationalism, we seem to be witnessing a sea change in public attitude against inaction by social media platforms to address hate speech online, and especially against Facebook for its unwillingness to take action against such content from heads of state in violation of its own terms of service. Facebook has in fact faced the wrath of a number of major advertisers – who have elected to boycott the company for a period of time in response to its decision to leave up hateful content from President Trump. It’s estimated the company will lose its top 100 advertisers, costing Facebook $1billion each month, yet that’s less than 5% of
overall revenue. So, while this boycott certainly exposes vulnerability to public sentiment, Facebook’s market valuation, at the time of writing at least, appears only modestly impacted.

Spring 2020 saw Twitter make the unprecedented move to push back on Trump’s long running history of disinformation by adding a fact check to a tweet with false information about electoral voting (Smith, 2020). The same week Twitter blocked a tweet of his stating “when the looting starts the shooting starts”, a phrase with a long history tied to calls for state sponsored violence. He is not the first head of state to face content moderation. Bolsonaro and Venezuelan President Maduro have had content blocked for violating community standard rules against Covid-19-related misinformation that could lead to physical harm. However, Trump responded with an Executive Order to strip internet companies of their legal protection from liability for content users post on their sites. The order is likely unenforceable, but while claiming to protect free speech, it is actually intended to do what all authoritarian regimes attempt to do: repress and sidelines media institutions.

Zeynep Tufekci (2020) points out the Order was also intended to send a message to Facebook, which has benefitted heavily from the Trump campaign’s advertising expenditure on the platform in both raw dollars and in the way the campaign has maximised usage of Facebook’s algorithmic tools. Tufekci reminds us that internal research from Facebook, circa 2016, found that 64% of joins to extremist groups follow from the company’s own recommendation tools, which feed users more and more extreme versions of content they engage with.

Meanwhile, white supremacist groups are building their own social network platforms such as Gab, in an attempt to create what we might call their own ‘sovereign digital space’ within a digital ecosystem increasingly intolerant of hate speech and extremism. Gab continues to gain popularity and describes itself as a platform for free expression. Other far-right extremists in the US and Germany have migrated to Russia’s Facebook-like platform VKontakte, which has proven to be far more permissive of hate speech, despite its disallowance in the platform’s terms of service.

Not content with only securing their own platforms, white supremacist groups have also migrated from mainstream Reddit channels to subaltern channels like 8chan and 4chan. Cloudflare recently took the decision to kick 8Chan off its services as well. White supremacist organisations have also created their own online payment and crowdsourcing platforms after GoFundMe, one of the largest crowdfunding sites, shut down several campaigns to raise money for the Nazi sympathiser who killed the woman in Charlottesville. After Patreon, another payment processor, cancelled the accounts for some ‘alt-right’ figures, new crowdfunding sites like Counter Fund and Hatreon emerged, marketing themselves as companies that do not police speech. It’s a telling example of the far-right’s efforts to redefine the narrative of ‘free speech’ when what they really mean is ‘an unmoderated space for hate speech’.
Content moderation and platform power

A handful of private companies control social media. This ever-increasing concentration of power over society’s communicative spaces and access to information is indicative of broader concerns over the privatisation of the internet and the public sphere itself.

Every minute, over one billion users upload approximately 400 hours of video to YouTube, amounting in total to almost 600,000 hours every day. Every hour, 21 million tweets are generated by Twitter users, as are 146 million likes by users of Instagram. Facebook, on the other hand, has 1.37 billion daily users and 2.07 billion monthly users.

As problematic as a lot of laws are, the transfer of speech regulation from states to private actors raises serious questions about the future of free expression and human rights online and in particular the ability of states to act as dispassionate regulators. The UN’s David Kaye argues we must put individual and democratic rights at the centre of state regulation and corporate content moderation: “This is not merely an industry problem, it’s a democracy problem” (2018). He goes further to argue, “While there may appear to be a benign quality to this governance… the companies cannot be expected to be public-interest minded governors and adjudicators of speech over the long term” (Kaye, 2018).

Platforms are determining the boundaries of speech with insufficient accountability or transparency about their policies and their implementation. Because internet services are
almost exclusively private industries, the terms and conditions of online services can have a greater impact on the regulation of speech than state-sanctioned national laws; content can be removed and/or accounts deactivated without judicial process or other formal state-driven checks and balances.

We are, in effect, entering a de facto co-regulatory set of arrangements for content management between private companies and states; this arrangement lacks sufficient transparency and often results in speech restrictions that go beyond state mandates. Terms of Service Agreements take on the weight of law and leave internet users with little consumer power; the public cannot negotiate the terms under which they use the tools and platforms, and user-based flagging systems create challenges over self-governance and contribute to inconsistencies with content removal decision-making (for discussion see Coyer and Wanstreet, 2015).

Users flag over one million pieces of content every day and over one hundred million every month. Flagging itself is a means of distributing the labour costs, as well as a means of self-governance, giving a layer of individual sovereignty to users over their environment. Crawford and Gillespie (2014) argue that as a method of governance, flags are both a practical solution, a way of mechanising a daunting task, and a rhetorical justification for content removal. Social media platforms, as they describe them, rely on users in three interconnected but distinctive ways: as content producers and producers of the core assets of the companies; as producers of behaviours and actions that are analysed and repackaged as the source of advertising revenue and company profit; and as content moderators through the filing of complaints, thus shaping the norms that come to define the brand. Flagging is not just a technical feature. It speaks to a very complicated interaction among companies and users, humans and algorithms, and the social, moral, and political norms and regulatory structures of the online arena that they constitute.

Content moderation policies remain one of the most closely guarded secrets among social media companies who want to guard proprietary tech property and retain cover from liability. The moderators of these platforms – perched uneasily at the intersection of corporate profits, social responsibility, and human rights – have a powerful impact on free speech, government dissent, the shaping of social norms, user safety, and the meaning of privacy.

Facebook accounts for almost half the traffic to major news websites, so these human decisions about the context and newsworthiness of content have an unprecedented impact on determining who can be heard and how knowledge is shared. The limits of this system and reliance on human moderators came to the fore in the early days of the Covid-19 pandemic, when automated content-moderation algorithms inadvertently blocked users from posting legitimate news articles about the coronavirus and there were no human moderators on hand to quickly rectify the situation.

**The consequences of platform power**

The practice of content moderation is itself complicated, highly subjective, and non-transparent. It raises fundamental concerns around freedom of expression and human rights and marks a significant shift in the transition of speech regulation to the private sector. Automation and artificial intelligence are increasingly being used and experimented with to block or remove extremist content and users. But humans also perform a significant
amount of content review and remain at the centre of the decisions, policy, and programming that determine the parameters of artificial intelligence.

More evidence suggests a breadth of challenges for digital sovereignty with an increasingly automated flow of information, reinforced by existing individual positions and interests. This also suggests the coming months and years might well define the struggles over platform power, fuelled by concerns over the corrosive nature of extremism and disinformation, especially as the two are so intertwined in the tweets of current strongman-nationalist political leaders. Social media companies can no longer pretend their laissez-faire attitude towards content is sustainable. We must be ever mindful of the consequences of platform power.
4. Sovereignty and competing visions of the internet

The pressure to monetise data is fierce. Facebook did not grow into a $600 billion company by protecting the rights of its users. Behind debates on the impact of extreme datafication, privacy, security, and trust, are challenges to sovereignty that will define our global future beyond the internet.

Three core cross-cutting issues have yet to be resolved: (i) The rights and roles of the state versus the rights of individuals; (ii) The rights and roles of the digital private sector as the provider of tools enabling states to erode individual liberty and autonomy; (iii) The role of the private sector in undermining individual privacy. Far from a global consensus, attitudes towards data – and responses to datafication – seem to be competing, indeed bifurcating, across regions of the world to give us three emerging internet ecologies:

(i) The Chinese model of tight central controls and censorship within its borders. This model is also to be found in other authoritarian countries but not to the same extent.
(ii) The US corporatist model privileging private-sector sovereignty and data monetisation;
(iii) The emerging European model of state intervention. This attempts to hold corporate power to account, mirroring the public-interest model of broadcasting. In 2016, the EU passed the world’s most comprehensive data protection laws, the GDPR.

It is not inevitable that the US is going to be the strongest of these three ecologies. What distinguishes these competing visions of the internet is, at their core, the role of sovereignty and whose sovereignty is being threatened or enhanced. Is it traditional sovereignty – meaning autonomous control – of the state that is at stake? Is it the independence of action of the new private-sector digital giants that Zuckerberg has compared to states? Or is it what we might call the individual sovereignty of the increasingly marginalised citizen? In the EU, internet users can request certain data about them be delinked online under the right to be forgotten. From within each of these perspectives, as the New York Times (2018) has argued, different imperatives, interests, rules, and regulatory regimes are rubbing against each other. We need to fundamentally rethink our understanding of what it means to be a digital citizen amidst the ever-increasing ways data is used to monitor, profile, and organise us (Hintz, Dencik, and Wahl-Jorgensen, 2019).

This can especially be seen with regards to data capture, retention, and monetisation, but also with the physical location of data and data storage. We tend to think of the Cloud as a vague untethered space, but every piece of data, every digital action and transaction, is in some way transmitted and stored in physical data centres located in different countries around the globe. This infrastructure is largely privately owned by a small group of powerful providers operating in the absence of joined up international cooperation, leading us, seemingly inexorably, towards a fragmented internet.

This leads us to the obvious empirical questions: What parts of the internet will be bordered and what will remain global? What are the implications of this for the free flow of information and our networked society? Does the world become more disconnected as a result? Which states, or more precisely, which kinds of states, will be strengthened by digitalisation? Answers to these questions remain works in progress.
5G and the US-China struggle: Decoupling on the new international frontier

The age of 5G is upon us. At the level of the great powers in the contemporary era, the US and China are creating two sharply defined technological and online systems, or as we have called them, ‘ecalogies’. This is part of a wider strategy on the part of both great powers to put distance between each other in a number of crucial economic and politico-strategic policy areas (Higgott, 2019). In keeping with the political-economic models of both states, the American model is still primarily private-sector driven with the FAANG group operating with minimum state intervention. China’s paradigm is state driven, with its major quasi-private actors such as Tencent and Huawei operating in close strategic harmony with – and sometimes direct instruction from – the ruling party, the Chinese Communist Party (CCP). But both systems envelop the national development of AI, big data, 5G, and instruments of cyber warfare within their wider national strategies.

Other major players – notably, but not only, India and Russia – are also increasingly interested in creating their own digital systems with the search for sovereign control as the primary driver. The EU is engaging in its own regulatory efforts to contain the global corporate internet actors. The EU has both Facebook and Google in court at the time of writing (June 2020). But will they succeed in their efforts to secure greater taxation and to make the tech giants accept greater responsibility for things such as content moderation? Amazon particularly is in the spotlight; facing pressure to pay its dues in Washington State where it is based. In fact, the city of Seattle just voted in a new tax on companies with the highest paid employees like Amazon, with money going towards economic relief and public services related to Covid-19. These issues, especially who taxes the tech giants – the home or source country or the host market or customer country – are hotly contested, especially across the Atlantic. OECD suggestions of tax ‘splitting’ are not playing well on either side of the ocean. In this transactional era, both sides see the decision as one that should be made by sovereign states and in the national interest. In June 2020, the US – insistent that Europe should not tax the monopoly profits of its tech companies – torpedoed the OECD’s efforts to reach a global consensus by withdrawing from the trans-Atlantic negotiation with the EU over a ‘global digital tax’ (Fleming, Brunsden, Giles, and Politi, 2020).

The 2020s will see further advances in the fields of artificial intelligence and quantum computing, which will have further implications for the core components of sovereign politics and power relations in the international economic and security systems. In this context, the struggle over 5G as the enabling technology of the future is at the core of US-China competition, with implications for the building of the Internet of Things, the development of autonomous vehicles, and improved cybersecurity. AI technology and the integrity of systems such as electric grids do, or will, all depend on 5G technology. Moreover, next generation WiFi systems need huge increases in bandwidth and their infrastructures will require 5G technology.

The political and international relations implications of this contest are evident. Politically, digitalisation has become a major factor in the ability of states to maintain and enhance what they believe to be their all-important sovereign autonomy at home and to compete successfully in the international system. The importance of the contest over Huawei reflects competing views over the protection of sovereignty. It is also a battle between companies and government. This is the case in the US and indeed, albeit to a lesser extent, China. US technology companies, especially telecom carriers and chipmakers such as AT&T and Verizon, are resisting pressure from the Trump administration that they cease resourcing components from ‘foreign adversary companies’. Effectively, shutting Huawei out of the US market completely will do great
damage to the economic wellbeing of these companies. Moreover, to do so, the companies argue, falls foul of anti-trust and competition law, laying them open to legal suits.

It is clear that in the contest between the US and China, pressure for allies to align with the United States under conditions of an emerging new bipolarity will be strong – especially vis-à-vis Chinese giants in 5G technology such as Huawei. US strategy in the digital domain, and in technology more generally, is to decouple and to pressure non-committed allies to choose; or less prosaically, fall into line. The strategy threatens wider relationships between the US and other states who are deemed to be allies but who do not tow the US line on the role of Huawei within their countries. Contrast the response of Australia, Canada, and New Zealand, as three of the ‘Five Eyes’ security community who have lined up with US in excluding Huawei from their digital industries and systems, with that of the UK (the fifth Five Eyes partner), which, in the face of immense pressure, initially at least, proposed that Huawei should assist in the development of UK infrastructure given the UK was comfortable it can safeguard its cybersecurity system from Huawei.

Along with France and Germany, the UK prior to Covid-19 was resisting US exhortations for a total ban on Huawei. But the issue has led to considerable tension between the US and its NATO allies and it has especially strained the US-UK bilateral relationship with US suggestions, in reality threats, that it might have negative externalities for wider discussions over issues such as a free trade agreement. Since Covid-19, UK resistance to US pressure has shown signs of weakening with the government announcing a review into Huawei activity in the UK. At the time of completing this manuscript, the UK had signalled a shift in its stance to most likely limit Huawei’s role in building out Britain’s 5G network, a move that is a big win for the US, amid concerns the Chinese technology leaves countries vulnerable to potential espionage. It is also significant that such a move follows on the heels of Hong Kong’s devastating new ‘Security Law’ and ensuing crackdowns on political freedoms and erasure of freedom of speech.

Unsurprisingly, US and European hostility towards Huawei has seen China turn to strengthen its position in other emerging markets and especially in Russia, which knows it cannot produce a quality 5G product on its own. Thus, China is almost certain to become the major 5G provider to Russia, especially given its lower cost when contrasted with potential European providers. Here too, Covid-19 is important given the questions around digital tracking as a challenging element in the containment of the spread of the virus.

The issue of Huawei also poses an interesting, somewhat paradoxical, discussion over the complex and at times contradictory understandings of the concept of sovereignty. In the UK, Tory MP Tom Tugendhat, chair of the foreign affairs committee in the last Parliament, argued that “… allowing the Huawei deal would call our sovereignty into question”. He rejected the idea that the Chinese should win the contract merely because they offered the cheapest option. Tugendhat went on to say that the choice of a 5G provider “… should not be economic but about sovereignty. Only nations that can protect their data will be sovereign.” With no sense of the contradictory nature of his comment, nor any appreciation of the complexity we have described in this report, did he appear to understand that the ability to make autonomous policy decisions free of bullying and threats from allies – in this case the US – can also be considered an essential element of state sovereignty.
The geopolitical ‘pecking order’

Is this forced alignment with US policy going to be the inevitable outcome for Europe and maybe even Japan? Will the struggle to prevent national fragmentation of decision-making within Europe in the face of these and other pressures prevail? If so, to what extent can it be led by the public interest and regulatory responses of European and other like-minded states in the face of growing pressure from China, and increasingly the US, to bifurcate the digital world? The answers to these questions – yet to be fully determined – cast massive domestic and international policy shadows over both near and long-term futures.

More generally, AI, to the extent that it is contributing to disruption of the formerly established world order, intervenes directly into any discussion of sovereignty in international relations. Is digitalisation, as some would argue, challenging the international ‘pecking order’ of sovereign states in a more complex order that is no longer defined by traditional indicators of sovereignty such as GDP, military capability, or geography alone? In the future, countries may be judged and assigned standing by their capacity to take part in a global system shaped by artificial intelligence. Change is coming about in several ways.

Firstly, if trends continue – although there are no guarantees of this – China will later if not sooner become the dominant power in AI development. For sure, US investment in AI still outstrips China’s in absolute terms and particularly in terms of private investment: $66.5 billion versus $14.5 billion in 2019. But this investment is largely in research to support the giant tech companies in their search for greater economic return. A more important indicator of state capability, and by extension state power, is public investment. China’s public investment in AI, at $22.5 billion in 2019, far outstripped that of the US, at $2.05 billion. Indeed, the US was exceeded by Germany, at $3.31 billion, and matched by South Korea, at $1.95 billion. Estimates, ceteris paribus, suggest China could overtake the US by 2030.

China’s ambitions would appear to extend beyond size and simply securing its own independent digital regime inside its Great Firewall. Rather, it is keen to rewrite the wider rules of internet governance and the way the internet functions and is regulated beyond its borders in order to put control of the internet firmly in the hands of governments, as opposed to the current regime which, absent of any central oversight, reflects a more laissez-faire approach in which the internet is largely owned and regulated by private, principally US, companies.

Instead, China, tired of its longstanding exclusion from the regulatory oversight process, has pitched to the UN – at a meeting of the International Telecommunication Union-ITU – the idea of a new Internet Protocol. This new IP would have a top-down design and would be built by China to reflect the interests of governments, especially those emerging powers – read China – that were left out of the first wave in the last quarter of the 20th century.

Led by Huawei and dressed up as the necessary technical requirements to meet the demands of a modern digital world, the creation of new infrastructure and standards would more closely reflect China’s “totalitarian impulse”, rather than that of a largely American private-sector digital community. This is what the Financial Times calls the core of China’s “digital foreign policy” (see Murgia and Gross, 2020; and de Nardis, 2014).

Supported by Russia, Iran, and Saudi Arabia, China’s proposals, unsurprisingly, go beyond the desires of the US and Europe, including the UK, who wish for a (quasi)-democratic alternative, but an alternative that nevertheless sees more power going to their intelligence agencies to secure
greater oversight of personal data. If China were to prevail, state-owned internet service providers would not only be able to control and monitor activity on the net but also control access to it. Moreover, other states could choose to follow China’s lead and use its technology, as indeed an increasing number of states in Africa are doing. A further variable that should of course not be ignored is price. Chinese technology is invariably cheaper to purchase than US technology.

Rather than a world wide web, we could be moving towards a world in which states would have what China describes as “cyber sovereignty” or Russia, following recent legislation, calls the “sovereign internet” (BBC News, 2019, ‘Russian internet’). Under China’s understanding of cyber sovereignty, control will be built into the infrastructure of the internet, thus removing any notion of a neutral internet infrastructure. The internet, in the words of the *Financial Times*, ceases to be “an agnostic postman” (Gross and Murgia, 2020).

Secondly, while not on a scale of the big two traditional big players, the UK, Canada, France, Germany, and at a smaller level Australia – all with their world class higher educational research facilities – have grown and continue to grow expertise and capability in AI and digitalisation. Astute and strategic policy development in the field of AI offers the opportunity for smaller states to play a greater, arguably sovereignty-enhancing, role in international relations. Other examples here are Israel, Ireland, Finland, and Singapore; although Singapore and Israel also face criticism over their advanced surveillance states. What these states might lack in scale they make up for with their research excellence – judged as a metric of citation of research papers by host country – and with the intensity of their upscaling of AI capabilities through a higher proportion of their populations being engaged in the IT industries. The US still publishes more top-flight research papers in AI than the next ten states, including China, combined, but the gap is closing.

Other states, although coming off very small bases, are growing their AI capability in an exponential fashion. In the long term, those countries making the right strategic decisions – funding and equipping institutions, business, and the citizenry generally with the necessary training in, and tools for, AI and digital technology development – are the ones that will enhance their positions in the global order.

Critical ethical concerns

Amidst the race for industry dominance and economic primacy, we must not lose sight of the very real and very critical ethical concerns in every aspect of AI development and deployment. There are currently many AI principles but no common standards. Moreover, there is a contest over who defines norms, including cultural norms. For example, the OECD AI ethics guidelines don’t talk about culture, but rather about humans in a normative way. Artificial Intelligence isn’t just coded, it’s trained through human behaviours that reflect existing biases, power imbalances, and sovereignties. Systems built by companies and states lacking equality or equity will mean systems that don’t reflect the public interest. In our rush to crown a ‘winner’ in the AI race, we risk missing a tremendous and perhaps unprecedented opportunity to build something truly global (Field and Nagy, 2020).

---

9 See Tortoise Media (2019).
10 Data for the preceding discussion draws on Hollowood and Clarke (2019).
5. Digitalisation: The trade-off between decentralisation and political control

As we have noted, the growth of digitalisation was meant, in theory at least, to enhance democratic engagement by greater openness, transparency, and individual empowerment. These technologies, it was argued, would enhance peaceful political protest by reducing barriers to citizen communication and political coordination. Starting with the invention of writing and then the printing press, new technologies and communication tools have always been harnessed to enhance social justice in myriad ways. In fact, activists are often ahead of the curve when it comes to developing and utilising tools for collective action and collaborative models.

While social media technologies were instrumental in unseating authoritarian leaders in Libya, Tunisia, and Egypt, what we saw was a cat and mouse game between states, publics, and tech companies. Even in the most restrictive regimes, people have found, and continue to find, clever ways to bypass state strictures, even virtually climbing the Great Firewall in China through the use of Virtually Private Networks (VPNs) or other circumvention technologies.

But to overly focus on these activities, in some ways exceptions, obscures the power of states, especially states such as China, with its ability to exert sovereignty over the digital world through increasingly aggressive regulations and technical capacities, including new crackdowns on VPNs. So these bypasses and circumventions remain in constant tension with the surveillance capabilities of digital technology that enable greater monitoring of citizens, especially in authoritarian states, and even democratic states tempted by the controlling fix that the technology offers. And there is an entire industry of controversial private companies providing tools that enable, and in some cases perform, state surveillance capabilities. So, does this mean the end of the global internet as we know it?

Indeed, in all states the temptation to observe one’s political opponents when the opportunity presents itself is proving very difficult, even for the most democratic of governments, to resist. This can be done in an easy, seemingly non-intrusive and fairly cheap, manner. Digital technology has made it much easier for regimes wishing to control dissent to identify their opposition. In this vein, we must also consider that internet shutdowns, or intentional disruption of internet-based communication and services, rendering them inaccessible for a specific population or location, are also a growing concern. While there is no singular ‘kill switch’ for the internet globally, many governments have routinely or occasionally abused their power to cut off internet access as a disruptive measure. In Ethiopia, where all the internet service providers are state run, the power to shut off the internet lies squarely in the hands of the state, which has abused this power with frequency. Even amidst the Covid-19 pandemic, the Indian government shut off internet access in two specific regions.

Iran has one of the world’s most closed internet regimes. Zimbabwe’s government shut down the internet for a time following anti-government protests. One of the longest shutdowns was India’s cutting off of parts of Kashmir under its control. China’s digital firewall affords it the ability to cut off the country’s internet from the rest of the world, but China doesn’t often deploy such a blunt instrument. Rather, its censorial regime is highly sophisticated and

achieves its intended purpose by filtering at the content level or blocking groups and individuals. Technical developments in data processing, spy malware, automated text analysis, filtering and blocking, and facial recognition have developed to high levels of sophistication but they are certainly not new. The US National Security Agency bugged the Germany Chancellery for many years, including Angela Merkel, her closest advisors and the staff of her predecessors. According to Wikileaks, they tapped up to 125 telephones of senior officers (Reuters, 2015). Russia too has taken advantage of Chinese firewall technology to curtail access to the internet from beyond its borders when it suits.

Does this ability to control, or at least keep tabs on, civilian populations and political opponents count as the enhancement of state sovereignty? We would argue no. We would argue that there is a difference between endeavours to preserve the sovereignty of the state and the enhancement of regime maintenance and the deployment of systems of control – and this is irrespective of the nature of the regime. This is a judgment applicable to authoritarian and democratic regimes alike. As noted in Foreign Affairs, citizen surveillance in the digital era is far less labour intensive, more inclusive, and easier to organise than it was in Cold War days in the former Soviet bloc (Kendall-Taylor et al., 2020). But it is no less problematic; rather more so, owing to the increased facilitation of the wholesale nature of invasiveness made possible by digitalisation.

Citizens and the loss of privacy

Citizens seem to be accommodating to their loss of privacy more than they ever did in the Cold War era. As Winner noted (1980), people are often willing to dramatically change how they live to adapt to the latest technological innovation but remain resistant to political or governmental pressures to do the same. In this regard, there is a correlation between generational change, technology, and the new frontiers of political power. Current generations raised on social media, knowledgeable of and comfortable with the emerging digital future, seem less concerned about digital intrusion into their lives and the ability of technology to influence their politics. Presumably, this is in part due to the dual use nature of the technology on which citizens come increasingly to rely to deliver necessary public goods – ranging from social credit systems and education through to bus passes.

However, increasing evidence demonstrates how these same technologies can foster inequality, through data mining, algorithmic policing, and predictive risk models that can discriminate against and harm vulnerable people (see Eubanks, 2018). Companies like Palantir develop discriminatory monitoring tools that are extensively used by law enforcement agencies such as the US Immigration and Customs Enforcement (ICE). US drug companies are already buying healthcare data from NHS patients; Amazon has been given free access to NHS data (Woollacott, 2019).

Further, digitalisation has effectively become not only the starting point for economic and political influence on social media; it is also now the distribution vehicle for rewards as much as punishment. AI-powered algorithms will see micro-targeting become increasingly sophisticated and ‘deepfakes’ – forms of synthetic media in which an existing image or video is replaced with someone else’s likeness, such as making someone appear to say something they did not – virtually impossible to detect.\(^{12}\)

\(^{12}\) See data and research from NGO Witness for more on deep fakes.
By extension, these innovations help minimise potential opposition to the activities of government. Recent data demonstrates how technological advancement of the internet overall has been a major benefit to authoritarian regimes and that ‘digital repression’ has enhanced their durability. Indeed, the data also suggests that a growth in the wave of authoritarian regimes is fostered by digitalisation at the same time as it increases the risk of democratic backsliding (Kendal-Taylor, Frantz, and Wright, 2020, pp. 23-28). We are in an era when digital technologies are empowering those states with the desire and proclivities to use them.

According to the UN Declaration on Human Rights, privacy is a human right. So, what kinds of privacy protections can we, and should we, expect if the internet continues to develop in this way? The record to date exhibits considerable ambiguity.

The large tech companies usually attempt to accommodate the interests of powerful states. Companies comply with state jurisdiction on many levels. Sometimes this means handing over private data on users at the behest of government requests. In some cases, this has resulted in the imprisonment of journalists and activists such as the case of Chinese journalist Shi Tao. In Pakistan, Google created a localised version of YouTube in order to convince the government to lift its three-year ban on the service. And when Google first entered the Chinese market in 2006, it infamously launched a localised version of its search services to comply with Chinese censorship rules. Many perceived this to be an attack on citizen informational privacy by complying with the ‘walled garden’ rules and working against the borderless free flow of information promised by a global internet. Google later pulled out of China in 2010 following discovery that Gmail accounts of Chinese human rights activists had been hacked. In 2018, Google was working on a project called Dragonfly – to be a new search engine in compliance with Chinese censorship – only to later announce, following a public outcry, the project’s cancellation. Since then, CCP-approved search engine Baidu has garnered the lion’s share of the Chinese market.

Google, Facebook, and Twitter all publish detailed annual transparency reports, highlighting the number and type of requests for content and account removal they receive from governments. But the level of transparency varies across companies. Requests received from the Internet Referral Unit of Europol pose a range of problems, not least the derivation of content-monitoring in non-transparent ways from law enforcement, but also because Europol often use a company’s terms of service to make its content removal requests, even though it is acting on behalf of states. The Ranking Digital Rights project publishes a highly researched assessment of the publicly available human rights policies of the major internet and mobile companies.

China continues to embed itself more deeply into the economic future of Africa. At the same time, the continent’s digital future has become equally connected to China. Chinese tech companies are now the most significant players in Africa’s fast-growing digital markets. Both state and private Chinese companies are working with telecom operators across the African continent to build powerful new data centres to accommodate the rapid growth of internet traffic, building out new fibre optic networks, and selling vast quantities of affordable smart phones enabling millions of people to get online.

Offsetting these undoubted benefits for Africa are a host of troubling human rights implications surrounding the export of the Chinese model of internet censorship and control. Indeed, Western news coverage is keen to detail how Huawei and ZTE are aiding some African governments in the surveillance of their citizens, blocking websites and introducing other
internet controls. Chinese tech company Cloudwalk announced the sale of artificial intelligence-powered facial recognition systems to the Zimbabwean government and Huawei and ZTE are also reported to have sold sophisticated digital surveillance tools to Ethiopia’s state-owned and sole telecommunications provider EthioTelecom. This technology, rights advocates argue, is unsurprisingly used to watch opposition politicians and journalists.

But it would be unwise to focus only on China in this area. The Ethiopian government, for example, appears to also be using surveillance technology FinFisher from the UK and Germany and Italy’s Hacking Team Remote Control System. Such tools allow security and intelligence agencies the ability to access not only information and activity from the computers of those targeted, but also to log keystrokes and passwords, turn on microphones and webcams, and weaponise a computer against its user. The US argues that African governments running Chinese digital systems open the possibility for Beijing to spy on them. But US and European warnings to Africa fall on stony ground as they come without an investment alternative, while Chinese investments have significantly improved mobile and internet communication on the continent.

Increasing state control over citizens needs to be contrasted with what we might call the diminished role of the sovereign state over increasingly important and unregulated sectors of socio-economic life. Without overstating the case to date, we are seeing significant growth in digital contracting, encrypted messaging apps, and anonymous web browsers like Tor. These innovations and other forms of anonymous digital interaction and cryptocurrencies, such as Bitcoin, are giving rise to what some call ‘techno freedom’ or, at its extremes, what Bartlett (2018) calls “crypto anarchy”.

Encryption might allow people to communicate and act online outside the reach of government – which is appropriate in open societies – and without which there would be no online banking, e-commerce, or any secure online operations. Bitcoin’s major interest for this report is not its utility and how it operates but its uniqueness as a currency. It operates with no state control of supply or value and no brokers, such as banks, mediating the relationship between users. Moreover, through the distributed software storage ledger Blockchain, it creates a huge tamper-proof, decentralised, database that via encryption, actually enhances individual freedom from government. Facebook’s cryptocurrency experiment with Libra has yet to launch but has already been met with concern. Libra is similar to Bitcoin in that it exists only in digital form with transactions recorded on Blockchain. But as a currency, it will be backed by real assets. Given Facebook’s poor track record with user data and privacy, it should come as no surprise that there is a great deal of concern surrounding the company’s entry into cryptocurrency and the kind of consolidation of power and digital market distortion that may result.

Digitalisation and pandemic: A new pairing

The global coronavirus crisis is reinforcing the growing centrality of digitalisation’s influences over contemporary society and politics. Many of the arguments advanced in the preceding chapters of this report on the relationship between sovereignty and digitalisation seem to coalesce in an era of pandemic. Just as digitalisation is affecting our socio-political and economic life both domestically and internationally, the impact of the pandemic appears to be exacerbating this change at the same time as it highlights the contradictions in our understanding of sovereignty.

In short, in the wake of Covid-19 the world will in all likelihood become less prosperous; less open; less free; and increasingly geopolitical and nationalist, as states turn in on themselves, seizing the opportunity to reassert national sovereignty and autonomy (a common refrain among realist scholars; see for example Kaplan, 2020 and Walt, 2020). At its broadest, the core challenges that come with digitalisation are being amplified by the current pandemic.

In our efforts to defeat Covid-19, digital technologies are being called into action as more and more people work from home online. Since the outbreak of the pandemic, government expectations that privilege a compliance culture – whether it is closer monitoring of the population or sanctions – have grown exponentially. Digital tools are an invaluable part of disaster management, but fears over the consolidation of the ‘surveillance state’ in the hands of governments and private companies are not unfounded. Unchecked, technological curatives can bring their own new diseases to an already unhealthy body politic.

Further, the crisis is exacerbating existing social and economic inequalities. Social distancing measures require greater reliance on digital tools that can only be realised with reliable high-speed internet access, bringing to the fore the need for universal and affordable broadband access. The economic and health impacts are being felt the hardest by those who cannot work from home, or work in industries where it’s not possible, or are already struggling with under or unemployment. In the US, Covid-19 has disproportionately affected people of colour. Online learning and home schooling exacerbate the already disproportionate demands on women. Higher education may not look or feel the same in the not so distant future.

Covid-19 raises major questions for digitalisation. Are we prepared for the kind of systemic shift to an online world post-Covid-19? Are we prepared to sacrifice personal privacy in order to control the pandemic? And if so, what kind of world does that look like? Under what conditions should the state be allowed to use surveillance tools? How can innovative public health tools be developed with adequate privacy and public protection safeguards in place? Can they be deployed without infringing on fundamental human rights? And how can we avoid hardwiring discrimination or harm into our reactive models? How can we mitigate the costs of granting states and companies unchecked powers that go well beyond the current state of emergency? In short, we must aspire to get the balance right between innovative and rights-respecting technologies that can help save lives on the one hand but also enhance the abilities for surveillance and privacy-invasion by states and private actors and contribute to the spread of misinformation and disinformation on the other.
Covid-19, did not of course create these challenges alone. But it has exposed the challenges around digitalisation and sovereignty. Will this pandemic be the tipping point that paves the way for a new era of dramatic political and social change? Even our physical worlds of work, education, friendship, and community increasingly take place online in ways that could well become the ‘new normal’. Digital fatigue and the social fractioning that comes from social and physical distancing must also be addressed. Covid-19 not only brings to the fore the full range of existing tensions globally but it is very much reinforcing paradigmatic debates over the future of our digital lives and the power of both the state and corporations in shaping them.

**Emergency powers tend to outlive their emergencies**

Governments around the world have made seeking new and extraordinary powers in the name of containing the virus one of their first responses to Covid-19. We also see some states using the pandemic as an excuse to suspend many freedoms and attack the press in the name of curbing misinformation. Iran took the decision to ban distribution of any print newspapers, claiming they could spread the virus without evidence of such transmission. Thailand authorised prison terms of up to five years for reporting that “is untrue and may cause public fear”, while in the Philippines, Iran, Honduras, Azerbaijan, Singapore, and elsewhere journalists are being threatened with imprisonment for producing “false information”. In Brazil, ultimate pandemic denier President Bolsonaro is nevertheless using Covid-19 as cover for his attacks on independent media.

Restrictions in Egypt and Singapore have led to prosecutions targeting opposition politicians, journalists, and watchdog groups. In Turkey and Cambodia, people have been arrested for comments made in relation to Covid-19. A reporter with The Guardian was expelled from Egypt; foreign correspondents have also been expelled from China. Russia’s Supreme Court has ruled it illegal to publish ‘fake news’ discuss it in public with prison sentences of up to five years for spreading false information about Covid-19. In Hungary, the pandemic has provided Viktor Orbán with an opportunity to further expand his authority through an emergency bill granting him sweeping powers to rule by decree. Like Russia, Hungarian law also allows for prison terms of up to five years for ‘spreading falsehoods’ or impeding government efforts ‘to protect people’. The vagueness of language itself grants the state far-reaching powers; in at least two cases, police have arrested individuals in rural communities for Facebook posts of opinion critical of the government.

It is not unreasonable to assume that such responses to the pandemic have less to do with public health and safety than with political power and the expansion of state control; in effect, a doubling up of existing authoritarian trends from both liberal and ‘illiberal’ democracies alike. These measures also have to do with protecting the political reputations of those seeking to re-establish their authority and retake control of, what Nossel (2020) describes as “the devastating narrative of a pandemic that has fed on human failures of anticipation, preparation, and mobilization”.

The pandemic may well encourage regimes of surveillance and censorship to become further embedded and justified on the grounds of public health. Nossel warns of the risk of this battle becoming a “forever war” (Ibid). Sean McDonald (2020) reminds us that emergencies should not be “… a blank cheque for state or digital platform power”. Surveillance and diplomatic policies written in the midst of a pandemic, promulgated via “escalating protectionist
declarations” rather than deliberative policy and the widely informed consent of all stakeholders will inevitably be sub-optimal. Emergency situations result in the suspension of many a tried and trusted system of institutional review. This in turn makes it difficult to determine if the systems being proposed will actually solve the problems at hand or enhance harm and/or potential harms via their deployment. The genie won’t just go back into the proverbial bottle.

An ‘infodemic’

We are in what the World Health Organization (2020) has called a “massive ‘infodemic’”, arguing misinformation is as deadly as the actual disease. The day after President Trump suggested that ingesting household cleaners might kill the coronavirus, the New York Times felt the need to tweet in large font “Please do not eat disinfectant”. In similar vein, the US Federal Food and Drug Administration (FDA) cracked down on religious leaders peddling dangerous and ungrounded curatives to their brethren. A Washington State NGO filed suit against Fox News and the Murdoch family over their deceptive coverage of the pandemic, including claims the network violated the state’s Consumer Protection Act for disseminating false information that the virus was a hoax and posed no threat to public health.

The wilful spread of false and often contradictory information isn’t always about getting across a particular narrative, but rather the undermining of trust in fact and science. Gregory Asmolov (2018) describes it as “… a manifestation of the state’s disconnective power”, the purpose of which is not to shape people’s perception of reality but to dissolve horizontal ties among people.

Joan Donovan (2020) points to the paradox that confronts us: “the same technological infrastructure that perpetuates this infodemic is created by platform companies that profit off the unrelenting spread of this information.” In the US, African-Americans have been the explicit targets of misinformation. Similarly, the EU asserts that Russia has been using the pandemic to spread misinformation via ‘troll farms’ to promote a wide range of false claims (Ward, Polglase, Shukla, Mezzofiore, and Lister, 2020). Many memes circulating on social media have been documented as part of this disinformation campaign targeted at the US and Western European countries. Posts on Facebook and videos on TikTok advanced the bizarre claim that 5G was spreading the coronavirus. As a consequence, over 70 cell towers were set alight in the UK.

The overabundance of information makes it especially challenging for people to find trustworthy sources and reliable guidance, which in turn amplifies the problem. Disinformation spreads and flourishes at unprecedented speeds in environments of mass uncertainty, fuelling anxieties, racism, and xenophobia. Part of this problem is embedded in how we consume information online. It should come as no surprise that harmful information often overwhelms good information. Donovan (2020) argues the current pandemic reveals a failure to quarantine online scams, hoaxes and lies amid political battles. She argues that Covid-19 lays bare the dangers inherent in tech company reluctance to act. The spread of harmful disinformation should actually be seen as a feature intrinsic to the system rather than as ‘bugs’ within it. For example, ‘coronavirus’ and ‘Covid-19’ are such unique keywords that topics attached to these themes are easily exploited by scammers. Pair these words with ‘masks’, ‘loans’, ‘unemployment’, or ‘vaccine’, she points out, and it’s even easier.
Platform power during a pandemic

In the midst of social isolation and quarantines, social media has become more important than ever. Journalists relied on Chinese social media to gain a better idea of what was going on. Although several doctors in China were reprimanded by the Chinese government about their sharing of information on the rising crisis, their warnings nevertheless went viral and the volume of personal stories and reports circulating in China was strong enough to force the government to be more honest and open about the crisis. The outpouring of public support over the death of Dr Li Wenliang was strong enough to eventually overpower censors.

Platforms are demonstrating they are capable of taking strong action in both the prevention and promotion of content when they want to. Facebook, Google, LinkedIn, Microsoft, and Reddit announced combined measure to elevate ‘authoritative content’ from credible sources like the WHO and CDC. A channel on Reddit was one of the first informal places where two medical doctors shared reliable, scientific information as far back as January. The WHO has also partnered with Tencent and Generation Z favourite, social media site TikTok, to respond to misinformation online. Google pushed WHO content to the top of search queries and is working with Facebook to target specific populations and demographics with health ads and through the use of ‘social media influencers’ across Asia. WeChat is using human fact checkers to scrutinise rumours circulating online (Deng, 2019).

Numerous countries around the globe began rapidly using digital tools to track the movements of people becoming infected with the virus. Apps now also exist to enforce the social distancing of those with the virus. Uber sent Mexican authorities data on infected riders to trace their route and banned users who had ridden with that same driver. Russia is experimenting with digital passes and QR codes. In the US, officials are obtaining personal data location in bulk from online advertisers.

On the content removal side, Twitter has removed tweets from Presidents Nicolás Maduro of Venezuela and Bolsonaro of Brazil for spreading misinformation about Covid-19. While the Indian government has asked WhatsApp and Facebook to be aggressive in taking down ungrounded conspiracy theories around the virus, the response from police has been to carry out mass arrests, raising human rights concerns. Google has blocked the YouTube account of Kremlin-backed news outlet RIA Novosti, deleting tens of thousands of videos from the agency.

There are risks with any such measures. “Because the platforms offer next to nothing by way of notification and appeals processes with respect to content that is taken down, there is a risk that amid valiant efforts to curb falsehoods and deceit, a good deal of legitimate content will disappear” (Nossel 2020). Moreover, the capacity companies have demonstrated to block and remove content identified as ‘misinformation’ raises real fears that governments will later ask for similarly aggressive measures to be applied against content they find distasteful or will justify as against the national good or public order. Either way, we risk a dangerous choice over who we want to censor or control information: governments or companies.

---

13 China-based TikTok has been banned by branches of the US military, both Republican and Democratic parties, and other organisations and companies citing security concerns. India has also banned TikTok, citing its need to preserve ‘digital sovereignty’.
Finally, there is the challenge of automated algorithmic content removal. In the time of pandemic, stay-home measures mean that the platforms are without the usual numbers of human content moderators. In March 2020, Facebook’s algorithms mistakenly removed posts of credible reporting and information-sharing, including posts about how to make face masks and calls from healthcare workers for donations of protective gear. The move was in response to Facebook’s efforts to keep profiteers from benefiting from the pandemic but good content was caught in the automated crossfire.

**Digitalisation and health surveillance: Freer or less free?**

Covid-19 represents a watershed in the history of surveillance. It is normalising what Harari (2020) calls the transition from “over the skin” to “under the skin” surveillance. The dilemma is that while health surveillance – knowing peoples’ temperature, heartbeat, and other biometric data for example – can assist in the containment and mitigation of infectious viruses, it can also legitimate an extensive surveillance system with all the attendant implications for civil liberties and human rights. Harari captures it thus:

“If corporations and governments start harvesting our biometric data en masse, they can get to know us far better than we know ourselves, and they can then not just predict our feelings but also manipulate our feelings and sell us anything they want – be it a product or a politician” (Harari, 2020).

China has responded to the pandemic by creating new digital infrastructures to track the movements of massive numbers if people in ways tied to individual identification, in addition to the already invasive programme of social-credit scoring. Israel is using mobile phone location data to identify people who have come into close contact with others who have tested positive. South Korea has used additional digital records, including medical and pharmacy visits, credit card transactions, CCTV etc., to track where exposed people have been, then followed up with interviews of those carrying the virus and their acquaintances. South Korea also has a very high capacity for testing. Police in Moscow are using facial recognition cameras to catch people violating quarantine.

South Korea, Taiwan, and others use smartphone location data to enforce individual quarantines. Apps leveraging the already built-in data sensors in smartphones are being used in Singapore, Kenya, and Poland. MIT researchers have produced a similar but more privacy-protecting version. India, amidst large scale lockdowns and overwhelmed medical facilities, has seen state and local governments publishing individually identifiable medical data. While social stigma and other community tensions remain a concern, their Bluetooth-based tracing app collects sweeping amounts of data but it is unclear how it will be used, and the government has given little assurances about de-identification, data sharing, and storage protocols.

Having acquired such abilities, governments are loath to give them up. Initially temporary biometric surveillance systems can be kept ready for the next iteration of the pandemic. But, as Harari says, it need not be a choice between health and privacy. States, he argues, need to build trust regimes with their citizenry, not surveillance regimes. The Electronic Frontier Foundation argues it is up to states to demonstrate that any powers they take upon themselves should be science-based, effective, necessary, and proportionate as required by recognised and accepted international law (Schwartz and Crocker, 2020). But is that enough?
These kinds of tools require a significant amount of location and personal data. Location data, information on people’s movements and physical location drawn from GPS and mobile towers, can be useful to inform decisions about the effectiveness of stay-home orders and social distancing, or to visualise travel patterns. It is important this kind of data be aggregated or de-identified. But even this has its limits. It can only account for those who have a smartphone and carry it with them at all times. Even in the US, that figure is only 80%; in India it’s less than one-third of the population.

Moreover, applying the same method to track infectious diseases as is used to track criminals and terrorists is fundamentally flawed at the technical level, let alone at the level of ethics. Cell phones aren’t capable of tracking that close, and while GPS can provide finer precision, it cannot recognise person-to-person proximity. In the meantime, governments are demanding new dragnet location surveillance powers to fight Covid-19. From the use of cell-phone tower data to track the movement of people, the pushing of new apps that aim to predict user exposure to the virus, to facial recognition and thermal imaging in public places, to law enforcement access to otherwise private public health data. Citizens lives are becoming diagnostic tools for public health.

China appears to be having more success ensuring compliance, but other countries, such as New Zealand, offer alternative examples, as does progress in many European countries. A UK project using only Bluetooth signals to track contacts within certain distances and lengths of time estimates 56% of the population would have to use the app for it to work. This translates to 80% of all existing smartphone users; a high bar. The more centralised the control of citizens and of the internet, the easier it is to require such measures. But at what cost? Chinese censorial and surveillance regimes should certainly not be an aspirational model for open societies.

Facebook has been creating co-location mobility maps using aggregated, de-identified location data from users to show where people from different geographic locations are most likely to cross paths, which in turn can help researchers understand whether people living in a hotspot are likely to intersect with people from a different neighbourhood or town. But sharing any data is fraught for a company like Facebook, which has mishandled user data and privacy on numerous occasions. We would be remiss not to mention here the little publicised recent US Federal Trade Commission agreement with Facebook for a $5 billion settlement over the company’s Cambridge Analytica-related privacy violations.

In spring, Google and Apple announced a partnership with the aim of developing contact-tracing in a privacy-protected manner, one that involved no centralised database, and would be made available to public health agencies. Its strength is its decentralised model, which won praise from rights-based groups. Michael Veale describes how the challenge was the desire of many countries such as France and UK, that prefer their centralised models. He concludes that the Apple-Google contact tracing system is good on individual privacy but cautions against the kind of infrastructural power it enables. In global crises and pandemics, he further argues, “those in control of the computers, not those with the largest datasets, have the best visibility and the best – and perhaps scariest – ability to change the world” (Veale, 2020).
Contact-tracing, or, identifying and alerting those who have come into contact with someone infected within a certain timeframe in order to track the spread of an epidemic, has potential and problems for the relationship between the state and the citizen. It requires political and public will. For programmes like this to succeed, there needs to be trust built on empathy, patience, and the ability to offer a human touch to someone exposed to a life-threatening virus (see Bourdeaux, Gray and Grosz, 2020).

The Guidelines on Ethical Issues in Public Health Surveillance issued by the WHO in 2017 are unambiguous: surveillance data should only be collected for a legitimate public health purpose and countries must continually monitor for harms. The American Civil Liberties Union further (2020) argues that data-driven systems and decisions in this area must be led by public health officials, and that the scope of programmes must be tailored to and limited to public health needs and not provide an open window for broad surveillance activities by the state.

Getting the balance right – between digital data and control on the one hand and citizen empowerment and privacy protection on the other – is a core problem in the modern social bond between sovereign states and their populations in an era of digitalisation. Covid-19 clearly exacerbates this problem.

Spyware and the private sector

Is responsible surveillance possible if governments increasingly rely on digital surveillance ‘spyware’, procured from private companies, to track and target people despite concerns over human rights abuse. Traditionally developed by intelligence agencies, spyware is increasingly also developed by a small but growing number of private companies, many run by former military intelligence experts. Some spyware can be embedded on your phone, for example, by opening up an infected email or link that can turn on the phone’s microphone to clandestinely record or even take pictures through your phone’s camera. Information gathered can include your internet browsing history, personal text messages, emails, and location data.

Israeli spyware firm NSO Group has reportedly developed a new product to track the spread of the coronavirus, which analyses massive volumes of data to map people’s movements to identify anyone they have come into contact with. Around twelve countries are testing the NSO Group technology. The software is sophisticated enough to gather two weeks of mobile phone tracking data from an infected person and then match it against location data from mobile phone operators that can pinpoint individuals who were in the vicinity of the person with the virus for more than 15 minutes.

But NSO Group’s history is fraught with human rights concerns. It is their Pegasus spyware that is suspected of helping the Saudi Arabian government track the location of assassinated journalist Jamal Khashoggi. Facebook-owned WhatsApp has filed a lawsuit against NSO Group claiming it violated their terms of service for use of the messaging app as a delivery mechanism for its spyware. The University of Toronto’s Citizen Lab (2019) has identified over 100 examples where NSO spyware been abused. Predictably, the company argues it cannot help how its products are used. But this raises important policy questions about the need for regulation.

14 Spyware is software intended to extract information from devices. It is installed without consent or knowledge from users. For more see Turton (2020) and de Montijoye et al. (2018).
Similarly, US-based Palantir is playing an increasingly powerful role in providing tools to address the pandemic. Palantir was co-founded by PayPal’s Peter Thiel, a Facebook board member and a vocal supporter of Donald Trump’s presidency, who has stated he “no longer believes that freedom and democracy are compatible”. The company is building a coronavirus tracking tool for the Trump administration’s Health and Human Services (HHS) department called HHS Protect, aimed at helping officials compile data from across state and local governments, health institutions, and colleges. It is not clear where the data is coming from, how it will be used, or even what exact data is being gathered. The company also has a lucrative contract with the UK’s National Health Service (NHS) that gives the company unprecedented access to confidential patient data, including physical and mental health records, religious and political affiliation, and past criminal offenses. Palantir seeks other such contracts across Europe. The data will be stored on a UK government server, raising concerns this is a dangerous move towards state surveillance. Given the UK’s ambiguous record of domestic surveillance programmes, these are not unwarranted concerns.

Palantir also provides law enforcement agencies with software enabling broad, warrantless surveillance and profiling capabilities. Its system synthesises and aggregates data in such a way as to give state agencies close knowledge of an individual’s relationships, activities online, personal details, and networks, which means friends, acquaintances, lovers, and others whose own data becomes caught up in the web of surveillance of individuals who might only have been pulled over for a minor infraction. Palantir software combs through far-reaching data sources including financial documents, airline reservations, cell phone records, and social media postings. Palantir’s methods and algorithms for tracking raise a host of concerns regarding individual sovereignty in the digital age. It’s not difficult to see the potential for abuse. How do citizens know governments will limit their use of such data to ‘just’ track coronavirus?

UN Special Rapporteur on Freedom of Expression and Opinion David Kaye recommend a moratorium on the sale, transfer, and use of this kind of surveillance software until a robust human rights compliant regulatory framework is in place. Currently, companies appear to be operating with little constraint. The US State Department has published draft human rights guidelines pertaining to the export of these technologies, modelled after existing requirements for US companies regarding anti-bribery and export controls.

Over the last decade, whistle-blowers like Edward Snowdon have raised global consciousness and public attitudes towards privacy and mass surveillance in the hands of states. The fallout over Cambridge Analytica played a pivotal role in moving the needle on public anger towards corporate and social media malfeasance; especially against Facebook. Even still, it can seem difficult to argue against measures when real lives are at stake, and an anxious public seeks answers. One problem is that we’ve heard all this before. After September 11, 2001, the US government seized unprecedented powers of surveillance and mass data collection, justified on the grounds that greater monitoring was necessary in the name of national security. The expansion and persistence of these surveillance and data collection regimes are further reminder, if any was needed, that ‘emergency powers’ tend to outlive their emergency.

Digital rights organisations, such as the Electronic Frontier Foundation (EFF), argue that “governments should not be granted these powers unless they can show the public how they would actually help, in a significant manner, to contain COVID-19” (Schwartz and Crocker, 2020). The EFF further argues, the benefit to government of the use of these powers must be
weighed against costs to privacy, speech, and equality of opportunity and that they require safeguards, limits, auditing, accountability, and assurances that their powers are necessary and proportionate.

Perhaps instead of enabling state intelligence communities, we should be enabling health officials (Gray, 2020). Policies and technologies should be developed alongside public health experts to meet a narrow set of needs, be time limited and walled off from other arms of government such as immigration and border control agencies, which means that sectors of the population would be unlikely to participate in public health measures if they fear their immigration status is at risk. Technologies are unlikely to be effective if they lack public trust.

**Decoupling and bipolarity in an age of pandemic**

Covid-19 is a global pandemic, let us not forget. It exacerbates tensions in the relationship between states and the international system – especially the US and China – in an era of heightened contest between the forces of nationalism and global cooperation. De-globalisation and decoupling, rather than cooperation in the tech and digital sectors, are trends that were in train prior to Covid-19. The bifurcation of these digital ecologies will continue to strengthen. What started out as a US desire to decouple its economy from that of China’s – especially in the arenas of advanced technology, digitalisation, and intellectual property – is now reciprocated by similar Chinese desire.

The need for global coordination and cooperation is pressing, and yet the US took the decision to abandon the World Health Organization during a pandemic. For all the WHO’s shortcomings, this was an irresponsible decision to take. Indeed, the overall effect of the era of the Trump administration’s transactional bilateral attitude to international relationships has been capped by Covid-19 and framed by the mismanagement of the crisis from the start by President Trump. China would appear to be making greater mileage from the pandemic than the US and this is notwithstanding its initial lack of transparency about the origins of the virus, its aggressive “Wolf Warrior Diplomacy” (Berkofsky, 2020), its manipulation of the media and the WHO, the less than optimal utility of some of its coronavirus aid to European states, and a dramatically higher number of deaths than officially reported (Hutt, 2020 and Schaefer, 2020).

Lacking leadership in Washington, with no federal testing or tracing initiative months into the pandemic, an overwhelmed and over-privatised medical system, and President Trump’s dismantling of the pandemic response system created under the Obama administration, states were pitted against each other. California governor Gavin Newsom went so far as to declare its independence from the failed federal efforts, flexing the state’s own purchasing power to acquire necessary medical supplies. The connection between patterns of governance, disinformation, and the intentional incitement of crises for political purposes can be seen in the US as well as Brazil, for example. The crisis demanded a response that was swift, rational, and collective but instead the Trump administration responded like a dysfunctional government whose leaders were too ill-informed and corrupt to act responsibly.

If the trends in US policy continue, it will lead to a more China-centric world boosted by the growth of, and growing acceptance of, China’s cultural confidence across the globe (for the quintessential expression of this position see the powerful new book by Kishore Mahbubani,
The Chinese Challenge to American Primacy: Has China Won? [2020]). Such a view is plausible, but only if a number of factors are ignored.

(i) Xi Jinping and the CCP’s standing from its handling of the pandemic appears to have been affected within China, where distrust has grown. The creation of both greater domestic military control and ideological control by President Xi gives substance to this point (see Thayer, 2020).

(ii) The trend ignores the fact that in an increasingly polarised United States, the one area of substantial and growing bipartisan agreement is over US opposition towards China’s role and influence in world affairs; especially as the US becomes the state most affected by the pandemic.

(iii) The trend makes light of the growing resentment and resistance in Europe towards Chinese ‘mask diplomacy’ as an exercise in image manipulation. The prevailing sentiment is at best suspended scepticism and at worst outright mistrust of China’s intentions and behaviour.

But China will in all likelihood continue to press its advantage; especially as the inadequate actions of the Trump administration continue to diminish its global soft power (see Campbell and Doshi, 2020). As Stephen Walt (2020) has noted, key attributes of US soft power have traditionally been a global appreciation of its innovation; support for some key public goods; and its expertise and policy competence, especially at the leading edges of technology. The Trump administration’s international policy behaviour – from lacklustre to simply wrong, across a number of issue areas, such as trade for example, but especially Covid-19 – has diminished this perception, especially vis-à-vis the standing of China. Indeed,

“If the pandemic results in a global recession and the US fails to manage international recovery efforts, economic and political power may both shift further in Beijing’s favor … If the US remains absent without leave, China may take the crisis as an opportunity to start setting new rules according to its own global governance vision, displacing Washington from future ordering efforts” (Rapp-Hooper, 2020).

In effect, notwithstanding the mismanagement of, and misinformation about, the coronavirus by China, the pandemic could turn out to China’s advantage in their world position. The coronavirus could become the page break between the old post-World War Two, US-led liberal order and the new, increasingly bipolar order, with two major regional blocs centred on the United States and China and other regions, notably Europe and the Russian-led Eurasia, playing secondary roles. China may emerge from this process stronger than it went into it.

Exposing and amplifying existing inequalities

The battle for supremacy in the digital domain is one of the keys to the issues of both decoupling and bipolarity discussed above. But it is not simply about the US and China. Moments of crisis also bring into sharp focus wider pre-existing inequalities. The pandemic is widening the impact of the digital divide in the Global South where most countries are virtually absent from the number-based narration of the pandemic and this has consequences:

“What is clear is that what gets counted exists, in both state policies and people’s imaginaries. Numbers affect our ability to care, share empathy, and donate to relief
efforts and emergency services. Numbers are the condition of existence of the problem, and of a country or given social reality on the global map of concerns” (Milan and Treré, 2020).

This data gap exists in both the limited visibility and quality of data that are already lacking in ‘normal’ times. Hilbig (2020) reminds us of digitalisation’s mixed record on development, and what harms might be amplified in responses to the pandemic, including potential abuse with increased surveillance, biometrics, behavioural controls, and the questionable practices of FinTech corporations, especially given the need for stronger civil society.

The private tech take-over of the welfare system has been a long in the making and the current pandemic is accelerating this development (Dencik and Garfrog Kaun, 2020). While companies like Google and Facebook have used the Global South as a test bed for new and unregulated mechanisms of data capture, these same mechanisms are being rolled out globally in the face of Covid-19. In addition, for-profit data collection is becoming increasingly central to how states manage their welfare systems. While we may be seeing the revitalisation of the role of the state, any renewal of social welfare will look quite different from that of the post WWII period. It will be driven by private corporations that will use their tools and platforms for profit irrespective of any public good they might deliver. “It will be based on opaque and intrusive forms of datafication”, not only the intensification of surveillance underway, but by two interconnected processes: “the transformation of human life into data through quantification, and the generation of different kinds of value from data” (see Mejias and Couldry, 2019).

Where do we go from here?

Since we started this report, we have now arrived in the middle of what might just be two generation-defining global reckonings. Not only the Covid-19 pandemic but also racial justice issue triggered by the police killing of George Floyd. Social media is being used more than ever to target communities of colour and incite white supremacism. At the same time, the level of digital engagement people have secured as a result of the global pandemic may be a contributing factor in the spread of global protests for racial justice, as is the availability of time some have for taking to the streets in protest. Equally linked, concerns about state and private-sector surveillance, and the right to privacy and assembly connect both these societally changing moments.

Tech companies control more human communication than any single government ever has (Benesch and Llansó, 2020). As Jennifer Cobbe and Elettra Bietti (2020) argue, as long as Covid-19 remains a global concern, the platform companies will play an ever-increasing role in mediating everyday life. Amazon has been a major, and massive, beneficiary of the pandemic, as home delivery demands spike. This is the future big tech has long dreamed of, and others warned of. But it needed a pandemic to operationalise it.

Digital tools of course have an important role to play but the best technological interventions help healthcare professionals, not replace them. Data brokers shouldn’t profit from the pandemic nor should they be allowed to ‘Covid-wash’ their business practices. Discussions about surveillance that focus solely on privacy miss some of the more basic concerns around weak quality-testing, poor problem selection, and the balance of powers between individuals, states, and the private tech sector. Regardless of how we might feel about particular
surveillance technologies, “it is neither new nor politically radical to suggest that where they implicate exceptional powers, both the constitutional and contractual checks on those powers should include robust oversight, sunset clauses and provisions for remediation of disputes, before these powers are exercised” (McDonald, 2020).

Ultimately, there is too much focus on the pandemic as a technical problem rather than a resource problem. When governments lack sufficient response capacity, is the focus on developing what amounts to surveillance tools wrongly prioritised? If so, perhaps we must reckon with the underlying reason for implementing such measures and what kind of regimes are being created and sovereignties protected. In short, we must keep in mind the human side of any pandemic response. In the battle between states and platforms over digital sovereignty, we must remember that neither end up adequately protecting the public interest. To protect the public interest, we need to rethink sovereignty and the way states and platforms work together.
Conclusion: Digitalisation and disillusion in the third digital
decade

Historical hindsight: Digitalisation in perspective

Full understanding only comes with historical hindsight. Contemporary, empirical, issue-focused study is important, but it cannot capture the whole picture of the impact of digital technology on society. As this report suggests, we live in an era of communication transformation that is as profound as Gutenberg’s invention of the printing press. The revolution in printing was liberating for humanity in many ways; from the fueling of the Reformation and the European Enlightenment, sowing the seeds of revolutionary independence in the US through, to the rise of modern science. The modern technological revolution in communication over the last several decades has been equally revolutionary and democratising but, by way of contrast, it has also been accompanied by large doses of disillusion.

The modern communications revolution has resulted in both social liberalisation and greater control, especially in states already exhibiting authoritarian tendencies. However, growing control is not a product of authoritarian states alone. The modern communications revolution has also created a new class of powerful and financially lucrative private actors with powers over information, communication, and a range of life’s daily activities. In addition, we suggest, the relationship with sovereignty is perhaps one of the most significant areas of modern-day life impacted by digital technology.

As Shoshana Zuboff has shown in her seminal article ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) and her subsequent influential book (Zuboff, 2019), we are entering a new era of economic organisation on the back of the digital technological revolution: what she calls “surveillance capitalism”. This comes about via the translation of human experience into behavioural data. If manipulated skilfully, this data can have the predictive power to create what she calls a “behavioural futures markets” that can “… nudge, coax, tune and herd behaviour…” (2019, p. 8) for material and/or political gain.

Beyond Zuboff, Sean McDonald and An Xiao Mina (2018) describe the fragmentation of the internet as a result of the ways governments, in particular, “… are using their influence to shape the ways that digital companies, markets, and rights connect us online”. This new form of realpolitik they call digitalpolitik; it can be seen as “… an emerging tactical playbook for how governments use their political, regulatory, military, and commercial powers to project influence in global, digital markets”.

In this new organisational world, Google has become to “… surveillance capitalism what General Motors was to managerial capitalism” (Zuboff, 2015). But, surveillance capitalism’s characteristics are no longer confined to the large internet providers. And as Natalie Maréchal and Ellery Roberts Biddle (2020) demonstrate, it’s not the content but rather the surveillance-based business models that are, or should be, the biggest concern. The acquisition and manipulation of data is now the default position for most large organisations, be they private or public. Acquisition is occurring at an unprecedented rate and in an asymmetrical manner. Further, as a simple empirical observation, personal sovereignty is eroded within the complex matrix of private data and access to this data by the modern state.
The battle between democracy and authoritarianism: Tech power and public interest

“In the coming few years either tech will destroy democracy and social order as we know it, or politics will stamp its authority on the digital world. It is becoming increasingly clear that technology is currently winning the battle” (Bartlett, 2018, p. 1)

Bartlett’s polarisation of our options is extreme. Under any circumstance, this report has provided sufficient evidence to suggest that the further unfettered independence of the major tech giants is not something to encourage. Unregulated monetisation of behavioural data is open to abuse and not in the wider interests of society. But, the alternative vision – of the state securing unfettered control over the internet – is, as we have equally argued, similarly unappealing and equally fraught with dangers.

Perhaps what is more likely to happen is a protracted war of attrition between sovereign states and transnational companies, each reacting to the other and still thinking that they can win this war, while in fact, neither will achieve a total victory. After some period of time, as Bertrand de La Chapelle suggested to us, there will need to be some kind of peace negotiations to hash out a set of principles distributing respective zones of influence and authority and how they interplay. To go back to the Westphalian origins of sovereignty, the same situation happened with the 30 Years War, when the warring parties, following massive casualties, recognised that there could be a decisive winner and there had to be a settlement. A different, but relevant historical analogy can be found in the struggle between Church and State, which only ended when they defined their respective zones of competence.

The current digital revolution is without precedent. In contrast to earlier revolutions, it is evolving exponentially rather than in linear fashion with regards to velocity, scope, and systems impact, and doing so across the spectrum of socio-economic production and governance at national and global levels. What will be decisive in the relationship between the digital giants, the citizen, and the state, is whether a balance between individual privacy and state sovereignty can be maintained in the face of the tech giants’ increasingly sophisticated and intrusive control mechanisms. But this remains an open question that is further complicated by the ambivalent attitudes of government towards individual privacy and the state’s assumed rights to sovereign control over its population.

For sure, digital technology is dual use. But the jury is – hopefully – still out on whether digitalisation facilitates authoritarianism rather than democracy. It clearly can and does favour both, depending of the starting point. We can see a divergence of trajectories along a spectrum between the massive authoritarian surveillance state on the one hand and new types of digitally enabled democracy – probably starting in smaller countries first – on the other. Innovation and democratisation should not have to be derailed in order for excess control to be contained, although constraining opponents is easier than enhancing democratic openness.

Unfortunately, the ability of society to address these issues is easier said than done. All states, from democratic to authoritarian, as a matter of right demand access to things like AI’s enabling of biometric identification technologies which, they argue, can then be used for good, in, say, the health domain. But they can also be weaponised against people at home and abroad, once acquired. Moreover, these competitive and repressive tendencies in digitalisation can be exacerbated by the need to come to terms with the dramatic changes and challenges in the global order of the last few years, as we noted in some detail in the discussion of Covid-19.
Multilateral and cooperative collective action problem-solving is in decline at the very time when cooperation rather than competition in the governance of the internet is becoming increasingly necessary. Initiatives with the most cooperative potential come from neither the great powers nor the large corporations. EU initiatives in areas like data protection may offer potential. But the EU’s ethical commitment is not necessarily matched by its implementation capability, especially in the face of resistance from the US and China.

The internet is currently owned, operated, and governed by giant, private tech companies that cannot be trusted to self-regulate. The internet should not be an ungoverned space. Both regulatory responses and greater decentralisation of digital spaces and architecture must be employed. However, we cannot expect consensual input from the major states in an international order that appears to be drifting inexorably away from its liberal underpinnings in the direction of a more hard-nosed, realist, nationalist-driven world order of renewed geopolitics, complicated by competitive geo-economic and geo-cultural/civilisational-nationalist dynamics (see DOC, 2019). This point is highlighted in our discussion of China’s digital foreign policy and its desire to redesign the governance of the internet.

Neither digital technology, nor the disruption that comes with it, are forces over which humans should necessarily be powerless. Technology is, after all, a product of human creation. Design matters. Privacy can be built into technologies just as easily as surveillance – it’s a matter of choice that it is not. Now, more than ever, is the time to establish global norms and ethics on how digital technology is used and regulated and to develop models that empower people. But this will not happen independently of human intervention and without human leadership. At the most basic level of public policy, we need a shared and comprehensive view of how digitalisation continues to reshape socio-economic, cultural, and political environments. Clearly, there is a struggle emerging to determine the respective weights of digital technology and people in the governance of national and international society.

At the domestic level, in the OECD world at least, the continued existence of the rhetoric of democracy and the practice of democracy are not one and the same thing. The future of democracy is no longer assured. For the minority who care to look, a nascent trend towards techno-authoritarianism in the hands of a skilled techno-elite is observable. Artificial intelligence and digitalisation exacerbate existing inequalities as well as create new ones. AI is not a neutral technology, even if outputs and design are squarely in the hands of humans (Kaye, 2019). Democratic and authoritarian politics alike are both shedding sovereignity to technology at the same time as they are trying to claw it back. Digital technology and AI can be and should be beneficial utilities in the delivery of public goods; especially in the health, welfare, and educational sectors and in the engagement of citizens in the political process, particularly in redressing digital divides and in support of marginalised communities.

But this won’t happen in the absence of human intervention to develop a stronger sense and practice not only of digital ethics but also about new principles for collaborative mechanisms to manage the transnational digital commons that hold the tech giants, and their algorithms and software – which have the ability to influence human behavioural attitudes – to account. We need stronger roles for civil society, better transparency from both the private and public sectors, and support for innovation in cooperative and community-owned platforms. Governments not only need the necessary workforces capable of spotting abuse, they need the political will to act. Not all governments will possess this expertise and even where they do, appropriate action is not inevitable, as with US inaction following the 2016 elections. Electoral
politics and the necessary accompanying legislation – especially the ability to contend with bots, trolls, and other influencers – hopelessly lags digital capability.

At the international level, unilateral transactional approaches will not be sufficient to secure the meaningful governance of digitalisation. The oligopolistic characteristics of the international operations of the tech giants – data gathering and use, market share, cross market holdings – are increasingly beyond the scope for control of all but the strongest of governments, no matter how powerful, to regulate. The legal powers present in the GDPR, for example, will only be as strong as European governments’ willingness to use these powers and an accompanying willingness to support other governments in holding the big tech companies to account. To rein in the behaviour of the big players, and create opportunities for new market entrants, and govern humanely, we must distinguish between home and host country governments. If we are to take sovereignty seriously, a subsidiarity principle would suggest that host country regulation should prevail. But as is more likely given the inequalities of power, home country regulation of the major digital actors will always prove more powerful. For example, attempts by the EU to reign in and tax the big American giants not only face resistance from the corporations themselves but also from the current US administration and, in all probability, future US administrations.

For democratic and human rights to prevail, decisions and policies must be guided by and grounded in law. Even EU legislation, which has demonstrated some positive potential, is undermined by state-level policies and practices around surveillance and mass data collection; for example, in countries like the UK, and with French anti-extremism legislation bypassing due process, and with authoritarian controls and state capture of the media in Hungary and Poland. How states, and especially the major players, behave at home will be the test of how they are likely to behave internationally. The ‘end of history’ has come and gone. The liberal order is unlikely to be restored. As Pascal Lamy (2018) notes, “Adjusting old narratives to new environments will not be enough”. Outdated mind-sets will need to be superseded in order to take account of the impact of modern communicative technologies on international relations as we strive to maintain and develop an open, and increasingly digitally networked, new order.

Policies, norms, and regulations have not been able to keep up with the pace of innovation in digitalisation. Superseding old narratives will require the restructuring of our understanding of both sovereignty and digitalisation. This restructuring must seek to secure an equilibrium in the contested prerogatives and properties of both in an era when it is clear that states no longer have a monopoly on governance and regulation but non-state actors such as the tech giants are not formally recognised as having the right to exercise de jure governance roles, notwithstanding their de facto ability, and at times eagerness, to do so.

**Next steps: Thinking beyond sovereignty**

This report has been an implicit challenge to the utility of sovereignty, traditionally understood, in the modern age, especially since the development of digitalisation. By way of conclusion we should, therefore, probably make our understanding of the limited utility of sovereignty in the contemporary era explicit. Given the vast bodies of literature on the subject, this is a daunting task and we are admittedly in danger of trivialising it. But it is impossible to look at the relationship between digitalisation and sovereignty as we have done in this report and accept that the traditional understanding of sovereignty as both a concept and practice is intact. This is especially so if we considered it as a weapon in the problem-solving armoury of the modern state where its utility is constantly challenged and exercised in new ways. While this
was not always the case, its disutility as a problem-solving device has grown dramatically since the onset of the current stage of globalisations in the last third of the 20th century. Initially picked apart by economic, political, and legal advances, both domestic and international, the onset of digitalisation has accelerated this process in exponential fashion.

The traditional theory of sovereignty discussed earlier in this work has been unpicked by practice. The classic theory of sovereignty – which sees states defined as the highest, undivided unit of absolute spatial authority and accountability – if perhaps once plausible, now no longer holds good. Political authority is no longer, if it ever was, “…unlimited, undivided and unaccountable” (Herzog, 2020). Such absolutist assumptions about sovereignty identified in this definition – notwithstanding the manner in which they are often pretentiously and unthinkingly idealised, and peddled, by modern-day politicians – have a hollow ring to them in 2020, in both theory and practice. Nowadays, the concept confuses more than it clarifies. Yet, for the vast majority of states, the idea that they possess sovereignty, and that sharing it is a bridge too far, is still the dominant mode of thinking. Politicians, sticking to this rhetoric, fail to see, or at least acknowledge, how digitalisation has created a whole new layer of private actors and practices that challenge traditional notions of sovereignty.

Digitalisation, more than any other process and practice, renders the traditional territorial notion of sovereignty redundant at the same time as it ushers in new articulations of state power, often ironically in the name of clinging to national sovereignties. The growing sophistication of the internet has given rise to new forms of centralisation, in the hands of both states and the principal digitalisation companies themselves. Authoritarian states seem especially keen to re-envision internet governance at the level of infrastructure as a means of re-coding domestic sovereignties and enabling, justifying, and growing their own surveillance regimes.

The prevailing mood among detached analysts and researchers on what to do about this situation is, to say the least, pessimistic. Several core questions must form the agenda for study in the immediate future if we are to have any chance of securing the democratic evolution of digital media and communication in the face of its more authoritarian tendencies. The last decade, especially, since the failure of the Arab Spring of 2010-11, has seen the optimistic assumptions of flatter, horizontal, and open access to both the provision and reception of information empowering the previously powerless give way to a growing recognition of the strength of hierarchical, elite, corporate, and indeed increasingly oligarchically controlled digital media. This does not mean there aren’t incredibly powerful ways digital technology can improve lives and act as a tool to hold power to account. Alternative models are being experimented with all the time. But we stand at a crossroads.

Research must redouble its efforts to mitigate the underlying ideological and anti-democratic tendencies in digital media that are all too often obscured by two explicit but unsustainable assumptions: (i) the assumption of the benign neutrality of digital media communications; and (ii) the assumption that our decision-making is driven by rational expectations that online information resources are driven by facts, truth, and the search for authenticity. Our initial complacency on this score is surely at an end. Neither of these two assumptions stand scrutiny in 2020. As a reading of the annual surveys of agencies like Pew and Reuters tell us – notwithstanding the popularity of search engines and social media – trust in internet information is declining over time. The problem we face, however, is that the lack of trust, rather than generating a healthy scepticism as to whether information is true or false, is just as likely to generate apathy and cynicism with accompanying negative consequences for citizen participation in political life.
The implications for the relationship between digitalisation and social and political life should not be lost on us. In an era when information and misinformation is available as never before, citizens, and indeed many states, face a crisis of public communication over which they have little, dare we say ‘sovereign’, control. If we cannot develop a better understanding of how citizens interact with, and are influenced by, the products of digitalisation, we will have no chance of putting digital communications at the service of the community rather than putting the citizen further under the control of the owners of social media and communications.

This is a global problem, not one for notionally sovereign states. Any successful resolution of the current impasse will not come from great power geopolitical games seeking to reassert the absolute sovereignty of the state, be it in a bipolar or multipolar context. It must come from a recognition of sovereignty as, at best, a fungible process of bargaining in hybrid, invariably digitally networked contexts. While there is evidence to suggest that in some international areas and international relationships, hybrid regulatory interaction was becoming something of a norm in the early years of the 21st century (see Slaughter, 2004 and 2017), this trend is now under challenge from the US-China struggle to decouple from one another and support distinct and contradictory digital ecologies. Not all networks will be undone and indeed some will continue to grow and new ones will be created – the global digitalisation genie will not easily be forced back into a bottle. But the problem remains that in the current era, the pursuit of nationalist, transactional international relations is regressive for these processes and habits of behaviour as both modus operandi and modus vivendi.
References


Gross, Anna, and Murgia, Madhumita (2020, March 27). China and Huawei propose reinvention of the internet. Financial Times. Available at https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2.


https://members.tortoisemedia.com/2019/12/05/the-global-ai-index-part-5-the-new-world-order/content.html?sig=yurXiggPLN9wUXwT63cyjY3NHA67borVPOb6Cb9vUc.


