DIGITAL POLICY LAB

Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry

Contents

Summary

- Covid-19 has revealed the critical importance of technology for economic and health resilience, making Europe's digital transformation and sovereignty a question of existential importance.

- Rising US-China tensions are an additional incentive for Europe to develop its own digital capabilities; it risks becoming a battleground in their struggle for tech and industrial supremacy.

- Democratic governments – keen to preserve an open market in digital services while protecting the interests of citizens – find the European model an increasingly attractive alternative to the US and Chinese approaches.

- The EU cannot continue to rely on its regulatory power but must become a tech superpower in its own right. Referees do not win the game.

- Europe missed the first wave of technology but must take advantage of the next, in which it has competitive advantages such as in edge computing.

- EU member states lack a common position on tech issues or even a shared understanding of the strategic importance of digital technologies, such as on broadband rollout or application of AI.

Preface

José María Álvarez-Pallete

Chairman and CEO, Telefónica S.A.

In times of uncertainty, humanistic values must serve as the compass that sets us on the right path. The covid-19 pandemic has accelerated the digital transformation of our societies and our economies at a dizzying rate. In just a few weeks of lockdown we have seen teleworking, e-commerce, and online education advance as much as over a five-year period under normal conditions.

Keeping communications up and running has been our first and primary contribution to this health, social, and economic emergency. Indeed, Telefónica became one of the support structures that kept the business, cultural, educational, labour, and financial activity of our societies alive in Spain.

Digital infrastructure has proved to be fundamental for social welfare, especially health and education, and the functioning of the whole economy. In the face of the crisis, Telefónica's mission "to make our world more human by connecting lives" has become more relevant than ever. We have learnt that connectivity is crucial for inclusive digitalisation and, with our mission and values as our guide, this crisis has brought out the best in us.

The year 2020 will be remembered as the year of the pandemic, but also as the year when our world restarted on a new course, and there is no turning back. We have difficult times ahead of us where we will need to cope with the economic stagnation and increased inequalities that we have lived through in recent months.

Now, more than ever, we need a new Digital Deal to build a better society. The values of solidarity and cooperation have prevailed in these critical times. This should inspire modern governance models as the traditional recipes no longer work. The close cooperation and dialogue between governments, civil society, and companies is of paramount importance to reach social commitments. This Digital Deal implies defending our values without disregarding fundamental rights in this new era, and setting course for a more sustainable, inclusive, and digital society.

The main axes of this new Digital Deal should be the following:
First, inequality is the greatest challenge we face. We should ensure that most of the population has access to technology and the opportunities brought by the new digital world, reducing the digital divide. Therefore, investing in people's digital skills is critical. Traffic on our online education platforms has grown by more than 300 per cent and 85 per cent of the jobs in 2030 do not yet exist. Reskilling and upskilling the workforce to meet the needs of the labour market and reinventing education for the digital age are essential to ensure that no one is left behind. And at the same time, social and labour protection systems should cope with the rapid evolution of the digital economy.

Second, we should make societies and economies more sustainable through digitalisation, supporting key sectors, technologies, and innovation to accelerate the green transition and the digitalisation of small and medium enterprises (SMEs) and public administrations. SMEs have great weight in the economy and job creation. Thus, it is necessary to set up a digital reconstruction fund at regional and local levels, which could be used to support them in their digitisation process.

Additionally, we need to build better infrastructure. Telecommunications have been confirmed as a vital sector in contemporary societies, but they can only fulfil their role if they have the best networks. We have witnessed that having the most powerful fibre network in Europe is something essential. Hence, it is crucial to reinforce and invest in very high capacity networks, as well as to enable new forms of cooperation and facilitate wide deployment of resilient, reliable, and fast networks. Moreover, building better infrastructure also means connecting the unconnected, reducing the digital divide.

Ensuring fair competition is also of paramount importance. The roadmap of renewed industrial strategies must be fine-tuned and defined to minimise national protectionism, modernise the rules on competition and supervision of the markets, and update fiscal policies. We ask for the same rules and the same obligations for the same services. At the same time, it is necessary to design national and regional long-term strategic plans to foster the development of local industries focusing

Foreword

Anthony Giddens

Life Fellow of King's College Cambridge and Emeritus Professor at the London School of Economics

The digital revolution is the greatest transformative force in world society today, developing at a pace unseen in any previous period of history and intrinsically global. An estimated 45 per cent of the world's population have smartphones and even more have occasional access to one. This is the first time ever that cutting-edge technology has gone en masse directly to poorer areas of the world. Combined with the impact of radio and television – themselves now largely digitalised – huge numbers of people have access to 24-hour breaking news. Social media have made a reality of Marshall McLuhan's global village, where people form personal friendships and intimate relationships, but where there is also gossip, innuendo, deception – and violence. What is Twitter, but empty chatter? And yet digitalised it intersects deeply with power. Gossip, innuendo, and deception: these are an intrinsic part of 'fake news', with all its disturbing effects in politics and other domains. The global village, it has aptly been said, will have its village bullies and so indeed it has turned out to be.

Demagogic leaders can communicate with their supporters directly in ways that were never possible before – and can keep whole swathes of the population under direct surveillance. New forms of resistance, and even insurgency, however, also arise.

As contributors to this volume point out, the realities of the digital age are a long way from the early hopes and aspirations that many had with the rise of the internet. Some of its pioneers, such as Tim Berners-Lee, the major figure in the creation of the world wide web, believed that it would be above all a vehicle for collaboration and democratisation. Yet as we all now know, its dark and destructive side brooks very large too. The uprisings of the Arab Spring were the first digitally driven democratic movements and at the time they seemed to many to presage a breakthrough. The reality turned out to be much more complex and disturbing.

The advent of the digital age is often equated with the rise of Silicon Valley, but extraordinary although that is, its true origins lie in geopolitics and political power – to which it constantly returns. The origins of AI can be traced in some substantial part to the contributions of Alan Turing during the second world war. Yet the driving force of the digital revolution more generally came from the 'Sputnik moment'. The first being ever sent into space was not a human, but a dog, Laika – a mongrel from the streets of Moscow – in Sputnik 2. The Sputnik programme was a huge shock to the American psyche. It prompted a massive response from the US government, with the setting up of NASA and ARPA (later changed to DARPA) and the pouring of hundreds of millions of dollars into research on the military frontier. The ARPANET was the first origin of what came later to be called the internet. The rise of Silicon Valley and the huge digital corporations is inseparable from the geopolitical transformations of 1989 and the unleashing of free markets around the world. They did not do the core research upon which their meteoric rise was based; and it was an artefact of a very particular phase of history.

Itself divided, Europe figures largely as a backdrop to this scenario, rather than as one of its driving forces. It is precisely this that explains the dilemmas explored in some detail in this volume. 1989 was a time of transformation in China too, and a turning-point – in Tiananmen Square. For better or worse, the reaffirmation of state power that followed was the springboard for the 'Chinese model' – a market economy coupled to, and overseen by, an authoritarian state, but one that in economic terms has been dramatically successful. China has its own huge digital corporations – of which Huawei is one, if by no means the biggest – but they operate within the penumbra of the state. The country now has the world's most advanced quantum computer and is more or less at level pegging with the United States on the frontiers of AI, including its applications to weaponry.

Europe has not wholly been left behind in the coming of the digital age – after all, Tim Berners-Lee worked at CERN. Yet in the 'new Cold War', if that is what it turns out to be, Europe once more finds itself caught in the middle, sandwiched between the US and China, with a digitally malicious Russia standing on the side-lines. Thus far at least, the impact of covid-19 has served to deepen these divides. Its consequences could introduce a whole series of further dislocations and rivalries across the globe. The papers in this volume provide a valuable assessment of how Europe, and specifically the European Union, should respond. The full panoply of strengths and weaknesses of the union are on display and it will be not at all easy to chart a way through.

Introduction: Europe’s digital sovereignty

Jeremy Shapiro

Research Director of the European Council on Foreign Relations

“Can we ring the bells backwards? Can we unlearn the arts that pretend to civilise, and then burn the world? There is a March of Science. But who shall beat the drums for its retreat?”

Charles Lamb, 1830

Change is the idiom of our age. In recent years, change seems to have arrived at a bewildering pace from almost every direction. New political movements, newly powerful states, and novel diseases all seem at times to threaten, as in the English essayist Charles Lamb’s day, to “burn the world”. At the root of nearly all these daunting changes lies the vast opportunity and perilous promise of digital technologies. In recent decades, they have fundamentally altered how people and societies interact on every level, from how we make war to how we make love.

As a result, the questions of who owns the technologies of the future, who produces them, and who sets the standards and regulates their use have become central to geopolitical competition. Nations around the world are trying to shape the developments in new technology and capture the benefits – both economic and geopolitical – that emerge from this era of rapid change. They are, in short, seeking to protect their digital sovereignty – that is, their ability to control the new digital technologies and their societal effects.

For European policymakers, the idea of digital sovereignty is part of a larger struggle that they face to maintain their capacity to act and to protect their citizens in a world of increased geopolitical competition. On a host of issues, from Iran policy to military defence and regulating disinformation, it appears that the European Union has never been as sovereign as it thought. A time of fiercer geopolitical competition, and an America more focused on its narrow interests, have exposed the EU’s lack of independence in new ways –not least in the digital realm.

It is now clear that, if Europeans want to reap the economic benefits of emerging digital technologies, ensure their politics remain free from divisive disinformation, and decide who can know their most personal information, they will have to protect their digital sovereignty and compete with other geopolitical actors in the digital realm.

The European Council on Foreign Relations has proposed a new concept of “strategic sovereignty” that can help guide the EU and its member states through this new era of geopolitical competition. Strategic sovereignty implies that the EU and its member states need to preserve for themselves the capacity to act in the world, even as they remain deeply interdependent. Promoting European digital sovereignty is a critical piece of this effort. The purpose of this volume is to aid in that effort by helping readers understand better the challenges and opportunities that digital technologies, and the geopolitical competition over them, poses for Europe and its member states.

The contributors to this volume examine the geopolitical context in which Europe operates on a variety of issues, including 5G, cloud computing, and competition policy, and suggest ways to better protect European sovereignty. The focus, reflecting the nationality of most of the authors, is on the situation in Spain, but the lessons apply broadly across Europe. This chapter sums up the issues explored by dividing them into problems that have been around for several years, new problems that have emerged in the last couple of years, and assessing the key challenges and opportunities that the EU and its member states face in enhancing European digital sovereignty.

Continuity

Technological developments naturally focus our attention on change. But, in this whirl of dynamism, many less stirring, but no less critical, pockets of continuity often go unnoticed. Technology can engender rapid changes, but, as many of the contributors emphasise, several aspects of the struggle for digital sovereignty have already been with us for several years and we can expect that they will continue to shape that struggle for many years to come.

The first concerns the **continuation of the bipolar competition between the United States and China** that is undermining international cooperation, particularly on technology issues. Nearly all the essays underline that this conflict will likely persist, and indeed that US-Chinese relations, particularly on technology issues, will continue to deteriorate. As both Fran Burwell and Janka Oertel show, the pandemic has exacerbated existing divisions between the US and China. Most of the authors see their burgeoning conflict as framing the European struggle for digital sovereignty. Europe remains digitally dependent on both the US and China in a variety of domains, from chat platforms to telecommunications equipment. Competition between the US and China means that both sides increasingly see the European market as a critical battleground in the larger struggle to establish their global technological and industrial dominance. Europe, in Oertel's words, is already "caught in the crossfire". As recent political debates within Europe on issues as diverse as 5G technology and internet regulation demonstrate, US-Chinese rivalry is starting to impinge on practically every technological issue.

The second area of continuity concerns the **capacity of digital tools, particularly social media, to spread disinformation and undermine democratic institutions**. As José Ignacio Torreblanca points outs, the coronavirus crisis has only highlighted the degree to which both foreign and domestic actors can use a combination of digital technology and social psychology to pursue a variety of political agendas, including disrupting democratic processes and exacerbating domestic political polarisation. The growing awareness of this problem has not yet lessened its prevalence and we should expect conflict within societies over how to regulate digital content. The fact that, in Europe, the dominant social media companies are American means that the struggle to regulate them will have geopolitical consequences.

A final field of continuity concerns **the persisting digital divide within Europe**. As Alicia Richart emphasises, this divide does not correlate with the size or power of the state. Some of the largest and wealthiest states in Europe, such as Germany and France, lag in creating digital infrastructure, while Lithuania and Greece are among the leaders. The more critical divide is also within states: between urban areas that tend to have effective access to digital infrastructure and rural areas. Digital divides have all sorts of pernicious effects on individual lives and national solidarity. But the coronavirus also highlights just how critical digital technology and infrastructure has become in enabling countries to retain their capacity to act, particularly in crises. Spain's strong digital infrastructure, as Richart points out, was essential to its capacity to manage the lockdown and its overall covid-19 response. Digital divides thus also threaten both European sovereignty and European resilience when the next crisis, regardless of its nature, hits.

Change

Despite these important continuities, the contributions to this volume also show some significant changes that have occurred in the last couple of years. The most salient appears to be **the increasing attention given to, and activity surrounding, digital sovereignty issues** by almost every level and part of government in recent years. As most self-help programmes suggest, the first step to solving any problem is recognising that you have a problem. Nearly all the essays, and particularly those by Torreblanca on disinformation, Andrew Puddephatt on internet governance, and Ulrike Franke on artificial intelligence (AI), document an increasing recognition that digital technology has become a critical battleground in geopolitical struggles. This seems almost a banal point given the constant drumbeat of news about cybersecurity and disinformation. But it is important to recognise that as recently as 2016, the idea that Europeans needed to understand, say, social media platforms as a source of national power remained controversial.

Concerns about digital sovereignty mean that digital competition is no longer just about economics. This realisation has given rise to a re-evaluation of Europe's digital competitors. The biggest change in thinking about digital sovereignty surrounds **the increasing concern about the US abuse of its dominant digital position.** As Andrés Ortega notes, there is a growing sense of a "neocolonial" dependence on US internet companies. European efforts to, for example, impose a digital tax, fine large American technology companies for anti-competitive practices, and consider new industrial policies to foster European champions in key areas all reflect this growing discomfort.

This reliance on the US, at least to date, far exceeds

European digital dependence on China. But the essays outline **an increasing wariness of China as both an economic and political competitor in the digital realm.** If, from a digital sovereignty perspective, the US is the biggest problem, China has become the biggest fear. As Ortega points out, China is increasingly interested in the European market and has been persistently moving up the value chain. China now challenges European (and US) companies in virtually every high-technology sector. But, as Oertel notes, the Chinese have begun to wear out their welcome in Europe. The European-Chinese relationship was deteriorating rapidly even before aggressive Chinese diplomacy during the coronavirus crisis added to the troubles. Chinese finance and equipment remain attractive and cheap. But new efforts at investment protection and recent attempts in the United Kingdom and Germany to revisit the issue of allowing Huawei equipment into the 5G network, for example, demonstrate a heightened concern that China will threaten European digital sovereignty.

This re-evaluation of the problems that both the US and China present for European sovereignty has also led to **a new way of thinking about future technology, particularly with regard to AI and the next generation of telecommunications standards.** Both Franke and Andrea Renda note that many EU member states have recently become convinced that AI represents both a threat and an opportunity for European digital sovereignty. Renda speculates that, even if European companies missed taking advantage of some recent commercial opportunities for new technologies, this new awareness means that Europe is well positioned for the next wave of technology. European companies have competitive advantages in some next generation technologies such as edge computing, which distributes processing power and data storage closer to the locations where they are needed. It is a useful reminder that, for example, after the fight over 5G is over, there will be a new battle over 6G.

European challenges

Both the changes and the continuities point to some clear challenges for Europeans in protecting their digital sovereignty.

As nearly all the contributors point out, a key European disadvantage lies in **the lack of significant European digital corporations with global influence.** Despite Europe's advanced digital capabilities, there is no European Google or Tencent. The increasing geopolitical competition over tech issues has made clear that this lack of national champions represents a big disadvantage in the struggle for European sovereignty. That said, it is much less clear what to do about it. Past efforts to create European champions have often turned into white elephants.

Part of the answer might lie in recognising that Europe also faces a challenge in **reconciling the liberal impulses of the single market with the new struggle over digital sovereignty.** One of the reasons that Europe lacks digital champions is that promising companies often get bought up by larger foreign competitors on the open market. Moreover, as both Ortega and Oertel point out, foreign takeovers of European companies allow Europe's digital

competitors access to both European technology and digital infrastructure. The continuing wave of efforts to regulate foreign investment at both the European and member-state level testifies to an awareness of the problem. But the difficulty of implementing those efforts in a way that does not descend into protectionism, and that preserves the intra-European competition that is at the heart of the single market, demonstrates how far the EU and its member states must go.

The final challenge for Europe is a familiar one and is implicit in almost all the contributions, though only Torreblanca really focuses on it. It is that, when it comes to technology issues, **it is not clear that there is a European position or even that most member states want one.** The differing approach and positions on regulatory issues, such as content regulation, not to mention intra-European competition for high-tech jobs, means that the EU starts at a disadvantage in competing for digital sovereignty with more coherent political actors such as China or the US. On the other hand, it is clear that, in comparison to its rivals, there is a European approach to issues such as privacy of data. And, as Ortega, Oertel, Franke, and Richart agree, if they work together, EU member states can vastly increase their global influence to push that common approach. The need to find a delicate balance between the compromises needed for a common position and the need to protect the particular interests of various member states will certainly continue to challenge European policymakers.

European opportunities

While these challenges are certainly daunting, the contributors also highlight several opportunities, both technological and political, that Europeans bring to the struggle to retain digital sovereignty.

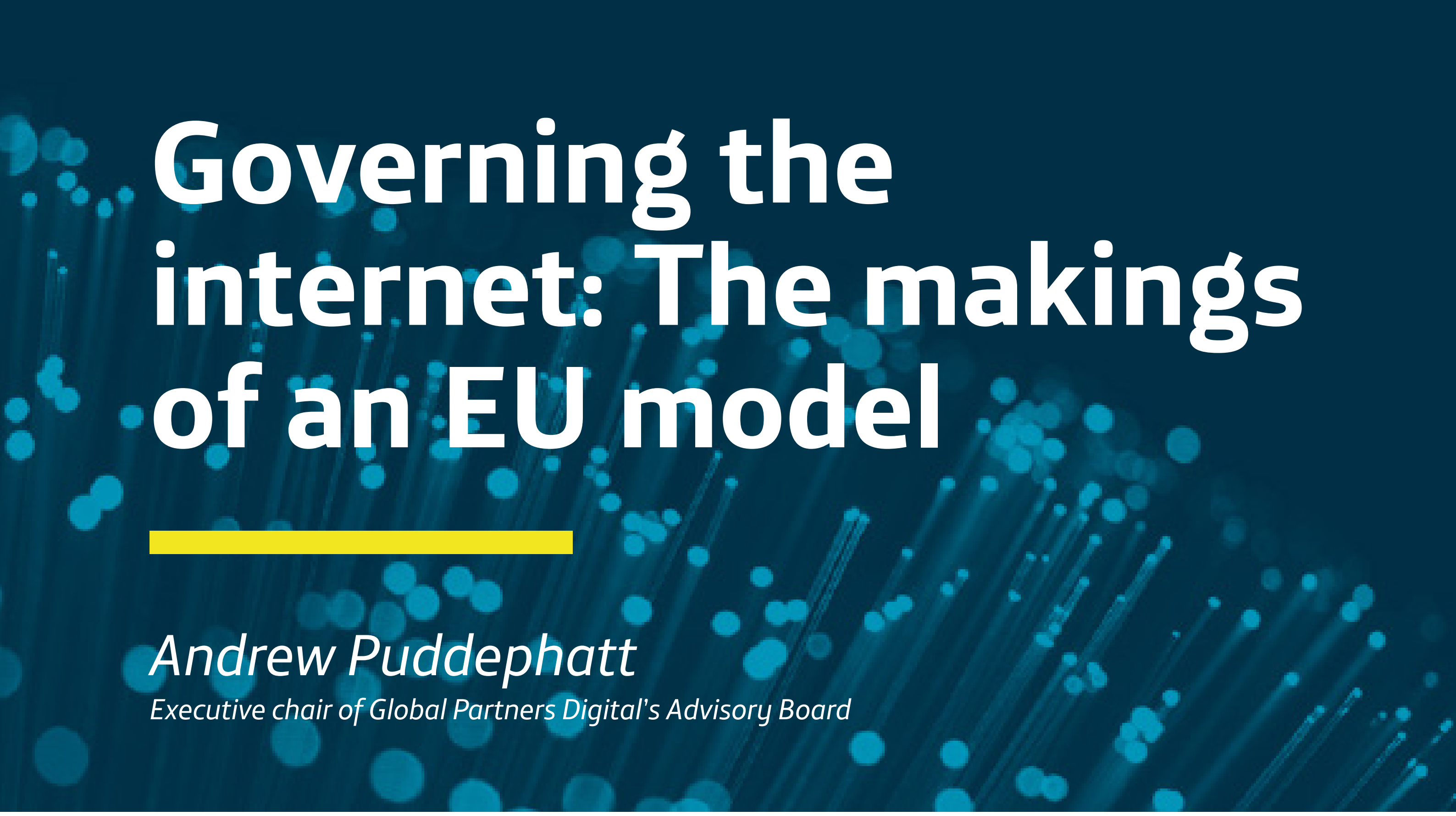
As many of the authors emphasise, the EU's clearest opportunity is **to exercise its regulatory power to shape the international environment** on digital issues. Regulatory power refers to Europe's capacity to leverage access to the EU market, and its developed framework for creating and enforcing regulations, to encourage other states to follow European practice. In the digital realm, the most prominent example of this effort is GDPR (the General Data Protection Regulation), which has forced companies around the world to comply with European practices on privacy and encouraged similar regulations in other jurisdictions, including in various parts of the US. Franke suggests that a similar opportunity exists to exercise regulatory power in the area of AI. She suggests that a focus on creating a European regulatory framework for ethical AI could both inspire others to emulate it and force compliance with European ideas of how to control this industry of the future. Torreblanca argues that Europeans have a similar opportunity to lead in the regulation of digital content.

More controversially, some of the authors suggest that the EU also has an opportunity to **use its competence in competition policy to gain an advantage in some key emerging technologies.** Renda, for example, notes that the coming shift from cloud-domination to distributed data governance, in which the rules for data management are established in the jurisdiction where the data resides, give the EU a competitive edge. Similarly, Richart sees an opportunity to use forthcoming advances in edge computing to bring storage and data flows under European regulatory control. As noted, the record on this type of industrial policy in Europe is very mixed, but the realisation that Europe's digital sovereignty is at stake has inspired a new willingness to experiment.

Finally, some of the authors even see an opportunity in the deepening US-Chinese competition over technology issues. The stark differences between the anarchic US approach to digital regulation and the heavy-handed state control model advocated by China opens a vast middle ground for European actors. Both Oertel and Burwell note that this might provide **an opportunity for European actors to serve as a mediator in US-Chinese disputes.** The role of mediator sits uneasily with the idea that Europeans have their own approach, but, of course, clever use of the position also provides the chance to shape the outcome. Mediation, however, would not usually imply equidistance between the US and China. For all of the complaints about US behaviour in the digital realm, Oertel, Burwell, Renda, and Torreblanca all express deep scepticism about the EU's ability to find the type of compromises with China that it often manages with the US. Although Ortega and Puddephatt appear somewhat more optimistic about working with China, even they indicate that its authoritarian model will pose some serious limitations.

No going backwards

Alas, there is no one to beat the drum for the retreat of digital technology. The competitive struggle for digital sovereignty is thus Europe's – and everyone's – fate. We are marching, for better or worse, to an ever-more digital future, likely full of smarter AI, faster communications, and more sophisticated disinformation. This collection of papers represents an effort to come to terms with that ineluctable fact, but also to realise that it offers Europe opportunity as well as peril. Europeans cannot stop marching, but with some careful thought, difficult political compromises, and wise leadership, they can shape a European digital future.



Governing the internet: The makings of an EU model

Andrew Puddephatt

Executive chair of Global Partners Digital's Advisory Board

In February 1958, US President Dwight Eisenhower set up the Advanced Research Projects Agency (ARPA) in response to the Soviet's Union launch of Sputnik 1 the previous year. The organisation's mission was to make investments in technologies that strengthened national security. Its research into communication systems that could survive a nuclear attack led in 1966 to the creation of ARPANET. Whereas previous communications relied on circuits – dedicated end-to-end technology, such as telephone lines – ARPANET used packet switching. This allowed the system to break data into packets and transmit it via different channels, before reassembling it at the destination point. ARPA developed the transmission control protocol (TCP) and the internet protocol (IP) to determine how data should be broken up, addressed, transmitted, routed, received, and reassembled. The application of these protocols to radio, satellite, and other networks established a system in which data moved through very different media. The term for the approach, "inter-networking", was soon shortened to "internet".

One of the key characteristics of this new technology was that its configuration was determined not centrally but by the network provider. Individual networks connected to one another through a meta-level "internetworking architecture", despite the fact that they had been separately designed and had their own interfaces. In contrast with earlier state-based mass communication systems (such as newspapers, radio, and television), the internet functioned without the need for national or global coordination. As such, internet governance initially seemed unnecessary. Although the internet operated according to rules, they were widely thought of as functional rather than normative due to their technically complex nature.

By the mid-1980s, the internet supported a growing community of academic researchers and developers. It functioned as an informal arrangement between groups of like-minded people who were willing to cooperate to build and develop the network. However, as it grew beyond a few universities, the network needed some management (to create and allocate new addresses, for example). At this stage, the administration of the registries of IP identifiers (including the distribution of top-level domains and IP addresses) was performed by one person – Jon Postel, who was based at UCLA. As his workload became unmanageable, with more countries beginning to utilise the technology, a new system was required. And, as the internet grew into a global network, it became apparent that there was a need for a minimum level of universally accepted technological standards.

Since its inception, the technical governance of the internet had operated outside direct government control – although, in practice, US-based engineers and US-based companies had de facto authority in developing its engineering protocols. Until 1998, internet governance had not been a political issue in Europe. But this changed when the US government pushed successfully to establish the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit organisation that took over Postel's role in managing domains. Governments across the world began to take a view on the issue.

For the US government, it was crucial that the internet was governed by a set of non-governmental and private organisations through ICANN. Washington preferred a market-orientated solution that involved private sector self-regulation of the internet (which protected US economic interests). By contrast, the European Union argued for a public-private system in which governments had an important role – a multilateral institutional framework. China, Russia, and other countries wanted a solely state-based system of internet governance, preferably one anchored in the United Nations. The EU eventually supported the broad US position but secured a role for governments in the institutional structure of ICANN, ensuring that Europeans joined the organisation's committees.

However, such technical arrangements were only one aspect of internet governance. Policy issues were more challenging. As the power of a globally interconnected communication network became apparent, governments began to realise that they were fast losing their control over communication technologies. Internet use increased exponentially, but its lack of overarching regulatory framework meant that what became known as "permissionless innovation" held sway over its development. The internet used existing telecommunications infrastructure – the telephone network – to grow organically, without the need for significant new investment (in countries where there was a robust telephone infrastructure). Anyone could plug their computer into the network and become part of the internet – firms required no permission to launch a service and had no regulatory hurdles to overcome. Accordingly, the internet grew more like an organic ecosystem than a planned network. Collaboration and consensus among providers were widely seen as the key drivers of decision-making.

The internet was born of a libertarian dream. Its early creators and advocates imagined it as a stateless space, outside of government control. Indeed, many believed that any kind of governance would destroy its character. In the early phase of the internet's development, the engineers, technicians, companies, and users who drove the process were content to create a communicative capacity without concern for how that capacity would be used. They did not appear to imagine the harms that could arise from anonymised unrestricted free speech – such as child abuse, trolling, the harassment of minorities, and the propagation of terrorism. The culture surrounding the First Amendment of the United States, which fosters free speech and limits the liabilities of carriers, was crucial to the internet's development. Many of the early innovators and creators of the digital world came from the US, where they could experiment without concern for future liabilities. As an English-language medium that (in most parts of the world) was only available to elites, the internet initially went under the radar of many governments that were inclined to censor and control communications.

By the early twenty-first century, a new era had begun. Governments across the world became alert to the potential disruption caused by access to digital communications, whether from text messaging using mobile phones, the creative use of social platforms such as Facebook and Twitter, the streaming of video direct to the web, or the use of the internet to bypass censorship. Governments increasingly looked for new ways to control and monitor the online space. At the same time, there were growing calls around the world for this unregulated environment to be brought under government control – calls motivated in democratic states by fear of crime and terrorism, and in authoritarian ones by governments' desire to preserve their power.

As the internet grew in size and capability, there was a sharp rise in the capacity of states and non-state actors to use digital technologies to disrupt and control communications, and to thereby undermine democratic processes. Criminal networks exploited these capabilities and corroded trust in the online environment. Repressive regimes used hackers to disrupt pro-democracy and human rights groups. And new communication companies became increasingly powerful. As Timothy Wu has documented, all the dominant media of the twentieth century – whether it be radio, television, film, or telephony – came into existence in an open and free environment. All had the potential for unrestricted use, but all fell under the control of monopolies in time. A similar pattern emerged in the digital world. The internet faced a challenge from both public and private power – and, sometimes, a deadly combination of the two.

Although many governments decry the apparent lack of rules on the internet, there is governance online. Such governance is provided by major companies through their terms of service, community standards, and screening procedures. And corporate algorithms sort, rate, rank, and recommend users' choices, constituting a type of market governance. So, the issue for many governments is not that the internet is lawless but that its laws are made by private companies through their codes and algorithms.

Countries such as China – which attempts to exercise total control over its domestic communications environment – reject any notion of an independent communications network outside of state supervision. The overarching goal of Chinese diplomacy is to promote the notion of cyber (or internet) sovereignty. In the words of President Xi Jinping, this means "respecting each country's right to choose its own internet development path, its own internet management model, [and] its own public policies on the internet." The Chinese model of the internet prioritises control through a broad range of tools and technologies that block, filter, or manipulate online content. It has rules for storing data on servers in-country, which – though Beijing portrays this as a way of limiting the power of US companies – helps the authorities access users' information.

China's desired goal is a long way from the US vision of a global internet run by the private sector. Beijing wants to see a series of interconnected national internets rather than a global infrastructure, with each national internet governed by the laws and values of its home state. It sees the private-led, adoptive model that has shaped the initial growth of the internet as expressive of Western, particularly US, dominance – something that is reflected in the support it receives from a coalition of technology companies and civil society groups. Chinese policymakers want the UN to play a larger role in internet governance, as they believe that they can strengthen their influence through the organisation or other multilateral, state-based forums.

Europe sits between these poles – though, diplomatically, it has usually aligned itself with the US. Internally, the EU and its member states have begun to play a major role in shaping platforms' content rules. In Europe, a vast body of "soft law" (comprising self-regulation, dialogues, and memorandums of understanding), multi-stakeholder initiatives, and co-working forums have helped develop online content policies and practice. But there is no systematic means of incentivising platforms to assess and address problems of harm and illegality that may emerge in their ecosystems – where their commercial incentives to do so are insufficient – or of assessing the effectiveness of their responses.

Approaches to governance

The establishment of ICANN did not settle the question of global internet governance. Concerns about US domination of the internet grew with the significance of the technology. As the internet grew following the invention of the World Wide Web – to include an increasing diversity of languages and content – a small number of US companies began to dominate the services it provided (such as Facebook in social media and Google in search).

The International Telecommunications Union (ITU), a UN body whose origins lay in the development of the undersea telegraph in the nineteenth century, began to lead efforts to govern the internet in the early 2000s – which, at this stage, was mostly carried by existing telecommunications infrastructure.

In response to member states' requests, the ITU convened the World Summit on the Information Society (WSIS) to consider the future of global internet governance, among other things. The WSIS met in Geneva in 2003 and in Tunis in 2005. The latter event came under authoritarian influence: Tunisian government employees who posed as members of fictitious organisations dominated meetings that civil society groups had organised on its fringes. The rancour generated by this overt repression of independent voices in Tunisia undermined efforts to place governments in control of the internet. As discussed above, Washington was determined to avoid anything that suggested such control, a position that EU member states ultimately supported.

This led to the creation of the Internet Governance Forum (IGF) – a multi-stakeholder, UN-based organisation designed to provide advice or, at most, set norms. The IGF has a five-year mandate that has been continually renewed. It principally operates through its annual meeting, albeit while coordinating with working and advisory groups on other occasions. The IGF has established regional and national branches, which meet with varying degrees of participation from local organisations and companies in different countries. Its lack of formal authority was never going to satisfy authoritarian states that have pressed for a system that allows them to control the internet. Accordingly, these states rarely sent representatives to the IGF. And, over the years, high-level attendance by Western governments has dwindled. Major corporations no longer invest significant resources in the IGF, while most of its attendees are from civil society groups.

There are ongoing attempts to promote a more state-based system of global internet governance. The Shanghai Cooperation Organisation – an intergovernmental organisation created in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan – has consistently acted as a vehicle to challenge existing internet governance models. In 2015 the organisation submitted a recommended a code of conduct on information security to the UN General Assembly. Its aim was to promote the rights and responsibilities of states in the information space, and to enhance intergovernmental cooperation by addressing common threats and challenges (which included the those posed by free speech in authoritarian states). This met with opposition from the US and its allies, including the EU.

Geopolitics has increasingly bedevilled attempts to create a global framework for managing the internet. Even on subjects such as cybersecurity – where there is common ground on the need to counter threats such as terrorism, child exploitation, and other serious crimes – it has proved impossible to reach a consensus.

Nonetheless, the concept of internet governance is far from redundant. It has mutated into a series of issues that various actors tackle in different forums. While it might have once made sense to advocate a global framework for governing it, the internet has become part of so many people's daily lives that it affects every area of policy (a trend reinforced by the social distancing policies that have followed the covid-19 pandemic). As the internet underpins most parts of people's working and social lives, such governance issues appear everywhere. In some areas – such as intellectual property – it may be possible to establish a global consensus. In others, geopolitics will block progress, with governance systems devolving to regional and national blocs.

One of the problems with the term "internet governance" is that it holds different meanings for different governments. For some, "governance" means "government" – a ubiquitous communication medium and a strategic asset that requires state control. For others, governance is a purely technical issue – concerning the protocols necessary to ensure that infrastructure works and evolves. For others still, governance should simply focus on mitigating the harms that arise from what is essentially a private sector medium. And then there are those who see it as a way of curbing the power of US (and, increasingly, Chinese) companies that are beholden only to domestic governments.

The EU experience

The EU has a long history of developing internet policy, albeit not in governance. Since the mid-1990s, the EU has been concerned about the potential harms caused by the internet. The EU initially emphasised soft law in its digital policy but, in the last two or three years, has shifted to a more proactive and interventionist approach. Today, the EU has the most developed policy, legal, and regulatory framework on internet issues anywhere in the world.

The EU's power rests upon its economic might. Its single market had a GDP of €15.9 trillion ($18 trillion) in 2018, the largest in the world. Although the United Kingdom's exit from the EU will reduce this to some extent (depending on its degree of market alignment), the bloc will still exert significant authority over companies that wish to do business in its territory. The EU has a lucrative market for internet companies: as of March 2019, an estimated 90 per cent of the EU population used the internet, ranging from 98 per cent in Denmark to 67 per cent in Bulgaria.

The EU initially responded to the internet by recognising its social, educational, and cultural importance, while also acknowledging its potential to disseminate harmful and illegal content, and its capacity to facilitate serious crime. The EU's approach to internet policy evolved to deal with internet service providers that create and run the infrastructure rather than the platforms that emerged in the twenty-first century. In its early years, EU internet policy had two guiding principles developed with the ISPs in mind. One was net neutrality, which required ISPs to treat all online data equally. The other was limited liability, which meant that no ISP could be held liable for hosting illegal content, provided that it removed such content after becoming aware of it. This limited liability provision is contained within the e-Commerce Directive. Articles 13 and 14 of the directive state that, to be shielded from liability, providers that host content must act "expeditiously to remove or to disable access" to information where they have "actual knowledge" of its illegality, and providers that cache content must do so after receiving or an order to that effect.

The rapid growth of US service companies (such as Amazon, Facebook, and Google), their phenomenal market capitalisations, and the lack of any similar European companies that were able to compete with them prompted the EU to rethink its policy. As the value generated by the internet appeared to accrue more and more to US companies, European

policymakers began to question limited liability. Platform companies do not just act as neutral hosts of content provided by others, as they use algorithms to track users' behaviour, and select or adjust content to reflect the needs of these users. In this respect, platform companies resemble editors who are responsible for the content they work on rather than a telephonic services firm, which is not accountable for discussions on its lines. And the opacity of US service companies' algorithms – which they regard as commercial secrets – has made it difficult for outside observers to judge whether they shape or merely reflect the world that users experience on the internet.

The EU is not a major geopolitical player that can impose itself on superpowers. Nor has it created globally significant service platforms capable of exercising influence across the world. But it has one tool that enables it to shape internet governance – the regulations it applies to its market and the requirements it places on companies that wish to trade in the EU. Due to the size and value of the EU market, multinationals want to trade in Europe. In doing so, they are forced to comply with EU regulations.

Other countries observe the bloc's approach to internet governance and replicate the aspects of it that appear to be successful. And, finding that they have to introduce new internal procedures to do business in the EU, companies change their behaviour.

The EU is currently focused on the ambitious goal of creating a single digital market. This is set out in the European Commission's Digital Single Market Strategy, which it estimates could increase EU GDP by €415 billion. The strategy is considerably more interventionist than previous approaches to policy, aiming to establish a harmonised regulatory framework that provides business and consumers with unrestricted access to digital goods and services across the EU. Although its goals are domestic, the strategy has governance implications for any company that wishes to do business inside the bloc.

An example of this is the P2B Regulation, which is designed to promote fairness and transparency for businesses that use online platforms. The regulation comes in response to long-held concerns about the way platforms favour their own services. Although it has not yet been formally adopted, the P2B Regulation reflects a range of concerns about the behaviour of large US platform companies, which it will require to conform to specific standards when operating in the EU market. The European Commission has already fined Google for abuse of its dominant position in the digital-advertising and comparison-shopping markets, as well as for placing restrictions on manufacturers of Android devices. The commission is now conducting investigations into both Amazon and Apple.

Another policy that has attracted global attention is the General Data Protection Regulation (GDPR). This came into force on 25 May 2018 with the goal of protecting EU citizens from online privacy and data breaches. It draws on offline data protection principles but addresses the implications of technological advances. It is designed to protect all EU citizens' data privacy and reshape the way that data controllers in companies across the region approach the issue. Importantly, the GDPR applies to any organisation that holds the personal data of people who reside in the EU, regardless of its location. Under the regulation, the EU can fine organisations up to 4 per cent of their annual global turnover or €20m – whichever is higher – for serious infringements; and up to 2 per cent of annual global turnover or €10m for infringements of their data protection obligations.

Many countries outside the EU are observing the GDPR's development and considered similar legislation. It has even had an impact in the US, with state legislatures considering provisions to protect privacy that closely resemble aspects of the regulation. The EU's Digital Single Market Strategy – which will involve further regulatory controls on digital businesses – is likely to have similar global implications.

Some observers have suggested that the world may soon have three internets. These would be a US internet where the rules set by companies provide de facto governance; a Chinese internet that is nationally controlled, serving the interests of the state and facilitating comprehensive digital surveillance; and a European internet in which the EU acts in the public interest to regulate the operations of digital markets and companies.

Given the geopolitical impasse on internet governance, the debate on the issue will almost certainly shift to national and regional initiatives. The US model is widely seen as furthering the self-interest of American companies (an impression reinforced by statements made by both Democrat and Republican administrations) and the Chinese model is mostly appealing to authoritarian governments. As such, the European model is emerging as one that democratic governments – keen to preserve an open market in digital services while protecting the interests of citizens – find increasingly attractive.

Internet governance will not primarily develop in the IGF, or the UN First Committee, or even the ITU (as important as each of these forums are). It is likely to emerge from detailed, bureaucratic, and painfully negotiated efforts to shape the market and incentivise corporate behaviour – an approach backed by the threat of sanctions. These are qualities that, for good or ill, the EU has in abundance and that are lacking elsewhere.

China: Trust, 5G, and the coronavirus factor

Janka Oertel

Director of the Asia Programme for the European Council on Foreign Relations

The current US-China confrontation is a battle for global supremacy. This contest for influence and leadership is playing out across various economic fields, but most prominently in the technology sector. In the last few years, there has been a lot of talk about the emergence of a new "tech cold war". Yet the analogy can be misleading: it oversimplifies the dynamics at play – and there is nothing cold about it. The confrontation is hot and fierce, and it is playing out in real time. Washington and Beijing are exchanging blows across various battlefields with varying degrees of intensity. Europe has already been caught in the crossfire on 5G – and things are likely to get worse.

Technology supply and value chains were designed to be efficient and profitable through interdependence and highly specialised global production. European companies are an inherent part of this arrangement: they are deeply embedded in value chains and occupy critical junctures in everything from radio access networks to the lithography optics used in semiconductor production. But tech nationalism is on the rise, and the unravelling of existing structures has already begun. The coronavirus crisis is accelerating this trend. In recovering from a pandemic that has hit the world economy hard, states will reorder their interests and priorities. Europe needs to find a new place in the emerging dynamics.

Washington initially failed in its blunt campaign to push its allies to ban Chinese vendor Huawei and its state-owned competitor, ZTE, from the roll-out of 5G telecommunication networks. European leaders, especially those at the heart of the European Union, were reluctant to move decisively against companies that had been important partners for years and were a key part of their 3G and 4G systems. But US policies ignited a sincere debate across the EU about the future composition of telecoms infrastructure and, as a result, relations with China more broadly.

American officials argued that Chinese vendors posed an unmitigable security risk to Europe's communications infrastructure and the backbone of the interconnected reality of the 5G world. However, Chinese tech champions – especially Huawei – embodied the strengths of a tech ecosystem that could rival Silicon Valley's. They often did so by benefiting from massive state subsidies, favourable domestic market conditions in China, intellectual property theft, forced technology transfers, and enormous amounts of state-backed capital for research and development – which boosted indigenous innovation.

Washington has huge incentives to slow the erosion of US tech dominance and the broader power shift towards China – especially in the midst of a pandemic that has shut down much of the US economy. Unemployment in the United States is at a historic high, and the health emergency will likely be followed by a recession. To minimise China's relative gains, the US administration is willing to maximise economic pressure on Beijing.

In May, the US Department of Commerce presented the latest in a long line of measures designed to achieve this: tightened restrictions on microchip sales to Huawei and its subsidiaries. With the move, the department's Bureau of Industry and Security (BIS) dealt a massive blow to the Chinese tech champion. This was quickly acknowledged by Huawei, which stated that it is now fighting for survival.

The BIS decided that, beyond placing restrictions on direct sales to Huawei, it would also require the company to apply for licences for purchases of semiconductors that are "the direct product of US design and technology". Semiconductors are both critical to Huawei's supply chain and one of the few remaining chokepoints for China's tech ambitions, as the country's capacity to mass-produce them is limited to just a few companies. Thus, the latest legal manoeuvre especially targets Taiwan Semiconductor Manufacturing Company (TSMC), which accounts for more than 50 per cent of global sales. The company has moved to the centre of the US-China confrontation, as Huawei needs access to high-performing microchips to fulfil its 5G ambitions. For years, the most compelling argument for Huawei has been that it can provide high-quality goods quickly and at a low cost. It has now become much more difficult for the firm to do so.

The full implications of the BIS decision are still unclear; there may be loopholes in it. But, with this latest salvo against the Chinese tech sector, Washington has emphasised that it takes the issue very seriously. And the current crisis plays into this, given US fears that China will capitalise on its opportunity to end the coronavirus-induced economic lockdown earlier than other countries.

China is an economic competitor that is exiting the first phase of the pandemic earlier than others due to the authoritarian nature of its regime, its high degree of digitalisation, and its existing surveillance structures, which extend to the neighbourhood level. These structures, which predate the digital age, have the capacity to control limited outbreaks more successfully than those in the West. Even during the height of the health emergency, strategically important sectors – including the indigenous microchip industry – continued to operate (even if at slightly limited capacity). And, by now, the tech sector has almost returned to its pre-crisis productivity level.

The Chinese leadership has announced initial stimulus packages to make up for the economic losses created by the lockdown, putting 5G roll-out and the construction of data centres at the heart of these measures. The nationwide introduction of 5G with up to 600,000 base stations – announced in late March – could give Chinese companies a huge competitive advantage over their rivals in their push to digitalise the economy. And more is to come: China is set to spend $1.4 trillion on boosting its tech sector over the next five years.

While it currently intends to approach licence applications under the presumption of denial, the BIS could still issue them to TSMC for limited production. This could be necessary to ensure that the company remains competitive, as sales to China make up almost 20 per cent of its business. Huawei has long expected US-China relations to deteriorate and almost certainly has a significant stockpile of the most critical supplies but, in the fast innovation cycles of the tech sector, these are only useful for a limited amount of time. And it is unclear how long supplies will last, or how quickly Chinese companies will be able to provide indigenous solutions to the problem. Even though the Chinese government places a huge emphasis on such solutions (and is investing a lot of money in them), it will have no real alternatives to non-Chinese products on the necessary scale in the short term.

The latest move by the BIS will make Huawei less international and more Chinese. The company will need to prioritise the enormous domestic 5G market – even at the expense of customers elsewhere. Accordingly, Huawei's ability to fulfil contracts has become another important consideration for European operators and governments as they decide on the composition of their new network infrastructure. Reliance on Huawei could be a gamble in terms of not only politics and security but also economics.

The European 5G debate

At various times in the last few months, commentators in the media have argued that European telecommunications operators will not exclude Chinese vendors, implying that the US has lost the battle over the issue. But, in reality, the debate is far from over and will be heavily influenced by the coronavirus. In late April, EU member states were supposed to report on the measures they had taken to comply with the EU's toolbox, a landmark set of policy guidelines for securing 5G networks in their role as critical infrastructure. Virtually all EU member states have complied with this request. But few of them have made a final decision on the role of high-risk vendors.

There is a pending debate on the topic in the Netherlands, where operator KPN has announced that it will swap from Ericsson to Huawei in maintaining its radio access network. Several European countries have introduced national legislation in the area. For example, French restrictions on Huawei's and ZTE's equipment in the core of the mobile network predate the 5G debate, while Sweden and Estonia have taken a case-by-case approach to Chinese firms that involves

the security services. All of them place significant restrictions on Chinese vendors in their networks, but they also still allow for a degree of strategic ambiguity. Denmark is likely to adopt a restrictive approach soon. Announcements pointing towards the exclusion of Chinese vendors have been made in Romania, the Czech Republic, Italy, and Poland. But the legislative processes to that effect are unfinished – and, for example, in Poland, heavily contested. This has sometimes led to delays in spectrum auctions.

The most technologically and intellectually sophisticated approach to the problem has come from the United Kingdom's National Cyber Security Centre. In contrast to its continental European counterparts, the organisation has years of experience in analysing Huawei equipment in a very in-depth fashion, and has been alert to the impending security risks for more than a decade (in relation to 3G and 4G). The UK has taken the most decisive step in Europe by banning ZTE outright, and by proposing significant limitations on Huawei's future role in its 5G infrastructure.

With the pandemic prompting calls to reassess supply chains for critical goods, some British MPs have increased pressure on the government to apply further restrictions on Huawei. This is likely to lead to a controlled phase-out of Huawei technology in the next few years, an example that many European governments may follow. Somewhat counterintuitively, Norway – another country just outside the EU – has received little attention for its main operators' decision to roll out 5G technology without Chinese equipment.

Germany, above any other EU member state, is key to the outcome of the debate in Europe. This due not only to the size of its telecoms market – which is the largest in Europe – but also to its special relationship with China and the significant presence of Huawei and ZTE equipment in its existing infrastructure. The German debate has been fierce, with the government split on how to respond to the challenge – interestingly, not along party lines of the grand coalition, but between those focused on foreign, security, and cyber issues and those who mainly deal with the economy. Germany's IT security and telecoms laws were both due to be updated early this year. Yet, so far, only a first draft of the changes to the IT security law has surfaced. The preliminary version includes a clear reference to the EU's 5G toolbox and calls for non-technical factors, such as trustworthiness, to be relevant in the assessment of a vendor. But it remains unclear in how Germany will assess the trustworthiness of suppliers.

A question of trust

Trust in China has become a huge issue for Europeans. Beijing's attempts to withhold information about the outbreak of the coronavirus and its initial management of the crisis have received widespread international criticism. Simultaneously, China's assertive attempts to shape the global narrative on the pandemic through so-called mask diplomacy or outright intimidation demonstrate that its communist leadership – with its back against the wall – has little time to play nice with Europe. China is focused on solving the domestic economic problems that the pandemic has created, including massive job losses, through increased spending at home.

Europeans seem to have been put on the back foot by Beijing's new approach. Although Europe made a significant course correction in its overall assessment of China in 2019, their relationship is now deteriorating with incredible severity and speed. The pandemic will have a lasting impact on China's image in the world. And, even more so, it will shift the techno-nationalist Chinese leadership's attention inwards in ways that make mutually beneficial cooperation increasingly unlikely. China will push to further decouple from international suppliers, prop up its domestic champions, and reduce its dependencies.

For Europe, the timing could not be worse. The post-pandemic economic outlook is bleak. The recovery will be bumpy. As the pandemic lockdown has demonstrated, there are deficiencies in the digitalisation of even Europe's leading economies. Investment in digital infrastructure, with a special focus the swift introduction of 5G, seems like an especially reasonable way forward. The overall economic situation could make telecoms operators more inclined to choose the cheapest available option. As Chinese vendors already permeate the European market for telecoms infrastructure, they could easily make an economic case for greater reliance on them.

But the countervailing argument may weigh more heavily: the pandemic has made clear that dependence on China for the supply of critical goods (such as masks and personal protective equipment) puts European governments at the mercy of the Chinese Communist Party in times of crisis. The coronavirus has revealed the importance of critical infrastructure to European citizens. And dependence on China has become part of the public debate across Europe, while scepticism about the country's reliability as a business partner will affect the political climate in most European states for months, if not years, to come. As a recent poll by the Körber Foundation shows, 85 per cent of Germans seek to reshore production capabilities and critical infrastructure to enhance crisis resilience – even if this comes at an economic cost.

It is troubling that, on basic digital infrastructure, most European countries are not up to speed in the truest sense of the word. This could damage Europe's long-term market position. As 5G will become an enabling technology for a new digital ecosystem in the next five to ten years – as it reaches its full functionality – Europe will need to support its major firms in the market by protecting them from unfair competition and Chinese takeovers. In this regard, EU regulation is advancing and has proven to be a powerful weapon in a battle that no member state can win by itself.

Coronavirus choices

The coronavirus crisis is a turning point for Europe's approach to technology and geopolitics. By seizing the moment for an economic rethink, the continent should make a renewed push for European solutions to challenges that are indifferent to the borders of the nation state – pandemics and cyber threats being the most prominent, but certainly not the only, examples of this.

Connectivity has been a buzzword in Brussels that never really caught on in the public discourse. Now that citizens have experienced the disastrous consequences of a breakdown in the international connections they rely on, digitalisation could take centre stage in their efforts to recover from the crisis. Europe needs to find a way to not only pay down debt but invest in future competitiveness.

Beijing will move swiftly while the rest of the world grapples with the crisis. And this will not be limited to domestic policy. It is also likely to entail a renewed focus on digital connectivity as part of its Belt and Road Initiative, as well as enhanced efforts to build a digital international order that caters to the interests of the Chinese Communist Party. EU member states need to adjust to this new environment as they make decisions on the economic recovery.

European discussions about technological sovereignty are an important first step in this direction. It is necessary to find pressure points through which to influence the debate on the issue and move from reaction to action. European companies that are part of global value chains are dependent on a rules-based order and commonly defined standards. Before the escalation between the US and China of the last few years, most Europeans had little awareness of the potential limitations they faced in access to technology, research, and innovation. Their commitment to deep integration and networked thinking left little room to consider vulnerabilities among all the opportunities. One could have foreseen the dynamics that have unfolded in recent years, but it seems that Europe needed a rude awakening from

its deep geopolitical slumber to understand how the world around it is changing.
There is a persistent myth that Europe does not have what it takes to prevail in the tech world of the twenty-first century and, therefore, can only choose which masters it will serve – be they in Silicon Valley or in Shenzhen. Europe does not currently field a competitor to big US players Amazon, Facebook, and Google or their Chinese equivalents Alibaba, Tencent, or Baidu. But Europe has what it takes to become a force to be reckoned with in the tech space. The continent has 6.1 million developers (compared to 4.3 million in the US) and multiple tech hubs – from the classic top three of London, Berlin, and Paris to the vibrant centres of Stockholm, Amsterdam, Barcelona, Dublin, Helsinki, and Madrid.

Members of the EU have an especially significant long-term advantage in the freedom of movement of humans and capital across their borders with one another, as well as their common regulation and their increasingly appealing investment climate – given the unpredictability of US and Chinese policies and market conditions. The European Commission has set out ambitious targets to ensure that Europe not only has a powerful market but is also a leading innovator in technology. To hit these targets, the Commission will need the full support of all member states and new partnerships with like-minded players, such as Japan, Australia, and South Korea.

As the volatile US-China relationship changes almost daily, Europe urgently needs to build up its resilience against external shocks. Washington and Beijing are considering several extreme measures related to technological decoupling that, aside from their security implications, could throw global supply chains into disarray. These include potential US sanctions on Chinese companies that trade in US dollars, as well as Chinese threats against the status quo in the Taiwan Strait. If the developments of the past two years have demonstrated one thing, it is that such high-risk, low-probability scenarios deserve far more attention than they received in the past.

The view from Spain: The EU's bid for digital sovereignty

Andrés Ortega

Senior research fellow at the Elcano Royal Institute, an independent consultant and director of the Observatorio de las Ideas

The idea of European digital sovereignty suggests the control by Europeans of their economic environment – in this case the digital environment – even when there is a high level of interdependence. It is always a relative concept.

The coronavirus crisis will impact on its fate in two ways. On the one hand, the pandemic has made it clear that Europe – the European Union and its member states – is overdependent on supplies, both in technology and health, from China and other countries; something that Spain, one of the countries that has suffered greatly from covid-19, has experienced first-hand. The process of deglobalisation and greater nationalism that it has accelerated will lead to a greater effort to control – in some cases to reshore, or even to nationalise or "Europeanise" – parts of supply chains.

On the other hand, the consequent economic crisis will lead to a greater financial focus by EU member states and institutions on reconstruction. And this reconstruction has to lead to more investment in research and development (R&D) in the digital field, even at a time when there will be great pressures on EU and national budgets. If European countries – including Spain, which lags behind in R&D spending – want to compete with the United States and China in this strategic field, they need to increase public and private investment. This has to be part of the industrial and commercial strategy of the EU. The fallout from the crisis will also lead to a rethink of the need for 'European champions' and a consequent revamp of EU competition policy. Seen from southern Europe, those champions cannot just be Franco-German. It can begin from a Franco-German initiative, as with GAIA-X or the virtual network for artificial intelligence (AI). But to be truly European, those initiative must include other member states, not just France and Germany.

When the Spanish philosopher, José Ortega y Gasset, famously wrote in 1911 that "Spain is the problem and Europe the solution," he was thinking mainly about science and what we now call technology. "Europe is science above all else," he said. More than a century later, we could say that Europe should be science and tech above all else. Moreover, Spain's efforts in this field have a distinctly European ambition, in the sense that Spain, alongside other EU member states, is too small to compete by itself, and, in some ways, even to cooperate, beyond being a client or a user, with the US and China. Even the US is too small in many senses, and should cooperate more with the Europeans in this field.

Spain is an advanced economy which dominates some technology sectors and has some leading research centres. But investment in R&D is inadequate in Spain: it shrunk in the years of the "Great Recession" and only began to recover afterwards. Moreover, it still trails GDP growth. We will see what happens now. Total public and private investment in research, development, and innovation stands at 1.24 per cent of GDP (2018), down from 1.4 per cent of GDP in 2010 but still below the EU average of two per cent. In 2016 and 2017, the private sector increased its R&D investment by 3 per cent. While this is positive, public sector investment fell by a similar amount in 2016, totalling €3.260m. Unlike other countries, Spain, despite having a "State Plan of Scientific and Technical Research and Innovation 2017-2020", does not have a defined general strategy on what its priority technology sectors should be, in general and with respect to China. As a country, Spain still needs to outline a technology and digitalisation strategy. This has to be part of a wider new industrial policy, especially given the manner in which the coronavirus crisis has shown the importance of digitalisation in keeping the economy going during lockdown, and the fact that countries with a strong industrial sector, like France and Germany, have better weathered such a crisis.

Spanish and other European firms complain that they are in a situation of excessive, even "neocolonial", dependence, on the big US and Chinese digital companies. The notion of European digital sovereignty would thus constitute a form of liberation for the tech field, even if cooperation with these US and Chinese companies is unavoidable and desirable. Spain now views its European policy in a pragmatic way. In the tech and digital field Spain would benefit from more funding from the EU and stronger industrial alliances with European countries and companies. It hopes that such opportunities will grow with the policies being put in place in the EU through the Next Generation EU recovery fund and the union's seven-year multiannual financial framework budget for 2021-2027, in which digitalisation and sustainability will be priorities. This could lead to greater Spanish involvement to push for greater European autonomy.

But while pursuing a European approach, Spain sees cooperation with US tech firms as both necessary and unavoidable. It views cooperation with China similarly, albeit it wants to see a greater degree of equilibrium and reciprocity on both the EU-China and Spain-China bilateral fronts. The "EU-China 2020 Strategic Agenda for Cooperation" adopted in November 2013 covers cooperation in science and technology. It was renewed in 2017 to emphasise innovation, the cross-border transfer of R&D results, and greater reciprocity in access to research centres; demands the EU had made since 2016.

For Spain, Latin America provides an added dimension to its tech relations with China. We could talk about a "technological triangle". This dimension, especially the digital one, features at the Ibero-American Summits. China is also very present in the region, with investments and trade, albeit mainly in raw materials, but also interests in the tech field. For this reason, Spain's approach to Latin America will also have to take into account China and its technological involvement in the region. This can be seen in the example of technological cooperation between Spanish, Chinese, and Latin American companies and research centres. There is thus a technological relationship between Spain and Latin America, another between China and the region, as well as one between China and Spain. This "technological triangle" could prove interesting and benefit each of its three elements.

On 19 February 2020 the European Commission issued three major initiatives, which were generally welcomed by Spain: a statement concerning Europe's digital future, a white paper on AI, and a "European Data Strategy". These outlined the major priorities in this field for the commission's term, and have been supplemented by other post-covid statements, like the European Council's "Shaping Europe's Digital Future". The commission's announcements led Andrea Renda, of the Centre for European Policy Studies, to welcome the dawn of "Digital Independence Day" in Europe. This is debatable. While the impact of the coronavirus is going to force changes in these strategies, the commission had initially earmarked an annual budget of €20 billion for European AI. Even if it generates a multiplier effect, by way of comparison, Alphabet, Google's parent company, spends more annually on its R&D. To be effective and credible – to end the notion of "digital neocolonialism" (or "techno-oligopolist dependency") –European digital sovereignty must be matched by sufficient European resources.

In 2000, when it approved the ill-fated Lisbon strategy, the EU set out to become "the most competitive and dynamic knowledge-based economy in the world" in ten years. Twenty years later, the less ambitious goal is "to become a global leader in innovation in the data economy and its applications". The US does not control America's big tech companies, although the Chinese Communist Party does wield control over Chinese corporations. But the fact is that, according to Forbes, none of the ten largest tech corporations in the world is European. Brexit could also impact on the weight, research, and innovation capacity of the EU, as the United Kingdom is one of the most advanced EU countries in this field of research and development. Learning to speak the "language of power" and of geopolitics also entails the EU acquiring capabilities and instruments, and not only of the military kind. A practical example would be that, before the current European Commission's term is up, at least two European companies feature among the top ten in the tech field. Given that this is not going to be a European search engine or a company comparable to Alphabet, it will be necessary to invent other things, hence the commission's proposals to focus not only on the immediate future but to look beyond it.

Capabilities and regulation: AI, data, and web-based services

According to a report by the Centre for Data Innovation which examined six metrics – talent, research, development, adoption, data, and hardware – the US "still leads in absolute terms". China is in second place – although, in future years, it may take the top spot – with the EU behind both.

There are some crucial aspects in which the EU, including Spain, trail the US and China. The commission documents outline some approaches to follow with regard to them. The first is AI, a cross-cutting technology that is already changing the industrial, and personal, landscape. It will flourish with the advent of technologies such as deep learning, neural networks, and 5G communications. As Anthony Mullen, an expert with the IT consultancy Gartner, has stated: "Right now, AI is a two-horse race between China and the US." Europe is a battleground – but to be battleground between two superpowers does not entail sovereignty. Quite the opposite.

Europe could become dependent on AI, and other technology, models that it does not control. Partly in response, the European Commission is designing a European AI strategy. Spain is also drawing up its own, but this work has been delayed due to changes in government and subsequently the covid-19 crisis. There is a general view that Europe is too far behind for the first and even second generation of AI, and it should concentrate on the next generations.

According to the commission, the success of EU-level work on AI rests on three pillars: an increase in public and private investment in AI; preparing for socioeconomic changes; and ensuring an ethical and appropriate legal framework. None of these pillars can be built by governments alone; instead, they require a combination of actors – governments, regions, European institutions, firms, and academia, for instance – working together across Europe.

The bilateral Franco-German cooperation treaty agreement signed in January 2019 creates a joint virtual research and innovation centre for AI and a digital platform for audiovisual and informational content. While such cooperation is welcome, it is neither comprehensive nor does it speak for Europe as a whole, even if both governments support the commission line. Spain would like to join the Franco-German effort in this field but is looking for a more European approach.

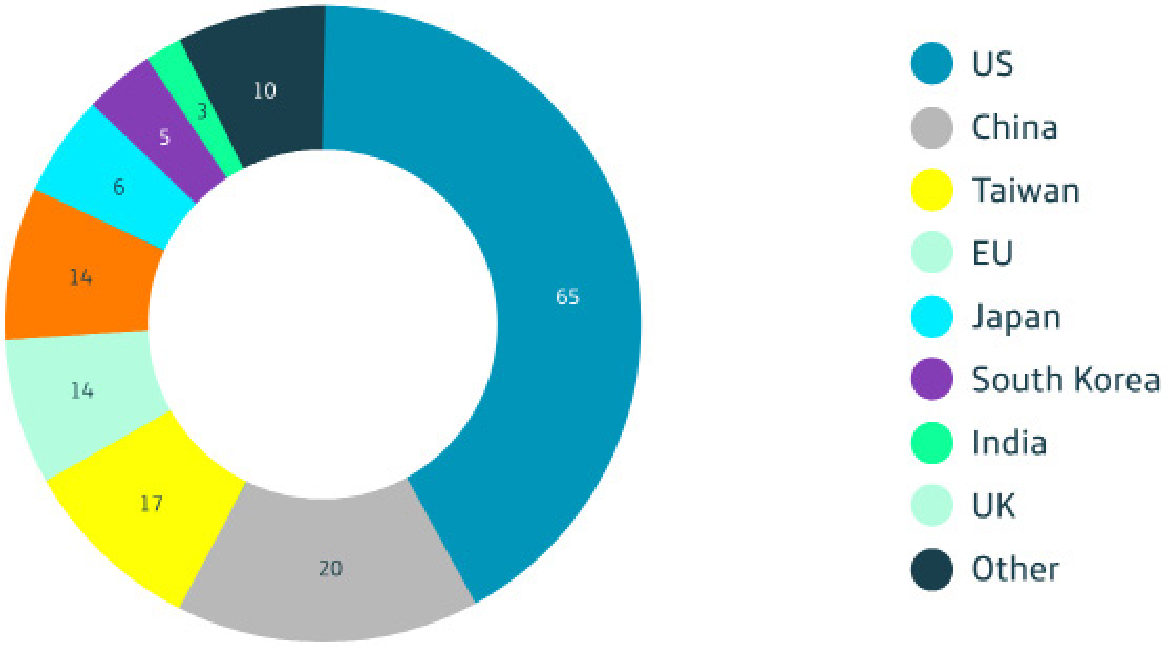
Big data and data services are another space for sovereignty. The "European Data Strategy"– which is closely related to AI – aims at "creating a single market for data that will ensure Europe's global competitiveness and data sovereignty". "Common European data spaces," it suggests, "will ensure that more data becomes available for use in the economy and society, while keeping companies and individuals who generate the data in control." This is also a way of ensuring that European data is controlled (and monetised) by European firms under European rules. That is why the commission is putting an emphasis on, and introducing financing for, European clouds and data centres. At present, these are overwhelmingly owned, even in Europe, by American companies (with China progressing in the data services market). But Europe is behind because of local, national, and European rules. China, for instance, can integrate all its immense data on medical issues, thanks to the sovereignty it exercises over the whole realm of data in its territory. The US comes somewhat close to being

able to do so. Europe, though, is far behind; it is not able to take advantage of its size because of the compartmentalisation of its data, and the priority it gives to privacy.

There are three main ways of approaching data control. In the US, major companies such as Facebook, Apple, Netflix, Google, and Amazon have access to large amounts of consumer data and monetise them, and offer large cloud services. In the EU – thanks to the GDPR (the General Data Protection Regulation) – citizen and consumer rights are a priority, potentially at the expense of the competitiveness of companies, countries, or particular sectors. China has a very different model: technology is sponsored by the state and the government exercises the power to acquire citizens' data. The choice between these three models will have tremendous implications for the future of the global economy and for geopolitics.

Regulation, which is intimately connected to this, has now become a major field of geopolitical confrontation. As Anu Bradford cogently argues in her recent book, "*The Brussels Effect*", Europe sees itself as a regulatory superpower.[1] It has had relatively global successes in terms of imposing its standards, for example in the field of data protection (through GDPR) and road vehicle safety, and it will soon do so again through taxes on carbon and digital commerce. It now wants to repeat these successes in AI and data, among other areas. That said, it is unlikely to maintain such sway unless it preserves or increases its capabilities. As Guntram Wolff rightly points out, "referees don't win" matches. There needs to be a dialogue between Europe and the US on the subject of regulation. That dialogue's main aim would not need to be achieving identical rules, but to attain interoperable systems that can work together. A good example could be the covid-19 tracing apps developed on a common system (Application Programming Interface – API) jointly by Google and Apple. All the same, this unusual collaboration between the two tech giants was not well received politically by some Europeans, especially as the duo together have over 90 per cent of the market of operating systems. Indeed, the commission responded with some guidance to be respected, by that and other systems, to preserve "European values". Some member states, like France, opted for other systems.

Location of the world´s largest tech companies



Source: Forbes

[1] Anu Bradford, The Brussels Effect (Oxford: Oxford University Press, 2020).

Web-based services, including e-commerce, could be the next battleground, not only between the US and China, but also between Europe and the US, and, eventually, China. America dominates the field (which includes the aforementioned cloud services) through a few big tech companies, such as Amazon, Alphabet, Microsoft, and Apple, plus, on a lesser scale, the likes of Netflix and HBO. Although China has its own big tech companies – for instance, Tencent and Alibaba – and is trying to penetrate the European market, US-Chinese competition has so far been limited.

In web-based services, as in AI and data, Europe is lagging and dependent on US and Chinese systems. With some small exceptions, like Spotify, it lacks the ability to create large enough companies in this field. In that sense, the industrial strategies of France, Germany, and the new European Commission will be vital. Cooperation between European and US companies remains inevitable and essential if Europeans want to stay relevant for the next tech generation.

If they cannot catch up, EU member states and companies could end up having to choose between US and Chinese web-based services. Although there is a choice to be made on economic grounds, it does not really exist on the political level since China's tech-related values and behaviour differ so much from those of the West. Still, Europe's governments and institutions do not want to be caught in the middle of a tech decoupling of the US from China. Some selective decoupling seems inevitable and Europe is keeping Chinese tech at arm's length, even while it seeks to avoid a cold war, including a technological cold war. Europe, in the tech field (as in other fields), does not want to have an equidistant relationship with Washington and Beijing – too much joins Europeans to Americans – but neither does it want to be caught between the US and China. Instead, Europe wants and needs to have a different kind of relationship with both. Could competition in these areas lead to a US-European anti-China tech alliance; one that others might join? It could possibly do so, but that alliance cannot come at the price of Europe's own technological development.

The battles for 5G

The case of 5G illustrates well the complexity of the issues Europe, and Spain, face with regard to digital sovereignty. Such technology is crucial because it underpins a series of other industries and will process huge amounts of information between people, companies, government, and machines (Internet of Things – IoT). The race for 5G dominance will probably be the most important one of the next five years. Europeans, and particularly Spain, relied much on Chinese technology for 4G (mainly Huawei, but also ZTE). They were heading in the same direction for 5G, as the cost differences were significant. Late in the game, however, the US – which did not itself have companies involved in the making of 5G equipment – perceived a security and economic threat from this reliance on Chinese technology. The US pressure was somewhat successful, even if America also wanted Europe to rid itself of Chinese 4G equipment; an aim that was not financially viable for companies.

Spain's government and companies are now following the European way – which is, in reality, the British way – of not having Huawei hardware or software in the "core" functions of 5G but only in the secondary, peripheral, ones. Even the UK is tightening its position and should influence in that sense other European players. In October 2019, the European Commission and the European Union Agency for Cybersecurity Cooperation Group published a public report stating that "threats posed by states or state-backed actors are perceived to be of [the] highest relevance" for the 5G system. This will "in turn increase the number of attacks paths [sic] that could be exploited by threat actors, in particular non-EU state or state backed actors, because of their capabilities (intent and resources) to perform attacks against EU member states telecommunications networks, as well as the potential severity of the impact of such attacks." The report did not single out any country or company; it aimed to serve as a basis for the preparation of a series of risk-mitigation measures.

The commission has recommended that EU member states exclude "high-risk" suppliers from their networks. Europe has two companies – Finland's Nokia and Sweden's Ericsson – which are capable of manufacturing equipment for 5G networks, and competing with Huawei and other Chinese companies (like ZTE), albeit at a higher cost. South Korea's Samsung is also a contender. But beyond 5G, the European Commission now intends to focus on, and not lose, the next race towards, 6G.

Europe is still searching for a certification strategy to prevent backdoors (hidden points of entry for spying or attacking). This is easier for 5G hardware than for software, which is constantly updated with security and other kind of patches. A European certification authority, at least for the core hardwares, would be the right solution, but some member states prefer a national approach.

In Spain and in other countries, there is worry about the lack of 5G suppliers: in the last decade this has fallen from 15 to just three: Huawei, Ericsson, and Nokia (plus some niche suppliers). This situation distorts price competition. The bigger and cheaper supplier is Chinese; the European ones are pricier. This applies not only to the European market, but also to others like Latin America. Spanish companies like Telefónica, as well as other European firms, are also very much present in Latin America where investment in Huawei 4G and then 5G technology has been important, but where more competition in terms of hardware and software for 5G would be welcomed.

In Spain, there is a perception that US opposition to Huawei is driven by a desire to win time for some of its major companies – such as Cisco and Maverick – to develop an industrial base for 5G equipment over the course of the next year, perhaps by acquiring one of the two European companies. More competition may be welcome, but this could come at the cost of undermining the European 5G industrial base, given that Ericsson and Nokia are already more expensive than Huawei. There is thus a contradiction between greater competition, providers, and European sovereignty.

Defence against undesirable takeovers

The fears around additional takeovers of strategic European companies by undesirable investors (whether from China or the Gulf) have grown with the economic fallout from the coronavirus crisis. But they were there before. This is also part of the sovereignty argument. The "Sputnik moment" came in 2017 with the acquisition of Kuka, a German advanced robots manufacturer, by the Chinese appliance maker Midea. In response, Margrethe Vestager, the EU competition and digital commissioner, said that European states should buy stakes in strategic companies to stave off Chinese and other takeovers. The European Commission has, moreover, urged countries to toughen their vetting of foreign takeover bids, warning that the coronavirus pandemic had left the bloc's "strategic assets" vulnerable to acquisition from abroad. Phil Hogan, the commissioner for trade, said that Brussels was ready to take on a central role in coordinating monitoring and information sharing. "Economic vulnerability could result in a sell-off of critical infrastructure or technologies," he warned. Even before the crisis, the previous commission was designing a plan for a €100 billion European sovereign fund that could invest in strategic sectors where the EU lags behind global rivals and that could intervene to protect those sectors, by, for instance, buying relevant companies when there is no European capital available. It is, however, unclear whether the new commissioners will push this plan forward.

Although the Spanish government, and others, encourages greater Chinese investment, it also supports greater strategic scrutiny or review by the EU. And with the economic impact of the coronavirus crisis, Spain (like other European countries) has taken measures to prevent strategic companies from falling into undesirable hands. We could even see temporary nationalisations to prevent it.

Brussels is looking to reinforce a system of information-sharing on investment screening that governments agreed on last year. The system was set to be active in October 2020, but the European Commission now wants member states to move faster and further. Spain is one of 12 EU members that has a national security screening system. Madrid is more careful about strategic investment after the 2017 acquisition by China Ocean Shipping Company (COSCO) Hong Kong of 51 percent of the container ports of Bilbao and Valencia.

Strategic competitors and sovereignty

Europe, including Spain, wants and needs to keep doing business with China and does not wish to completely extricate itself from China's technological ecosystem nor to disengage from it and its economy. As a result in March 2019, the European Commission, in a statement that was later supported by the European Council, announced a policy that acknowledges that "China is, simultaneously, a cooperation partner with whom the EU has closely aligned objectives, a *negotiating partner* with whom the EU needs to find a balance of interests, an economic competitor in pursuit of technological leadership, and a *systemic rival* promoting alternative models of governance [italics added]." The four qualifications go together.

But Europe also sees itself in a different competition with the US, one that, as we have seen, has been described as "neocolonial" in the field of digital. Angela Merkel, Germany's chancellor, has supported the idea of digital sovereignty, and competition with Silicon Valley, when, for example, urging Europe to seize control of its data from US tech giants. The information economy and tech competition are clearly becoming central to the EU-US relationship, although, as has been seen, Europe is not equidistant from the US and China, and has to rely on American big tech companies.

Many countries in Europe – for instance, Germany, France, and the Nordic states – have strong technological cooperation with China. This is less the case with Spain, although this is changing. Scientific and technological cooperation between Spain and China has great potential to develop, to the benefit of both countries. But it requires a less competitive and more cooperative approach

and a similar attitude in both countries towards technological agreements. Spain also needs to develop a specific strategy for its dealings with China, both in general, and in the technological field in particular. Spain wants to act within the framework of Europe-China relations, but also to promote an institutional bilateral framework. Spain thus still needs a clearer strategy for scientific and technological cooperation with China.

Conclusion

European integration was not a dilution of sovereignty, but rather a **sharing of sovereignty** to create greater collective sovereignty. This is a notion that is not well received in Beijing and Moscow. In "*The European Rescue of the Nation-state*", Alan Milward argued in 1993 that European integration had served to strengthen the member states[2]. This is no longer true, and therefore, for a country like Spain, it is necessary to move on to a truly European approach in terms of technological policy in general, and in particular towards China. In terms of digital and tech issues, Europe does not want to be caught in a position defined by competition between the US and China. But even if it will not opt for equidistance between Washington and Beijing, it needs to have tools to reach some kind of relative digital sovereignty or at least autonomy. To achieve that, it should encourage greater public and private investment in the next generation of AI; web-based services, including data; semiconductors; and 6G. This would not only foster growth but also help Europe to become, as it needs to be, more autonomous in a post-covid-19 world.

[2] Alan Milward, The European Rescue of the Nation State (Oxford: Oxford University Press, 2020).

US-EU relations: A post-covid transatlantic digital

Frances G Burwell

Distinguished fellow at the Atlantic Council and a senior director at McLarty Associates

The coronavirus outbreak in spring 2020 was devastating for many individuals, societies, and economies. But it also had a significant impact on the state of the transatlantic relationship, heightening levels of misunderstanding and distrust even as both the United States and Europe were jointly facing tens of thousands of fatalities. Donald Trump's sudden restrictions on Europeans travelling to the US, and his threats to cut off funding to the World Health Organization during the pandemic, were unpopular across Europe. Many in the US policy community saw the raising of internal EU border controls, and the struggles to agree to financial support for all of Europe, as emblematic of the European Union's inability to cope with the virus – and potentially as the death knell for the union itself.

But in both the US and across Europe, the covid-19 experience also made clear the importance of the digital world. With millions working from home and sometimes quarantine, and connected to friends, family, and colleagues by the internet, the importance of digital policy for the modern economy was starkly clear. Even as misinformation about the virus spread across social media, governments turned to potential tracking apps and analyses of medical data to find a way out of lockdowns. At the same time, countries such as China and Russia used the internet to spread falsehoods and to increase surveillance of, and even control, their populations. The virus sharply revealed the differences in governmental approaches to the internet and their citizens.

But with this new awareness, will the US and EU be able to use the covid-19 experience to build stronger cooperation in the digital space, and so ensure that their citizens and economies – and even their democratic governance – remain secure in the future digital age? Initial impressions are not promising. The virus reinforced within Europe the desire for greater digital sovereignty, based on a strong, European-controlled digital infrastructure that will be resilient in the face of disinformation and other disruptions. In the US, as well as some other countries, the virus exacerbated a nationalist approach to economics that has been growing under Trump.

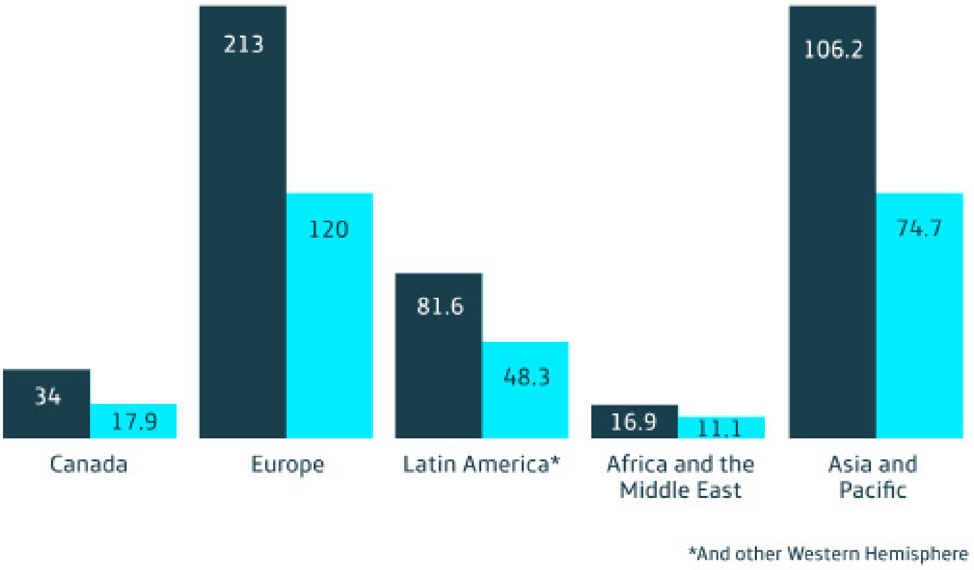
The choice facing the US and EU

Both the US and the EU now face a choice. The EU has initiated a broad effort to regulate the digital economy, but must now ensure – even in the midst of efforts to spur a post-covid economic recovery – that this drive for digital sovereignty does not turn into protectionism. Instead, the EU should use this opportunity, and the new awareness of the importance of digitalisation, to lead a multilateral effort to tame the worst excesses of the internet while fostering innovation and creativity. The US must return to participating in – if not leading – the multilateral economic system while also pursuing a more strategic domestic conversation on the digital economy; one that is not simply a reaction to the latest privacy or security breach. If the US and Europe fail to make the right choices, the main beneficiary will be China, which has consistently demonstrated its global ambitions during the covid-19 crisis. The result will be a digital world with three distinct approaches – US, Chinese, and European – with China more likely to convince many emerging markets to adhere to its more authoritarian, state-driven approach to both digital governance and commerce. But if the US and EU can together develop standards of commerce and behaviour in the digital world, they can be the global leaders, ensuring that most countries adhere to standards that support individual privacy and open markets.

Transatlantic discussions of digital policy often seem far removed from global strategic concerns, with their debates over differing US and EU approaches to topics such as intermediate liability and adequacy agreements. To those engaged on the digital frontlines, especially from the corporate trenches, these differences seem huge and certainly may be worth significant sums to businesses. But for many policymakers, including those who have been the mainstay of the transatlantic relationship, these discussions seem technical and arcane. This is especially true in the US, where the US-European partnership is predominantly seen as a security partnership based on NATO, and cybersecurity – and NATO's role in cybersecurity – is the pre-eminent digital issue.

In reality, digital issues are central to the health of the transatlantic partnership. The digital economy is a key part of the US-EU economic relationship. The transatlantic economy is the strongest trade and investment partnership in the world, generating $5.6 trillion in commercial sales and supporting 16 million jobs in 2018. While measuring the digital economy is still more art than science, a few indicators demonstrate its scope. Cables bringing digital data across the Atlantic carry 55 per cent more data than across the Pacific, and eight new transatlantic cables are planned in the next few years. For both the EU and the US, the leading import destination for their digitally enabled services is the other, representing about one-third of such exports. In 2017, US exports of digitally enabled services to the EU totalled $190 billion, and imports totalled $118 billion, giving the US a surplus of $72 billion. (Digitally enabled services are difficult to measure. This figure combines US government estimates of trade in information and communications technology services trade as well as additional services potentially enabled by them). That same year, US corporations, through their local affiliates in Europe, supplied $180 billion in information services, while only supplying $3 billion in China and $21 billion in Latin America. Of all US overseas investment in the information industry, 73 per cent was in Europe in 2018.

US trada digitally-enabled services ($US billion), 2018



Source: US Chamber of Commerce, John Hopkins SAIS

Aside from the economic data, however, the digital economy now pervades almost every element of daily life in both Europe and the US. Whether it is shopping or dating online, watching movies, taking online courses, navigating on the roads, or personal banking, Americans and Europeans are constantly connected to the internet. Issues such as online privacy, copyright infringement, and understanding the source of online news have become key to the functioning of society.

At the same time, however, both Europeans and Americans are concerned about the security of their personal and financial information online. A 2019 Eurobarometer survey revealed that only 32 per cent of Europeans have trust in the internet, and, in another survey, 43 per cent of Europeans believed their data might be misused via the internet. Americans are not immune to these concerns: according to a 2019 survey, Americans are worried about how their data is collected and used, with 79 per cent concerned about how companies use the data, and 64 per cent expressing the same concern about government. With internet usage now well over 70 per cent in both the US and Europe, such widespread security concerns will inevitably be a sensitive domestic issue.

European initiatives

Over the past decade, the EU has responded to the growing economic and political importance of the digital economy – and to the concerns of its citizens – by launching a series of regulatory initiatives. The Digital Single Market Strategy, launched in 2015, aimed to reduce or eliminate barriers to digital activity between the member states and improve access to online services and products for citizens and businesses. While still far from complete, it has tackled differences in roaming charges and access to movie downloads – seemingly mundane issues that matter to individual citizens. Following the 2013 revelations by Edward Snowden of significant US government surveillance of European citizens' communications – including German chancellor Angela Merkel's mobile phone – the EU passed the General Data Protection Regulation (GDPR). This is arguably the most comprehensive privacy legislation in the world, which imposed strict conditions on the handling of EU citizens' personal information, even if that data or citizen was physically outside the EU. When it came into effect in May 2018, companies around the world found themselves having to comply with GDPR. Although creating EU digital sovereignty was rarely mentioned at the time, both the digital single market plan and GDPR were clearly intended to enhance EU digital capabilities and provide citizens with a form of sovereignty, or control, over their own personal data.

By the time of the arrival in December 2019 of the European Commission led by Ursula von der Leyen, the idea of greater European sovereignty over the digital economy had become important enough to feature in her political declaration outlining her priorities. In it, she called for the EU to "achieve technological sovereignty in some critical technology areas". Moreover, in her inaugural speech before the European Parliament, digital policy in general was identified as one of the commission's top priorities, along with the "Green Deal", and she again stated that Europe "must have mastery and ownership of key technologies".

The focus within the commission has been largely on technological sovereignty – ensuring that the EU has a secure, high-quality digital infrastructure and the ability to develop and sustain key cutting-edge technologies. This requires supporting research and innovation, but also creating an appropriate regulatory environment. The previous commission had already taken steps to address infrastructure security in the face of growing cyberattacks. The 2016 Network and Information Systems directive obliges member states to identify essential network operators and then requires those operators to adopt appropriate cybersecurity measures and report breaches. In 2020, in the wake of growing concern about Chinese investment in Europe, the EU warned member states that non-EU vendors for 5G and other technology could pose significant risks, especially if they were closely connected to foreign governments. While the EU did not ban Huawei outright – despite US pressure – a number of European governments have curtailed Huawei's role in their networks. At the same time, the commission outlined the importance of a European cloud service, and began discussions with the German and French governments, which had already launched the GAIA-X cloud project. These measures are clearly intended to promote a resilient infrastructure as a key element of technological sovereignty.

The second element of tech sovereignty is the ability to develop a European capacity in key emerging technologies. The commission has identified a range of technologies, including artificial intelligence (AI), super-computing, blockchain, and quantum communications, where Europe might become a global leader. A new Digital Europe research programme is expected to support this effort with €9.2 billion in funding, pending final approval of the EU's next budget. In keeping with this ambition, in February this year, the commission released a preliminary legislative proposal on AI. It also released a strategy for data management, noting the importance of data collection and governance to almost all the key technologies.

There is a third element to the EU effort; one far more political and also a defining feature of the European approach. Ever since the passage of GDPR, the EU has seen itself as a global leader in establishing standards related to online activities that are intended to safeguard its citizens and ensure an ethical approach to the dilemmas posed by the digital world. This is not only true in privacy, including the "right to be forgotten", but also in online content, where some EU countries have restrictions on illegal or hate speech. Whether EU standards accomplish those aims – and whether they are better than other arrangements – is less certain and a matter of political judgement.

Both the data strategy and AI proposal include potential rules seeking to ensure that data collected and controlled in Europe, and AI used in Europe, would be managed according to ethical and "human-centric" (but not yet precisely defined) standards. As Thierry Breton, European commissioner for the internal market, put it: "My goal is to prepare ourselves so the data will be used for Europeans, by Europeans, and with our values." The Digital Services Act, which is expected to be outlined by the commission in late 2020, is also expected to propose rules intended to reinforce European norms on content, consumer protection, and platform liability. Such rules go far beyond technological sovereignty, with its emphasis on infrastructure and key industries, and instead use an emerging set of European norms for behaviour and responsibilities in the digital world to develop standards that will have an extraterritorial – if not global – impact. By being the rule-maker, the EU hopes to gain more control over how digital activities are conducted within Europe and how its citizens are treated online, and thus enhance its broader digital sovereignty.

The US approach

The US has not undertaken such a comprehensive approach to digital policy. Instead, on the federal level, there have been sporadic efforts to address four separate concerns: privacy, consumer protection, security, and online content. Efforts have been divided among a group of federal agencies, including the Federal Trade Commission (FTC), the Federal Communications Commission, and the National Institute of Standards and Technology. In Congress, occasional bursts of interest in regulating the tech sector have usually faded with little consequential legislation. Given the absence of regulation at the federal level, some states have taken the initiative. Most prominently, California has adopted the California Consumer Privacy Act (COPA), which has many similarities to the GDPR and came into effect in 2020.

National US privacy legislation dates from 1974, when the Privacy Act provided certain protections for citizens when their data was held by the federal government. Laws addressing privacy in the health and financial sectors were passed in 1996 and 1999 respectively. None of these laws was intended to deal specifically with data protection online. Data protection in the US has not only been sectoral, but also focused on consumer protection. The FTC is responsible for ensuring that companies do not engage in "unfair or deceptive practices" and has used this power to examine whether Facebook and others have misled users about how their data is treated. Privacy has not been totally ignored in the US, however, as COPA, and the interest a few other states have shown in similar measures, demonstrates.

Security has been a major concern of the US government, especially following the attacks of 9/11. The initial response was for US intelligence agencies to undertake mass surveillance of online activities. This practice raised significant concerns not only in the US, but also in Europe. The Snowden revelations provided a considerable boost to European efforts to create comprehensive privacy legislation – an effort that would lead to the GDPR. Surveillance by the NSA was rolled back somewhat by the 2014 Freedom Act, which protected American citizens from bulk data collection, but instead required the NSA to submit more specific requests when asking for data from companies. Of course, in an era of terrorism and extremism, some of that data is useful to law enforcement on both sides of the Atlantic. The 2018 Cloud Act requires US technology companies to provide data requested by law enforcement agencies through a warrant or subpoena, even if that data is stored outside of the US. The United Kingdom has signed a bilateral agreement providing reciprocity and the EU has initiated negotiations to that end. Finally, one additional element of the US approach to online security is the concern about foreign vendors, whether Kaspersky cybersecurity products, or Huawei on 5G networks.

Since the arrival of social media, the US and Europe have been confronted with sometimes gruesome terrorist content online. More recently, concern has grown about the role of social media in spreading false or misleading information that has either political or health and safety consequences. While Europe has taken some steps to restrict and police such misuse, the US has taken few significant steps, as most speech is protected under the First Amendment of the US constitution. Only a few topics – such as child pornography or that identified as providing "material support" to terrorists – have been made illegal. Since the 2016 election, there has been increased debate, especially in Congress, about the role of social media in spreading false or misleading information. The social media companies have responded by requiring better identification from advertisers, but no significant legislation has been passed.

Differences in perspective

As this comparison of the US and EU approaches to digital policy reveals, there are two major differences in perspective. Firstly, the US has generally treated the digital economy as an extension of the traditional economy and applied existing regulation on privacy, content, consumer protection, competition policy, and other areas. The EU (and most member states) has viewed the digital economy as posing new challenges, both to consumers and to businesses, that require new regulations. In particular, concerns about the security of citizens' data, the role of platforms in linking buyers and sellers, and the potential for harmful content on social media sites has spurred an effort to design a comprehensive regulatory regime for the online world.

Secondly, while European officials and opinion leaders often present this effort as a matter of achieving digital sovereignty, these words are almost never heard in the United States – and with good reason. The European search for digital sovereignty is rooted in a perception that Europe has to date been dominated by non-EU companies, especially US and Chinese firms, in the digital space. This is not a misperception. Of the top 100 digital companies identified by Forbes in 2019, only one EU company (Deutsche Telekom) made the top 20, while US companies claimed 12 spots; China and Japan two each; and Hong Kong, South Korea, and Taiwan one each. Less than 4 per cent of the market capitalisation of the world's 70 largest platforms is European. In January 2020, Apple alone was valued at $1.42 trillion – more than the entire DAX index of Germany's leading 30 companies.

For the US – home of the so-called GAFA (Google, Apple, Facebook, Amazon) – there has been no need to recapture the digital economy from the influence of non-US companies. The presence of large Chinese online actors has only recently become a concern, primarily in the infrastructure and security fields. As a result, European concerns about US tech firms has seemed puzzling and even misplaced to many in US industry and government circles. Some have dismissed Europe's ability to achieve its goals, while others have questioned whether this is simply protectionism, intended to establish a digital "Fortress Europe". Moreover, European rhetoric about sovereignty has raised suspicions among some in the US tech sector and policy community: sovereignty from whom and for what purpose? Many in the EU portray digital sovereignty as the tech version of "strategic autonomy", the EU ambition to achieve resilience, and more significant capabilities in the traditional defence and security realms. However, many in the US, even in the transatlantic policy community, asked similar questions about strategic autonomy – autonomy from whom? – and felt it was aimed at distancing the EU from the US.

The Trump administration has been particularly suspicious of EU ambitions in the defence sector, compared to previous governments. The administration has been less vocal in expressing concerns about EU digital policy, in part because digital issues have simply not been a priority. With a few exceptions, this administration has shown little interest in technology or digital policy, whether in the US, in the G7 or G20, or related to major trade and investment partners. The one exception is the prospect of a digital services tax, which has caused much concern. France approved

such a tax, which would have affected companies – primarily US platforms – which generate €750m in global digital services and €25m in France. The Trump administration threatened the imposition of tariffs on French goods, until Emmanuel Macron agreed not to implement the tax while the OECD effort to find a consensus solution is under way. That process is expected to reach a conclusion at the end of 2020, but the Trump administration has recently suspended its participation in the effort, claiming that "no headway" was being made.

However, the US cannot ignore forever the impact of Europe's search for digital sovereignty. The widespread implementation of the GDPR – including by many US firms – demonstrated to Europe that it could create regulations with global reach. As the EU ramps up its digital agenda, US companies are likely to face additional rules, especially on data governance, use of AI, platform liability, and other digital issues. These rules may affect, for example, the ability of US companies to import goods or services that use AI into the EU, or how they manage data pools derived from EU data.

Thus, the US and the EU each face a choice. The EU must decide how restrictive it will be in the name of protecting European citizens and supporting European innovation and companies. Will it discriminate against non-EU companies? Will its rules – however well intentioned – impede international trade in digital services and perhaps even stifle Europe's ability to innovate and grow? As the world looks for a post-covid-19 economic recovery, European economic growth, including in the tech sector, is in everyone's interest. Europe should look to build its digital sovereignty without becoming a digital fortress.

For the US, the choice is whether to engage with Europe as it moves forward on its digital agenda – or not. A refusal to engage, or even a continuation of the neglect of the past three years, will not prevent the EU from moving forward. US companies will have to comply with EU rules or lose a major market. The smart choice for the US is to engage with the EU and work to help shape its emerging legislation. That engagement, such as the recent US comments on the GDPR review, will be most effective if undertaken in an atmosphere of constructive cooperation, which has been missing from the US-EU relationship for some time. The US should seek early engagement on pending EU legislation on data governance, AI, and digital services. It should re-engage in the OECD process on digital services taxation. By constructing its own comprehensive federal privacy law, the US would put itself on a level footing with Europe and remove some of the uncertainties that surround continuation of data transfers across the Atlantic. Finally, the US and the EU together should inaugurate a Digital Council to provide their top leadership with a forum for discussing the rapidly evolving digital economy and how the US and EU can together adopt the best approach for their citizens and prosperity.

Artificial intelligence: Towards a pan-European strategy

Andrea Renda

Senior research fellow and head of global governance, regulation, innovation, and the digital economy (GRID) at the Centre for European Policy Studies (CEPS)

Recent years have seen the rise of AI as a top public policy priority, especially in developed countries. Superpowers like China and the United States compete to dominate this field, making unprecedented levels of investment and engaging in aggressive strategic moves to strengthen their position in the global arena. Academics and NGOs denounce the extreme examples of "surveillance capitalism" in the US and authoritarian surveillance in China. These continuing tensions, which encompass the whole digital policy domain (and are exemplified by the US ban on Huawei), are an important obstacle to achieving a globally accepted system of rules and regulations on AI. Efforts by several countries (for example, France, Canada, and Japan) to create an Intergovernmental Panel on Artificial Intelligence, and later a Global Partnership on AI, have been undermined by the lack of trust and the growing competition between the US and China, to the extent that some commentators see the looming prospect of a "splinternet" as a likely evolution in this increasingly strategic domain.

Against this background, the European Union started its debate on AI in 2017 in a rather dystopian way, with the European Parliament's resolution on Civil Law Rules for Robotics, which foresaw the rise of smart autonomous robots and evoked the need to attribute rights and duties to these new legal entities. The same resolution also called on the European Commission to consider the creation of an agency for AI and to establish a comprehensive policy framework to mitigate the risks of this powerful, dual-use technology. Due to its almost exclusive focus on the risks of AI, the parliament's position provoked a very critical reaction from the scientific community, but it at least placed AI on Europe's policy radar: a few months later, the European Council also called on the commission to take action to address AI.

The commission's AI strategy was officially launched by the adoption of a communication on AI in April 2018. The communication, which was published in parallel to the commission's proposals on establishing a "common European data space", adopted a more positive stance towards AI compared to the European Parliament's initial resolution. It laid the foundations for a comprehensive AI strategy by clarifying the main elements of the future EU policy mix on AI. The main assumption behind the strategy is that Europe "can lead the way in developing and using AI for good and for all, building on its values and its strengths". Those strengths, the commission suggested, include world-class researchers, labs and start-ups; strength in robotics and world-leading industries (especially in transport, healthcare, and manufacturing); the digital single market; and a "wealth of industrial, research and public sector data which can be unlocked to feed AI systems".

“Europe can lead”: The first steps of the EU AI strategy and the work of the High-Level Expert Group

The main assumption – that “Europe can lead” – was accompanied by three separate, but complementary commitments: to increase investment to a level that matches Europe’s economic weight; to leave no one behind, in particular when it comes to education and ensuring a smooth transition towards the AI age in the workplace; and to ensure new technologies reflect European “values”. With respect to the latter commitment, the commission made explicit reference to GDPR (the General Data Protection Regulation), which, at that time, had not yet come into force, as well as to Article 2 of the Treaty on European Union, which lists the EU’s founding values as respect for “human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities” and a “society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail”.

Expert advice: Ethics guidelines and investment recommendations

The communication also announced the adoption of a series of initiatives on AI, including the creation of a High-Level Expert Group on AI (AI HLEG), as well as the launch of an AI Alliance, which quickly attracted members from civil society, industry, and academia (more than 4,200 as of 15 May 2020). The AI HLEG’s 52 experts were asked to come up with a series of ethical guidelines, which were published in April 2019, and to make policy and investment recommendations, which were unveiled in June 2019.

The AI HLEG’s recommendations significantly influenced EU institutions. In particular, the ethics guidelines introduced the concept of “trustworthy Artificial Intelligence”. This required that AI meet three cumulative requirements: legal compliance, ethical alignment, and socio-technical robustness (for example, in terms of security, safety, and reliability). The guidelines represented a step forward compared to the ethical principles previously adopted by many corporations, governments (for instance, the Montreal Declaration), or NGOs (such as the Toronto Declaration drafted by Amnesty International and Access Now), due, in particular, to their references to legal compliance, coupled with potential means of verification and enforcement.

The AI HLEG observed that any “human-centric” approach to AI requires compliance with fundamental rights, whether or not these are explicitly protected by EU treaties, such as the Treaty on European Union or by the Charter of Fundamental Rights of the European Union. The experts argued, for instance, that these rights do not view human beings as “objects to be sifted, sorted, scored, herded, conditioned or manipulated”. Moreover, they suggested, the EU’s commitment to such notions as “respect of equality, non-discrimination and solidarity” requires that AI does not produce new inequalities, especially those which might negatively affect “workers, women, persons with disabilities, ethnic minorities, children, consumers or others at risk of exclusion”.

The guidelines identified four key principles (defined as ethical “imperatives”) for “trustworthy AI”: respect for human autonomy, the prevention of harm, fairness, and explicability (that is, the information used and the process followed by AI systems to reach particular outputs or decisions must be as transparent and traceable as possible for those directly and indirectly affected). The four key principles were then, in turn, translated into seven requirements that AI systems should comply with in order to be defined as “trustworthy”. These principles included areas that reflect key EU public policy priorities – such as the protection of privacy and the pursuit of social and environmental well-being – along with requirements that more commonly feature in discussions around ethical AI. These include human agency and oversight, transparency, accountability, technical robustness, and the protection of diversity and the avoidance of bias and discrimination. However, perhaps the most innovative feature of the ethics guidelines is the attempt to help increase compliance with the requirements through the publication of a detailed assessment list, which was transformed into an interactive web-based tool in June 2020.

The AI HLEG’s policy and investment recommendations explicitly called for making the “trustworthy AI” assessment mandatory for all AI systems deployed by the private sector which have the potential to have a significant impact on human lives. These include, for example, AI which interferes with an individual’s fundamental rights at any stage in the system’s life cycle (that is, from design to development, commercialisation, update, and finally disposal). The mandatory assessment would also apply to AI related to applications that, if they malfunction, pose, for example, specific threats to people’s safety, endanger equipment or property, or risk environmental harm. It seems clear, therefore, that the AI HLEG does not consider “trustworthy AI” as simply an “aspirational goal”, but rather as the foundation of a wholly new risk-based legal system, in which critical applications that potentially impinge on fundamental rights are subject to a mandatory assessment. The AI HLEG also called on the European Commission to consider the establishment of an "institutional structure" that could help collect and spread best practice in a more agile way than judges, regulators, and lawmakers are normally able to.

The AI HLEG took a critical stance on a number of emerging uses of AI, which are thought to create significant risks for users and society. These include mass surveillance and the use of lethal autonomous weapons, on which the group called for an international moratorium. The AI HLEG also explicitly recommended that policymakers issue regulations to ensure that individuals are not subject to "unjustified personal, physical or mental tracking or identification, profiling and nudging through AI-powered methods of biometric recognition such as: emotional tracking, empathic media, DNA, iris and behavioural identification, affect recognition (that is, the capability to detect the emotional state of an individual), voice and facial recognition and the recognition of micro-expressions". Such methods should only be allowed in exceptional circumstances, for instance, in the case of pressing national security threats and even then only if "evidence based, necessary and proportionate, as well as respectful of fundamental rights".

The AI HLEG also recommended specific actions to protect children, including a comprehensive "European Strategy for Better and Safer AI for Children". In particular, it suggested that EU legislators introduce a legal age at which children receive a "clean data slate" (which would apply to both the public and private sector) and recommended monitoring of the development of personalised AI systems built on children's profiles to ensure their alignment with fundamental rights, democracy, and the rule of law.

The white paper on artificial intelligence: From words to action

The EU AI strategy reached a turning point with the arrival of the new European Commission led by Ursula von der Leyen in December 2019. It set the green and digital transitions as its twin key priorities and, in the first 100 days of her term, the new president announced an initiative on the human and ethical consequences of AI. At the same time, and especially following the appointment of Thierry Breton as commissioner for the single market, the commission has also stepped up its efforts on the data strategy. This issue is intimately related to AI policy and crucial in terms of future partnerships and alliances at the international level, due to the existing differences in the legal framework for data protection and privacy in different countries, and due to Europe's growing emphasis on technological and data sovereignty.

On 19 February 2020, the commission launched a comprehensive package containing its ideas and actions on the digital transformation, including a white paper on AI and a European strategy for data. The package, which is both very assertive and comprehensive, marks another step forward in Europe's quest to lead on "human-centric" AI. It is based on a specific vision of the future of data and AI, including the expectation of a forthcoming paradigm shift, from a cloud-dominated environment to data being much more widely held. In the years to come, the commission expects the current 80/20 situation (80 per cent of data stored in the cloud and 20 per cent locally) to shift to a 20/80 scenario (with 80 per cent of data being locally stored, in, for example, devices, cyber-physical objects, and edge computing). With this shift, platforms – such as Google and Alibaba – may become less dominant. In such an environment, the commission hopes, Europe will have a chance to compete through brand-new infrastructure based on a federated cloud, a cloud infrastructure that can accommodate various heterogeneous cloud services under a common set of interoperability specifications (possibly scaling up national initiatives such as GAIA-X); dedicated data spaces in key sectors (such as manufacturing, health, and mobility); and open data from public institutions and research projects. This will all be fuelled by a new public-private partnership on AI that will nurture Europe's specialised knowledge, especially in robotics and "embedded AI" (AI integrated with hardware systems and devices).

The white paper sets a double goal of creating an "ecosystem of excellence" along the entire value chain and a unique "ecosystem of trust", chiefly based on a "human-centric" approach. In doing this, it reflects the commission's initial 2018 approach; one based on a combination of competitiveness ("excellence") – which requires research and innovation, investment, skills, and industrial policy – and ethically aligned AI ("trust"), which calls for a risk-based approach to regulation.

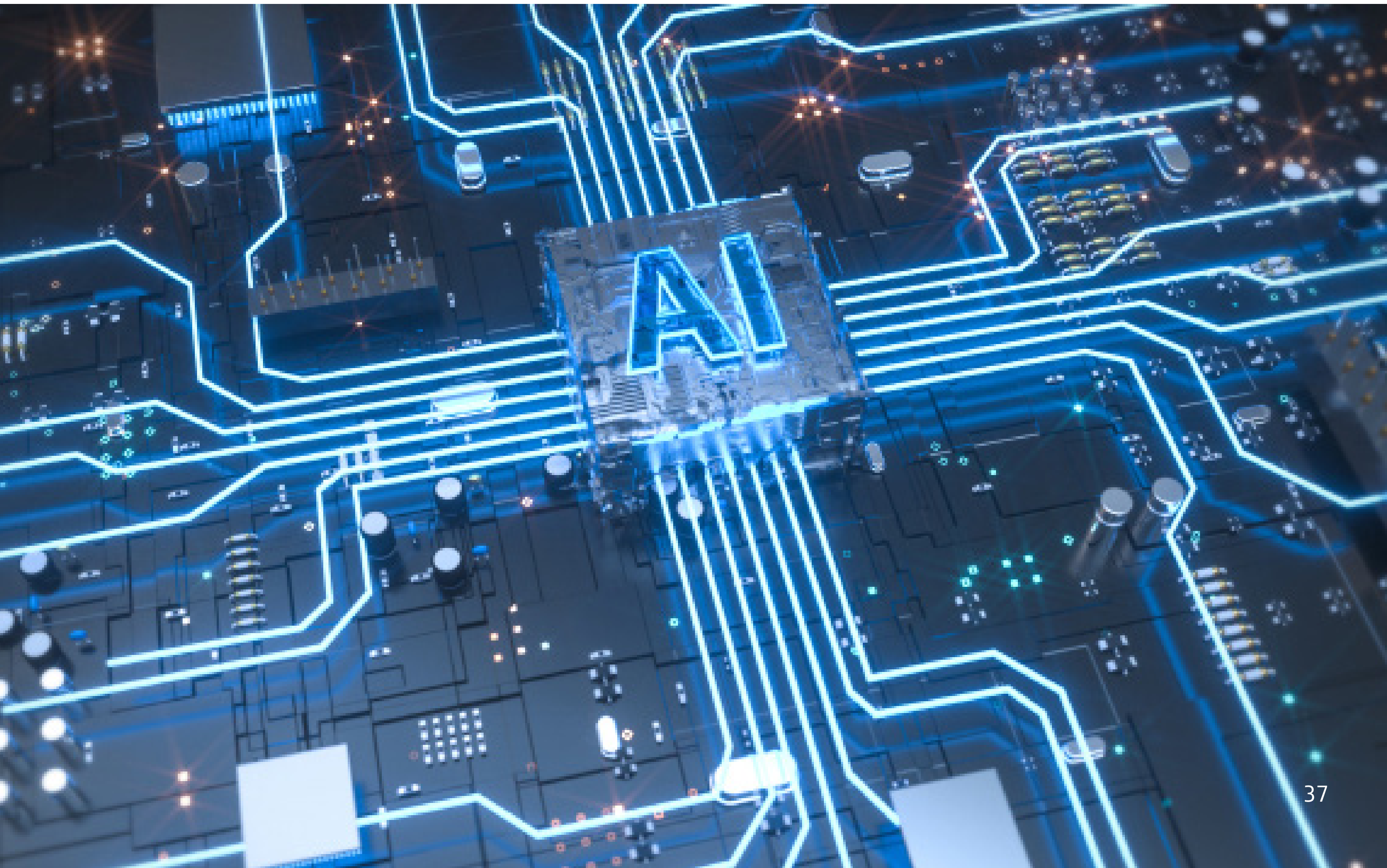
On the "excellence" side of the equation, the commission announced the creation of testing centres that can combine European, national, and private investments; new action on skills and support to small and medium-sized enterprises; a dedicated budget for equity funding (starting with €100m); and, most notably, the launch of a new public-private partnership in AI, data, and robotics.

On the issue of "trust", along with changes to the products liability regime, the white paper reflects the work of the AI HLEG. It thus calls for the adoption of a flexible, agile regulatory framework limited to "high-risk" applications, in sectors such as healthcare, transport, police, and the judiciary, and focused on provisions related to data quality and traceability, transparency, and human oversight. Specifically, the commission announces that, for high-risk applications, rules could relate to training data; data and record-keeping; the provision of information to users; and the AI system's robustness and accuracy. In these areas, there could also be human oversight requirements and specific requirements for certain particular AI applications, such as those used for remote biometric identification. Some of the potential rules have already provoked concern among non-EU countries: for example, the possibility that AI systems developed and trained outside of Europe will be required to be retrained with European data ahead of their commercialisation.

The work programme of the commission indicates a legislative initiative on AI is now expected by the end of 2020. It envisages a follow-up to the white paper, focusing on safety, liability, fundamental rights, and data. At the same time, the commission is working on a legislative initiative on the governance of data space, which should complement the AI strategy by creating a European approach to data.

The EU and the global governance of AI: future scenarios

Over the past two years, the commission has made significant progress towards developing a strategy that puts the EU in the driving seat when it comes to the responsible development of AI. This EU approach seems to be guided by the belief that while Europe may have missed the first generation of digital transformation (the so-called "B2C wave") – which led to the emergence of a handful of prominent cloud-based "superstar firms" – it can still compete in the forthcoming second wave of edge computing and more decentralised data storage and, indeed, holds an advantage in some of the key technologies. Apart from 5G, where companies like Nokia and Ericsson are able to vie with Chinese and South Korean rivals, the commission sees a favourable market for Europe in "low-power computing systems for both edge and next generation high-performance computing" as well as on neuromorphic solutions (solutions that mimic the neurobiological architecture of the human brain) that are well suited to automating industrial processes and transport modes.



The aim of the EU is to act as a global standards-setter, by seeking to exploit its rule-making ability to export its rules and standards to the rest of the world. This has been termed "normative power Europe" or the "Brussels effect" by commentators and academics[3]. Following the experience of the GDPR, it will certainly entail the introduction of extraterritorial rules, which bind those who wish to interact with the European single market and its consumers, regardless of the location of the company's headquarters. However, compared to the GDPR, the approach proposed by the commission contains some interesting new elements. In particular, the data strategy and the announcement of the creation of a European cloud federation (based on GAIA-X) will lead to a new phase in Europe's regulatory expansionism. This will be based on software code, rather than simply law. Large cloud operators from non-EU countries have already recognised that being admitted to the future European federated cloud infrastructure will imply adhering to a set of protocols and standards that embed compliance with European rules, starting with privacy but also encompassing the forthcoming requirements for high-risk AI applications. Similarly, the data spaces announced in the EU strategy for AI will incorporate the EU acquis – the body of common rights and obligations which are binding on all EU countries – as software code.

It is difficult to predict whether the EU strategy will succeed at an international level. The commission certainly seems to have understood that without a broad international alliance for responsible AI development, the EU's efforts will be dwarfed by the gigantic investment and military endeavours of the US and China. Initial breakthroughs, such as the proposed creation of an Intergovernmental Panel on AI and the Global Partnership on AI, have led to a stalemate mostly due to the opposition of the two battling superpowers. And while the OECD and the G20 have largely converged with the EU approach in their principles for responsible AI, these promising developments may not usher in a more harmonious and coordinated future due to the looming, contrasting interests of the "G2". The reasons are not hard to discern: while the US regulatory principles for AI adopted in January 2020 seem to mark an important step towards a convergence of widely agreed principles for responsible AI, the recently adopted "Beijing AI Principles" and the Chinese de facto endorsement of the OECD/G20 process make these less strategically interesting for a White House which is more focused on excluding China and striking a deal with "like-minded countries".

Deepening international cooperation would also entail taking action at the more technical level. A joint effort by the International Standardisation Organisation and the International Electrotechnical Commission is currently under way to coordinate the development of digital technology standards, while the IEEE Standard Association, an engineers' professional organisation, is creating process standards in other areas including software engineering management and autonomous systems design. International cooperation will also see the further involvement of non-state actors, which have been extremely active in recent years through far-reaching multi-stakeholder initiatives, such as the Asilomar Principles and the Tenets of the Partnership on AI.

Should these efforts fail, two other scenarios – which are not necessarily alternatives or, indeed, desirable – appear feasible. On the one hand, a group of "like-minded countries" could create a coalition that excludes large powers such as Russia and China, by building on the EU's guidelines and requirements for "trustworthy AI" and establishing research cooperation on technology-based privacy protections. On the other hand, this fragmentation of the international dialogue on AI could create a fracture in global internet governance. This may end up leading to a deeper division of the internet infrastructure, such as the oft-evoked "splinternet". This latter scenario would be disruptive for the digital world, and possibly conducive to a very unstable global order, beyond simply the realm of AI or the internet economy.

[3] Anu Bradford, The Brussels Effect. How the European Union Rules the World (Oxford: Oxford University Press, 2020). and Richard Whitman (ed), Normative Power Europe. Empirical and Theoretical Perspectives (Basingstoke: Palgrave Macmillan, 2011).

Disinformation: Democracy, platforms, and foreign agents

José Ignacio Torreblanca

Senior policy fellow and Head of the Madrid office of the European Council on Foreign Relations and Professor of Political Science at the Universidad Nacional de Educación a Distancia (UNED)

With hundreds of millions of people around the world having lived through the covid-19 pandemic glued to their mobile phones for vital information, the lack of access to reliable and verified information has become an additional issue of concern for health authorities. The director-general of the World Health Organization has warned of the existence of an "infodemic" in reference to the worrying spread of hoaxes, fake news, and disinformation related to this deadly virus. The European Union's high representative for foreign affairs and security policy, Josep Borrell, bluntly summed up the seriousness of the problem: "disinformation", he said, "kills". And some studies have concluded that the volume of false information circulating on social media during this crisis is similar to the volume of legitimate information.[4]

The infodemic citizens are experiencing during this global health crisis is not a one-off phenomenon, but rather a structural element from a previous information crisis that has now revealed itself in all its crude vigour. For this reason, and even though it is a cliché to say that every crisis is also an opportunity, this crisis could create the right conditions for progress in the fight against disinformation that has been rumbling along in the background. This fight is enormously complex and requires action on multiple fronts. The right to truthful information and, at the same time, the responsibility of social media and internet platform operators must surely be the central elements of the charter of digital rights that is the subject of an increasingly broad consensus.

The information crisis

It is well documented that representative democracy is undergoing a deep crisis. Freedom House and other relevant organisations have demonstrated that there is a worrying rollback of democracy at a global level – a trend now in its thirteenth consecutive year – and a rise in populist forces and movements within both democracies and authoritarian states.

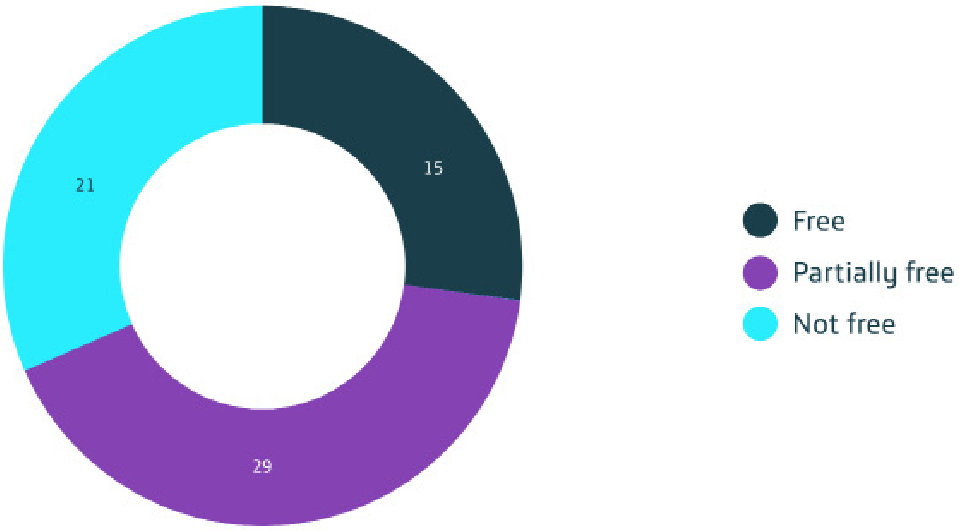
This essay does not deal with all facets of the democratic crisis in a systematic way. However, it is worth pointing out the close connections between the crisis and the digital revolution, given that technological change has weakened the role of traditional democratic intermediaries: political parties.

This disintermediation hampers not only political representation but also traditional media outlets, whose business model has been undermined, making it far more difficult to fund high-quality journalism. Essentially, this occurs due to the flight of audiences and accompanying advertising income towards digital platforms and social media. Having disintermediated traditional media, tech giants have become closed monopolies that take advantage of their dominant position to impede or block the progress of other companies. [5]

[4] Laura Rosenberger and Philip Howard (2020). "Memo: Disinformation and the Covid Crisis". Global Progress.

[5] Jason Lanier (2018). Diez razones para borrar las redes sociales. Editorial Debate.

Internet freedom rating of 65 countries



Source: Internet freedom rating of 65 countries

Largely because of their nature (but also due to inadequate regulation), these new intermediaries –technological platforms and social media – do not provide re-intermediation to make up for the disintermediation they cause. They lack, therefore, the qualities necessary to generate a democratic public sphere as an alternative to the one they are destroying. Evidence of the subsequent erosion of citizens' trust can be seen in the fact that, according to data gathered by Eurobarometer in 2018, 68 per cent of Europeans say they are exposed at least once a week to information that is fake or distorts reality. Revealingly, while 53 per cent of Europeans say they still trust the press, only 24 per cent say they trust the information that reaches them through social media and messaging apps. The alarming conclusion is that 82 per cent of those surveyed say that fake news and disinformation constitute a problem for democracy, a situation that has been identified as the "information crisis".

Hacking democracy

Disinformation and problems with representation predate the digital era. Each wave of populism and democratic crisis has been associated with an information crisis and an element of media technology. The press played a massive part in mobilising the first waves of populism that shook European democracies towards the end of the nineteenth century, and radio has been a close companion of all totalitarian regimes, from those of the 1930s to that behind the Rwandan genocide.

Therefore, while the digital revolution creates a phenomenon that is nothing new – the opportunity to manipulate public opinion – it is distinct in its capacity to do so much faster and more effectively than was previously possible.

From a democratic perspective, there is a series of endogenous issues with social media and digital platforms. The previously mentioned disintermediation is one. So too is a business model based on the so-called "attention economy" and the need to keep users within applications for as long as possible – to expose them to the maximum number of adverts and gather the maximum amount of data about their behaviour. The monetisation of attention requires the prioritisation of emotions and the most striking or controversial events; in terms of politics, this means amplifying negative or confrontational messages that stoke polarisation and generate traffic.

Another issue is the opacity of the algorithms that decide what takes precedence and must be seen first or most frequently by users of platforms and social media. A third factor is the lack of adequate filters and controls, allowing false information to be passed off as legitimate. At the same time, the networks' automated advertising systems permit and foment the creation of websites that look like authentic media sites, but that work as repositories and recyclers of fraudulent information. These media pretend to be journalistic in nature but, in reality, they are agents in the service of a given cause of political actors, and their main aim is to palm off false information. [6]

[6] Kirill Meleshevich and Bret Schafer (2018). "Online information Laundering: The Role of Social Media". Alliance for Securing Democracy, Policy Brief. No. 002.

Alongside the transmission and retransmission of these messages – whether they be true or false – carried out by social media based on their algorithms, there are third parties that, by using advanced instruments (fake accounts or bots), are able to create or amplify certain conversations, distorting the idea or perception that other users have of what is really happening and what is being said in a digital forum. For example, as revealed by an Alto Analytics study that examined 25 million movements on social media, 0.05 per cent of users – who showed unusual behaviour suggestive of automation in the transmission and retransmission of content – were responsible for at least 10 per cent of content of a political nature during the May 2019 European election campaign in Spain. Other studies by the same company have detected similar patterns of abnormal behaviour related to phenomena such as the election of Jair Bolsonaro as president in Brazil, the yellow vest protests in France, and anti-vaccine movements, among others.

Investigations into the Brexit referendum of June 2016, together with the US presidential election in November of that year – which brought Donald Trump to power – have allowed analysts to better understand how certain unscrupulous actors were able to exploit some of those characteristics of social media to manipulate voter sentiment and, potentially, sway the vote. Project Lakhta, an internet troll farm located in Saint Petersburg and coordinated by the Internet Research Agency, published 10 million false tweets, 116,205 fake Instagram posts, 1,107 YouTube videos, and 61,483 posts on Facebook, gaining a combined audience of 126 million people in the United States. Such huge digital activity was not only important in terms of quantity, but also had a significant qualitative impact in that it was designed and directed with very precise patterns of segmenting messages among communities. One example of how the campaign drove right-wing voters out to vote was through fake adverts in which Muslim organisations created in Saint Petersburg – but which appeared to have a US headquarters – supported votes for Hillary Clinton ("Muslims for Hillary").

Within the Trump campaign, there was a convergence of instruments of micro-segmentation and disinformation utilised by the Kremlin. This effort was directed by Steve Bannon, financed by Robert Mercer (who also supported Brexit), and designed by Cambridge Analytica – a company led by Alexander Nix that teamed up leading experts in psychometric techniques designed to understand voters' emotions and how to manipulate them effectively.

The ease with which it was possible to present distorted information, manipulate emotions, and influence the voting intentions of millions of Americans sprang not only from the lack of scruples on the part of a handful of companies or businesspeople, but rather from the simple way in which these companies were able to appropriate the personal data of 87 million citizens – thanks to their collaboration with Facebook – and to use them for political ends. In this way, they garnered precious information about voters that other political campaign leaders and pollsters lacked, which allowed the Trump team to focus campaign resources and messages on 13.5 million potential voters in 16 key states in the Midwest. This was something that conventional campaigns had not previously accomplished, owing to the absence of precise profiling data.

It has been estimated that the combined impact of these actions meant that 25 per cent of US citizens were exposed to some element of fake news during the peak of the campaign period (October-November 2016). But this rate was more pronounced among conservative voters: six in ten hits on fake news aggregators were concentrated among the most conservative 10 per cent of voters. Moreover, older people were the most susceptible: the over-65s were five times more likely to share fake news items than people between the ages of 18 and 25.

Although companies such as Facebook have repeatedly denied offering their clients products based on information regarding the emotional states of their users, there is plenty of evidence that they have done just that. Even more seriously, Facebook not only appears to have gathered emotional information but may also have experimented – successfully – with techniques designed to boost electoral participation through social pressure from the peer group closest to the voter. In the 2019 US Congressional election, it mobilised an extra 340,000 voters through an experiment involving 61 million users. Facebook has also looked into how to influence its users' political opinions and even their votes by changing the ordering and sequencing of information about candidates and parties, applying the theory of "emotional contagion".[7]

The geopolitics of disinformation

Interfering in elections constitutes only a small part of the disinformation problem; its scope and impact have made it into a global issue of the greatest importance. Freedom of the Net identifies some 30 governments that act as producers and disseminators of content intended to distort the information that circulates on the internet, pointing to Russia, China, Iran, and Saudi Arabia as major culprits.
As has become increasingly clear during the

[7] Adam Kramer, Jaimie Guillory, and 7. 7. 7Jeffrey Hancock (2014). "Experimental evidence of massive-scale emotional contagion through social networks". Proceedings of the National Academy of Sciences, June 17, Vol. 111. No. 24.

covid-19 crisis, information is a new battleground in the geopolitical competition between authoritarian regimes and liberal democracies. In the case of Russia, this increasingly involves activity designed to sow confusion and mistrust in scientists and politicians. China's strategy is aimed at papering over the damage that the origin and initial cover-up of the virus have done to its international image.[8]

That Moscow and Beijing are the actors making the most systematic use of disinformation is no coincidence. Nor is this phenomenon limited to the covid-19 question; indeed, it is a strategy they have developed. This is the case for two reasons. Firstly, control of information is an existential necessity for authoritarian regimes; dictatorships cannot coexist with freedom of information. Therefore, they need to develop and deploy strategies based on propaganda and disinformation, which they can then replicate externally.[9]

Secondly, in a hostile geopolitical environment, it is essential to spread disinformation. On the one hand, this is true in a passive sense, in that they need to block or filter their citizens' access to truthful news from the outside; on the other hand, they need to do so in a proactive or offensive manner with the aim of weakening or deterring enemies. This latter strategy – consisting of the dissemination of false and malicious information that undermines the enemy's self-confidence and, therefore, its will or capacity for confrontation – has dominated relations between Russia and the West for the past decade.

Paradoxically, in the case of Russia, the consistency and perseverance in its disinformation strategies are directly related to its weakness. Despite having immense natural resources and powerful armed forces, Russia's leaders are aware that Western power is superior in the economic and military spheres.

But of a far greater threat than the West's military might is the attractiveness of its lifestyle model for Russian citizens. Since the secession of Kosovo and the pro-democracy protests in Russia in December 2010, the Russian regime has had a clear understanding that its survival depends on weakening the attractiveness of the West's way of life, in the eyes of both its own people and of Western citizens themselves. This has driven a strategy that strengthens the vertical nature of power within Russia and, in parallel, an external strategy designed to increase Westerners mistrust in their democratic institutions. This external strategy aims to boost support for the anti-system forces that have the best chance of carrying populist Eurosceptic parties to power in each country, from France's Rassemblement National in France to Alternative for Germany, to Italy's the League. The idea is that these forces will weaken both intra-European cohesion

[8] Juan Pablo Cardenal (2020) "Propaganda china para un escenario post Covid-19". Centro para la Apertura y el Desarrollo de América Latina.

[9] JSergey Sanovich (2017). "Computation Propaganda in Russia: The Origins of Digital Misinformation". Computational Propaganda Research Project, Working Paper No. 2017.3.

and the transatlantic relationship.[10]

Disinformation does indeed weaken democracies and, simultaneously, strengthen authoritarian regimes. The mass media communications and totalitarian propaganda tools of the past have given way to means of mass surveillance that combine with artificial intelligence technology – which allows for tighter control of citizens through the gathering and exploitation of data to compile political profiles of them. Despite the fact that the internet was born amid utopian dreams of global freedom and universal knowledge, 71 per cent of the 3.8 billion people who now have access to the web live in countries where they can be fined or jailed for expressing their political views or religious sentiment online, and 56 per cent in states whose authorities block content for ideological reasons. In fact, only 20 per cent of internet users live in countries widely considered to be free and, even in countries where elections are held, only 7 per cent of users can vote without risk of electoral interference.

Duty of care

The well-intentioned utopianism that fostered the beginnings of the digital revolution led directly to a lax set of regulations. In 1996 the US passed the Communications Decency Act, whose section 230 establishes that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". The objective was to preserve freedom of expression and permit growth and innovation in the digital sector – and this was certainly achieved. In practice, however, it made digital platforms into "notice boards" that were exempt of any responsibility for their content, apart from in a very small number of instances.

The Communications Decency Act ignored the fact that these companies were much more than mere neutral repositories in which users placed their content; in fact, they have been and are active agents that order, sequence, and retransmit content so as to monetise it through advertising sales, effectively converting them into editors. As is true of other digital platforms such as Uber, the paradox is that they were not initially regulated with regard to the service they provided or under the legislation of the sector in which the companies claimed to belong to (communications platforms) – instead inhabiting a kind of legal limbo where, for the most part, they remain today.

From that well-intentioned utopian thinking at the inception of social media has emerged a far more pessimistic vision of democracy's compatibility with these networks. Now that the commercial workings behind the services these companies provide have been revealed – not to mention their permeability to foreign powers and agents – the discourse surrounding the global forum, the birth of a global conscience, and what Mark Zuckerberg has termed the "fifth estate" has lost its lustre. The malicious actions of authoritarian states are possible largely due to democracies' failure to provide adequate regulation for social media. This is why an entirely new regulatory approach to the problem is needed – one based on "duty of care" on the part of platforms. [11]

That regulatory approach is something the EU is well placed to implement, and even lead globally. So far, the White House and Congress have shown scant capacity or interest in facing up to the American tech sector, which contributes in a substantial way to the global clout and economic well-being of the US – as well as to electoral campaign financing. Moreover, the First Amendment of the US Constitution places far more stringent limits on the possibility of restricting freedom of expression than the terms of European legislation. For its part, China seeks to create its own Silicon Valley on a local scale to take maximum advantage of the capacity of new technologies in the exercise of social control – and to thereby sustain the authoritarian Chinese Communist Party regime with an asphyxiating layer of digital technology.

By contrast, the European Commission has already had success in the area of privacy with the General Data Protection Regulation.[12] The introduction of the regulation was a watershed moment for big tech companies, which were forced to adopt much higher privacy standards in Europe than in the US. In fields such as copyright, artificial intelligence, child protection, the right to be forgotten, and disinformation, the EU has shown clear signs that it has the capacity to become a regulator and standards-setter on a global scale, leading some to describe the bloc as a "regulatory superpower". [13]

The European Commission has decided to treat disinformation as a threat to democracy, public policy, citizens' security, public health, and the environment. The Commission's approach stems from the idea that disinformation is not an accidental by-product or unintended consequence of freedom of expression on social media. It has concluded that those who create it and those who collaborate in its dissemination bear equal responsibility. After intense negotiations, tech

[10] JMira Milosevich (2017). "El poder de la influencia rusa: la desinformación". Análisis del Real Instituto Elcano. 20 January 2017.
[11] William Perrin (2020). "Implementing a duty of care for social media platforms" Renewing Democracy in the Digital Age. Berggruen Institute.
[12] Boletín Oficial del Estado (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
[13] Anu Bradford (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press, USA

companies have been made to adopt a code of conduct that obliges them to check on fake profiles and accounts, and to periodically report on the action they have taken in this area. The Commission is, therefore, correct when it states that the fight against disinformation requires a more transparent and responsible ecosystem, as well as efforts to promote digital education and media literacy. Twitter's clash with Trump in May 2020 – when, for the first time, the platform invited the president's followers to fact-check his tweets and labelled some of them as glorification of violence – marked a sea-change that opens up whole new avenues (such as, for example, labelling tweets by officials from Russia or China as also in need of verification).

Besides the European Commission, many European states have either adopted or are considering steps against disinformation. But it is not an easy battle. As in so many other regulatory spheres, pointing to what needs to be prevented is much easier than drawing up a catalogue of measures that solve the problem – especially when, as discussed above, the problem is the ecosystem itself. For instance, the German government has opted for a strategy that consists of fining internet platforms that fail to eradicate content that has been reported and verified as fake or an example of hate speech. France, on the other hand, has chosen the route of establishing judicial control of platform content. [14]

The once-comfortable existence of tech platforms, previously characterised by continuous growth in income and users, is today marked by concern regarding the sustainability of their businesses. As a representative of one of the sector's biggest companies said at a seminar held by the European Council on Foreign Relations in London, tech platforms do not feel confident about providing assurances that the content posted on their sites complies with legislation – even if they hire thousands of people to check what users are publishing. And this is understandable. If in the same country two judges can hand down completely different rulings on the meaning of expressions displayed on the web, imagine the challenge when the network is global. What a judge in the US might consider to be protected by freedom of expression could, say, constitute a criminal offence such as hate speech in Germany.

An additional problem raised by the issue of regulation is that of efficacy. Any steps towards control or prohibition always prompt an adaptation on the part of the opponent. The regulation and limits placed on content visible on Facebook and Twitter have already had the unintended consequence of incentivising the migration of toxic content to networks such as WhatsApp – where distribution could be equally or even more viral, but detection and control is much harder to achieve – or to other closed platforms. Technology is always one step ahead of the regulator, especially with regard to illicit realms – and this means that it is all too easy for governments to end up with the worst of both worlds, sacrificing freedom without gaining security.

Finally, it is impossible to ignore the fact that, together with the supply-side disinformation problems, there are also problems in terms of demand. These range from people's psychological and cognitive predispositions to receiving and sharing this kind of information, to other issues related to a lack of a political or news culture – which, therefore, require educational initiatives that are by their very nature difficult to carry out in a democracy. [15]

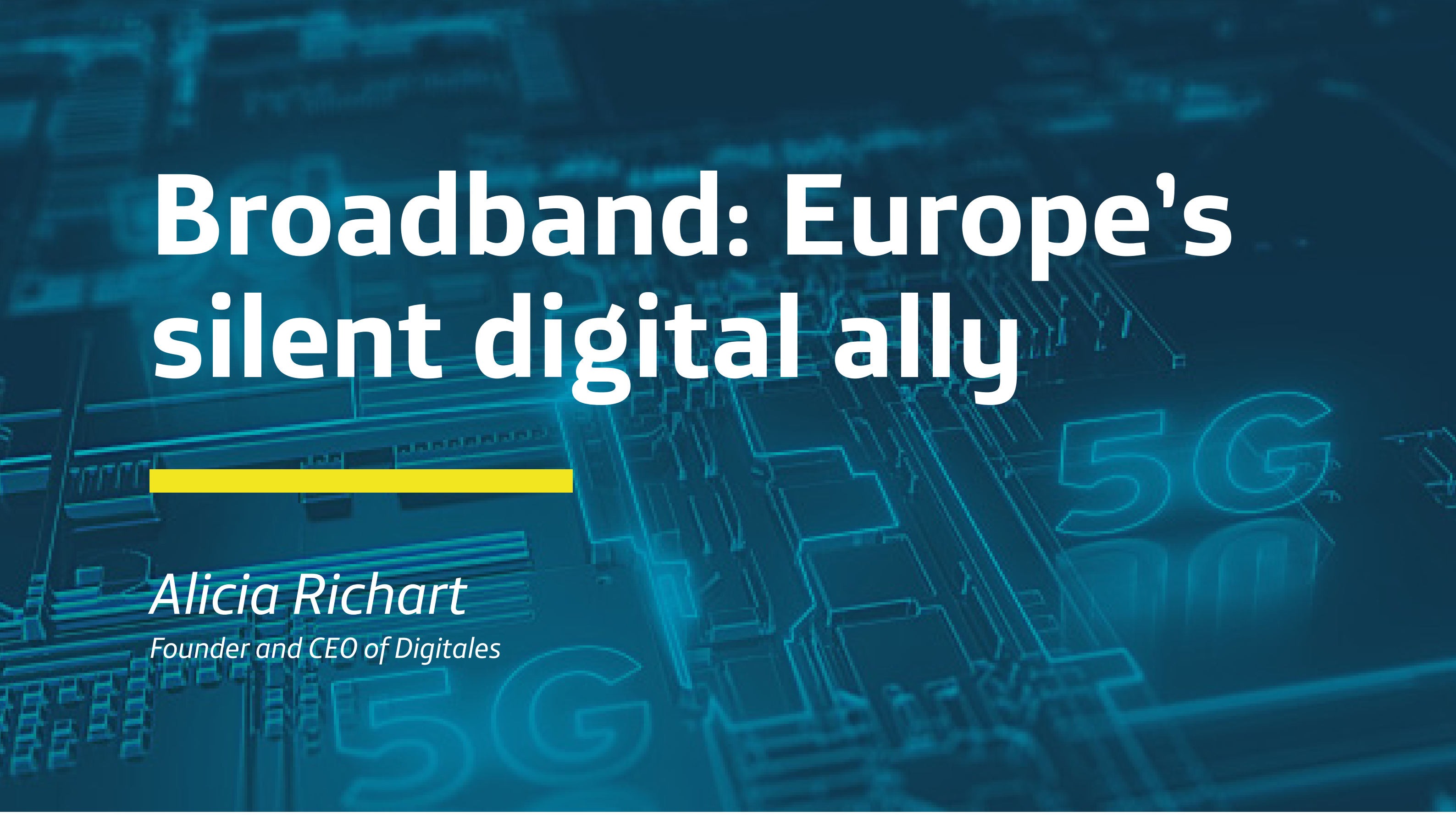
Conclusion

The dilemmas are stark: providing governments with the power to censor content currently in the hands of the tech companies is as bad an idea as leaving it in the hands of the companies themselves. At the same time, the absence of limits could harm the public democratic sphere and make it permeable to disinformation from both local and foreign agents; erode citizens' trust in institutions; and cause significant damage to people and specific rights.

Therefore, the EU and its member states need to act in a differentiated way on various fronts. On the international front, they should take firm action against those who use disinformation as a weapon to weaken democracies, while also leading a global regulatory response rooted in the universal values and principles that underpin representative democracy: human rights and a multilateral liberal order based on rules that are highly beneficial to Europe. On the domestic front, while users must be protected from the worst and most evident harms on networks that violate their fundamental rights, the EU should take a constructive and cautious approach to build and sustain a high-quality public space and media organisations that provide accurate facts for public debate (as opposed to polarisation and attacks on democratic institutions). This requires a triple alliance between responsible governments, companies, and citizens – an alliance based on dialogue and experimentation.

[14] Carme Colomina (2019). "La desinformación de nueva generación." Anuario Internacional CIDOB: pps. 61-66.

[15] Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera (2018). "Information Manipulation: A Challenge for Our Democracies", report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August.



Broadband: Europe's silent digital ally

Alicia Richart
Founder and CEO of Digitales

On 18 March 2020, right at the height of the covid-19 pandemic, Thierry Breton, the European commissioner responsible for the internal market, met with Reed Hastings, the co-founder and chief executive of Netflix, to discuss how to keep the internet running smoothly as the lockdown measures approved by governments across the continent forced more daily activities to move online. The meeting took place amid fears that fibre-optic networks would not be able to withstand the increase in traffic caused by massive bandwidth consumption both for professional and home use.

Breton, whose portfolio includes cybersecurity strategies and digital services, disclosed the conclusions of the conversation in a tweet asking users for their cooperation: "To secure internet access for all, let's #SwitchToStandard definition when HD is not necessary." The commissioner argued: "Teleworking and streaming help a lot but infrastructures might be [under] strain." According to its statement, Netflix committed to reducing the bit rate, understood as the number of bits that are conveyed or processed per unit of time. on all its content in Europe for 30 days. "We estimate that this will reduce Netflix traffic on European networks by around 25 per cent, while ensuring good-quality service for our members," the company suggested. In other words, it would downgrade the picture quality of its broadcasts so as not to collapse broadband networks. The same request – "to adopt measures to guarantee the proper functioning of the internet during the battle against the spread of the virus" – was also made by the European Parliament.

"Making Europe fit for the digital age" was ranked third in the commission's list of priorities for 2019-2024. But this was not just another element in the usual litany of priorities. Its new president, Ursula von der Leyen, pushed the commission to deliver a digital strategy within the first 100 days of her term. In keeping with this new impetus, on 19 February, shortly before most of Europe went into lockdown, the commission issued three major documents: a declaration concerning Europe's digital future, a white paper on AI, and a European strategy on data.

Digital transformation was a top European priority long before the onset of the coronavirus. However, there is no doubt that the pandemic has done more for the digital transformation of European societies, businesses, and government than any other policy or strategy. As entire societies and economies have gone into forced hibernation, the sectors that most quickly and ably switched most, if not all, of their operations to digital saved themselves from economic collapse. But, more than this, they also provided essential services to other sectors and helped their countries weather the crisis.

The digital component of Europe's resilience to the coronavirus cannot be underestimated. Most of this capacity relies on countries having reliable networks able to sustain not only standard operations, but a sudden and massive switch of others to digital networks. Even if network capacity was a key issue, which the commission was duly focused on before the current crisis, the coronavirus has highlighted both the strategic importance of digital broadband and, in parallel, the existing vulnerabilities and asymmetries that EU member states are facing. After the coronavirus, there is every reason to consider broadband as a key element of Europe's strategy to achieve digital sovereignty.

Europe's digital backbone

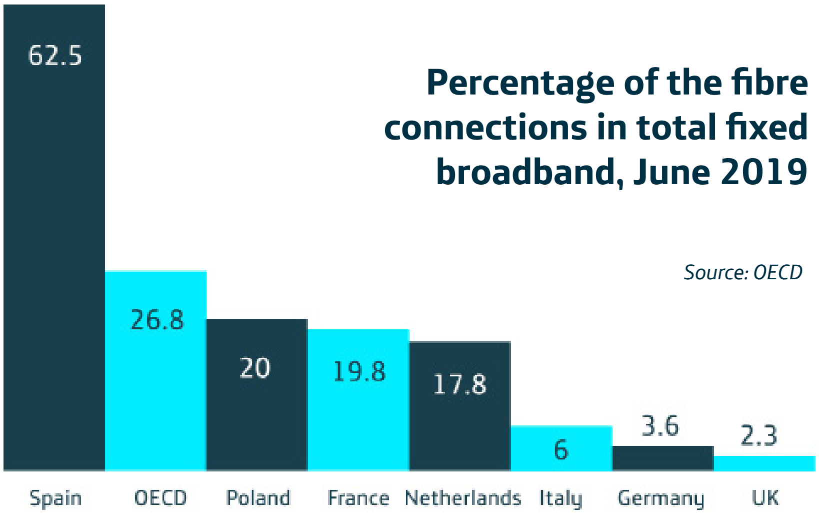
While the coronavirus pandemic has led to a rapid rise in demands for faster broadband in Europe, these calls predate the health crisis. Internet technology has begun providing an ever-increasing range of communications services and access to data and applications. These sustain huge volumes of video traffic and provide connections for billions of smart objects. This, in turn, require fast broadband access and, with it, robust broadband infrastructure.

The European Commission set an ambitious target under its 2014 Digital Agenda for Europe to guarantee "universal broadband coverage with speeds at least 30 MbPs by 2020" and "broadband take-up of 50% of households with speeds at least 100 Mbps by 2020". These targets reflected the marked differences in terms of available broadband infrastructure between different member states and between urban and rural (including remote) locations. Broadband infrastructure is crucial for the development of the digital economy and can stimulate innovation, productivity, and employment. A lack of access thus brings with it significant implications for those who are affected, and creates the so-called digital divide.

The EU's broadband objectives for 2020 were built upon in the commission's strategy on Connectivity for a European Gigabit Society in September 2016. It set out to ensure access by 2025 to one gigabit per second (Gbps) for all schools, transport hubs, providers of digital services, and digitally intensive enterprises; access to one Gbps download speeds for all European households; and 5G wireless broadband coverage for all urban areas and for major railways and roads. This has been complemented by a raft of initiatives including the new European Electronic Communications Code, the 5G Action Plan, the Connecting Europe Broadband Fund, and the Connecting Europe Facility. An additional €3 billion is budgeted for under the CEF-2 Digital strand of the 2021-2027 multiannual financial framework to finance strategic digital connectivity infrastructure.

Success has been mixed. While broadband coverage has certainly been improving across the EU, access to fast broadband is less uniform with rural areas remaining significant weak spots. According to the commission's latest Broadband Coverage in Europe study in October 2019, nearly 223 million EU households (99.9 per cent) had access to at least one of the main fixed or mobile broadband access technologies (fibre and 4G respectively) at the end of June 2018. The study also found that 83.1 per cent of EU households had access to faster broadband offered by next generation access services. However, rural broadband coverage continued to be far lower than the national average across EU member states, with just 52.3 per cent of EU rural households having access to high-speed next generation services.

Furthermore, take-up of ultra-fast Fibre to the Home (FTTH) broadband technology has been relatively slow in some member states. FTTH essentially means that the fibre broadband internet from the local exchange is connected directly to homes via routers, enabling an ultra-fast broadband service that can permit speeds of one Gbps. This is significantly faster than the traditional copper telephone line used by previous broadband services. According to the commission's report, just 29.6 per cent of EU households had FTTH. DSL remains by far the dominant fixed access technology, used by 92.2 per cent of households, followed by VDSL, used by 56.7 per cent.



Percentage of the fibre connections in total fixed broadband, June 2019

Source: OECD

Surprising asymmetries

On most issues, member states align quite naturally according to their economic size or strength. But this is not the case when it comes to broadband infrastructure. This disparity very clearly indicates that EU states do not yet share a common understanding about the strategic importance of broadband or of its significance as a vital asset in times of crisis.

The percentage of fibre connections in total fixed broadband differs significantly between member states. According to a June 2019 report, Lithuania ranked third among OECD countries with a 74.6 per cent take-up rate compared to Belgium with 0.98 per cent and Greece with 0.16 per cent. Of EU countries, Lithuania is followed by Sweden (68.95 per cent), Latvia (68.54 per cent), and Spain (62.53 per cent), which is sixth among the OECD and fourth in Europe.

What is shocking about this is that Germany and France – which are not only the two largest EU economies but, at least at first sight, digital leaders with well-conceived digital industrial strategies – rank thirty-third and twenty-fourth respectively. The fact that Germany comes after Mexico and Colombia in fibre connections indicates a massive underinvestment by its authorities in recent years. Most importantly, however, it shows that EU member states should consider the expansion of fibre connections a strategic priority. The commission also needs to ensure that proper targets are set and funded with the aid of the new budgetary instruments available in the revised multiannual financial framework.

However, it should also be noted that the annual growth of full fibre take-up is encouraging. Several member states appear to be on track to meet the 2025 target of having predominantly gigabit-capable broadband connection available to all homes. In Germany, it would appear that FTTH is finally being increased. This is especially thanks to the actions of certain cities and players like Deutsche Glasfaser. The national "Gigabit for Germany" project is also worth noting in this regard. In the United Kingdom, which has also lagged behind due to the decision to rely on VDSL copper solutions before switching to fibre, several players are taking the opportunity to build their business by exploiting the gap in the market. France is clearly at a halfway house and still has very ambitious targets to meet. Italy, which for a while enjoyed a solid advantage thanks to pioneering investments by FastWeb, plans to make up lost ground. This is evident in the success of the Open Fibre plan by the national energy company, Enel, which had installed more than 2.5 million points (for households) by January 2018.

Lessons learned from Spain

As mentioned previously, the OECD report reveals that 62.53 per cent of broadband lines in Spain are connected by fibre optics, which means it ranks sixth out of 38 countries. Its FTTH network is now the largest in Europe, and the single largest in terms of the number of homes which are connected. At the end of 2019, this amounted to more than 23 million homes. Moreover, all towns with more than 10,000 inhabitants already have a fibre network to use for any kind of activity, including business-to-business and business-to-consumer.

The fibre optic network deployed in Spain is the broadest in Europe with more than 33.3 million access points, covering more than 75 per cent of the population, with 4G coverage at over 95 per cent. The fact that Spain leads Europe for fibre connections (and is third in the world) allows it to withstand the peak of traffic that networks are experiencing in the current coronavirus-related, high-demand situation. This resilience is also thanks to the efforts of telecommunications operators to ensure the network's efficiency, capacity, and flexibility.

What the Spanish government and operators often refer to as the "Spanish fibre miracle" has meant an unprecedented investment effort in a context of market contraction for operators since the last recession. Since being liberalised between 1998 and 2016, the telecommunications sector in Spain has seen a huge total investment of €126.6 billion in a relatively short period of time. The country's operators have installed fibre optic cables that reach 31 million locations, more than France, Germany, the UK, and Italy combined. According to the OECD, only South Korea and Japan surpass this number.

In FTTH terms, Spain exceeds 10.2 million connections, of which 42.6 per cent are operated by Telefónica, with 4.3 million lines. Orange has 3.1 million, Vodafone 1.2 million, and MásMóvil 1.1 million, according to data from the third quarter of 2019. At the end of last year, Vodafone described deployment of 2.9 million FTTH lines and MásMóvil 1.3 million. Furthermore, both Vodafone and Orange – British and French companies respectively – have better networks in Spain than in their home countries. Spain has the greater number of fibre optic lines, as well as those of the best technical quality. In fact, Spanish connections reach the home (FTTH), while in other countries they only connect with the building (FTTB). For example, Germany has a fibre penetration of 2.3 per cent, of which more than two-thirds only reach the exterior of the building. In Spain, 97.2 per cent of the population has access to 4G and fibre penetration stands at 74 per cent of households, compared to 26 per cent across Europe as a whole and 15 per cent in the United States.

This capacity was put to the test on Monday 16 March, the first time that the network had been seriously challenged by simultaneous massive use for both entertainment and teleworking. In the first days after a state of emergency was declared, mobile voice (mobile phone) traffic increased by 40 per cent and fixed data traffic by 70 per cent. WhatsApp use increased six-fold, Netflix four-fold, and the use of video conference tools (such as Google Hangouts, Zoom, Webex, and Facetime) multiplied by factors of between six and eight, said José María Álvarez-Pallete, the president of Telefónica, in an interview. Telefónica registered 35 per cent growth in internet traffic on its fixed network in the first month after the onset of the crisis. This figure is the equivalent to the growth which normally occurs in a whole year. And the telecommunications network of Telefónica and the rest of the operators withstood the test. The Spanish experience shows the importance of public and private cooperation, strategic thinking, and a stable regulatory framework. That framework was updated in 2014 under the new General Telecommunications Act and the Spanish Digital Agenda. Several decisions taken in the midst of a recession were key at the time, and were adopted by both the operators and the government itself. These included prioritising and simplifying investments; the specialisation and retraining of technical teams to develop planning and design activities for optical networks; collaboration work by companies; the launch of high-quality convergent products; and a regulatory system that facilitated access for operators to ducts, making installation cheaper and faster.

Tech in the covid-19 era

The case for robust internet infrastructure across the EU has never been greater than in the context of the coronavirus pandemic. It has sustained the burgeoning technological initiatives that are attempting to tackle the disease, whether through stopping its spread, treating patients, or helping develop vaccines.

A recent European Parliament report has identified ten technologies to help fight the coronavirus, ranging from artificial intelligence (AI) to track the disease; nanotechnologies to test future vaccines and treatments; 3D printing for medical hardware, such as ventilators and facemasks; and blockchain applications to maintain medical supply chains. As the report notes: “Unlike previous public health crises, this one seems to be transforming citizens from objects of surveillance and epidemiological analysis into subjects of data generation through self-tracking, data-sharing, and digital data flows.” In doing so, technologies have been able to provide solutions to key problems presented by the pandemic and, as such, have played a critical role in our emergency response. Indeed, the EU’s ability to respond to the health and economic crises largely hinges upon its ability to harness these technologies.

It is, however, worth noting the high cost Europe is paying for its digital backwardness compared to the Asian countries that have shown diligence and effectiveness, especially in AI. Data, traceability, and digital control of infections have been essential in overcoming and eradicating the covid-19 epidemics in China, Singapore, Taiwan, and South Korea.

Each of these countries relied on their strong technology sector – and, specifically, AI, data science, and other technology – to track and combat the pandemic, while leading technology companies accelerated their health-related initiatives. Thus the development of AI and big data made the identification, tracking, and forecasting of outbreaks more immediate. This was accomplished through, for instance, the analysis of news reports, social media platforms, and government documents. In addition, the use of AI's predictive capabilities enabled more effective proposals regarding existing drugs that could be useful.

The use of cloud computing resources and the supercomputers of various technology companies are also accelerating the development of a cure for, or vaccine against, the virus. The speed with which these systems can execute calculations and model solutions is much faster than standard computer processing.

The price of Europe's digital underdevelopment – and the need for urgent changes and reforms in education, legislation, entrepreneurship, and its weak co-operational ecosystems – is undeniable. Furthermore, there is also the issue of governments' inefficiency in facing such global challenges, only now beginning to agree ambitious commitments in AI, among other initiatives.

As we have seen, technology and data analysis are, and will continue to be, fundamental. We must support technology and the enormous opportunities it offers us to anticipate future threats, and to make the right decisions to tackle them. We must share information and do so in an agile and effective way – and this is already within our reach. We must lay the foundations for a global big data system that allows us to face viruses like covid-19 with a different perspective, sharing knowledge as one humankind.

In this sense, projects such as GAIA-X, the European data area, and big data health initiatives should be driven forward and, if possible, developed further. Launched in early June 2020, GAIA-X is a collaborative project between, Germany and France, with the cooperation of the European Commission and some 100 companies and organisations to develop a European cloud concept. The project is motivated by the notion of "data sovereignty" or, more precisely, "data governance", and aims to bring data flows and storage under greater European control. It reflects the fact that not only will more and more core business processes run on cloud-based services, but that all major cloud providers are American-based companies and therefore subject to US jurisdiction. This makes Europe vulnerable because it cannot shape the way data is managed and governed.

Even so, the development of these projects will not be without difficulties: the timetable, precise technical details, financing, and even the governance are not yet clearly defined. Furthermore, the data spaces currently available have had years of development behind them and have very highly developed technical specifications. Nonetheless, the ultimate goal is to have a viable ecosystem of interconnected digital services that work seamlessly and are capable of offering industry and other sectors of the European economy a real and competitive alternative to today's dominant providers.

The incredible leap forward in the use of technology in recent months will not stop here. As the historian Yuval Noah Harari has suggested, the current situation will drive it even further: processes that previously would have taken years or decades now take place in a matter of days. No one would have imagined two months ago that the vast majority of Spaniards could switch to working from home overnight. What matters most now is that this definitive push, which has ensured that we see the digital sector as a pillar of our society and an essential service, is accompanied by a strategy that guarantees and drives forward recovery processes in Europe.

If digitisation and innovation were crucial in what we might term the pre-covid-19 era, supporting them – through, for instance, promoting continuous training and the development of digital skills – is now even more urgent. The steps taken, and support provided, by governments today will enable the technology sector to cement itself as an essential pillar of economic activity; one that will also be a source, directly and indirectly, of employment. Technology is a silent ally, as has been demonstrated during the pandemic, and a fundamental one in the post-covid-19 age.

France and Germany: The emergence of ethical AI

Ulrike Franke

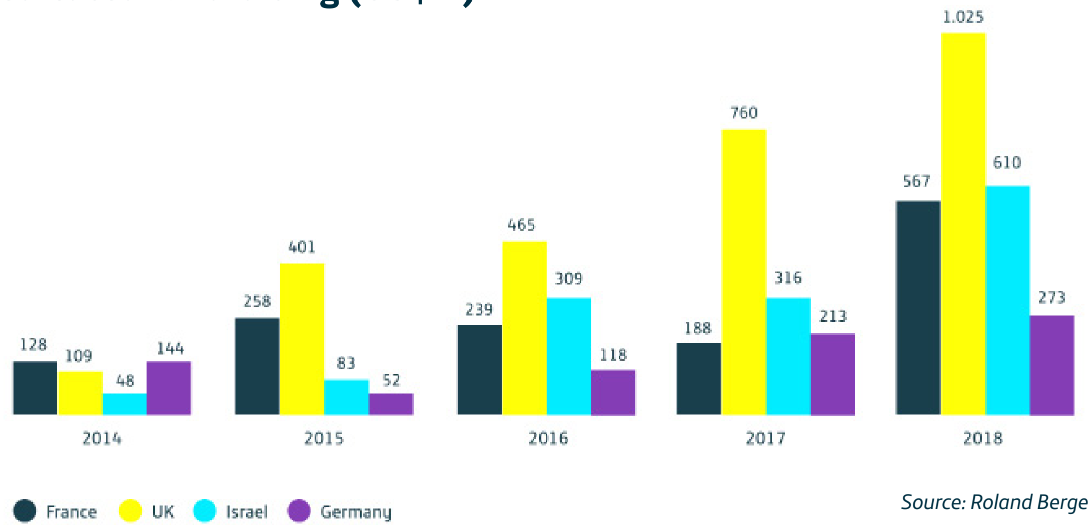
Policy fellow at the European Council on Foreign Relations and a policy affiliate at the Governance of AI project at Oxford University's Future of Humanity Institute.

When trying to decipher Europe's take on artificial intelligence (AI) and get a sense of where Europe is headed in terms of AI policies and capabilities, one is almost automatically driven to look at the European Union. The EU is a convenient object of study – it publishes its reports in English, and many translations, and all documents, are easily accessible. There is also good reason to look at the EU when it comes to AI, as it has – and in particular the new European Commission under the leadership of Ursula von der Leyen has – identified AI as one of its priorities. From 2018 onwards, the EU published a series of important policy documents, such as the Declaration on Cooperation on AI, the Communication on AI, and, most notably, the Coordinated Plan on Artificial Intelligence, from December 2018, which doubled as an early AI strategy for the EU. In 2019, the EU's High-Level Expert Group on AI – a group of 52 experts from academia, civil society, and industry – published their Ethics Guidelines for Trustworthy Artificial Intelligence, as well as policy and investment recommendations. Most recently, the commission published its White Paper on Artificial Intelligence, called "A European approach to excellence and trust". And the EU not only trades in words, but is putting real money behind its plans. The commission aims to increase AI investment (public and private) to €20 billion per year over the next decade, and in 2021 it plans to launch "Digital Europe", a programme focused on building the strategic digital capacities of the EU, which also includes billions for AI and supercomputers.

Given the EU's apparent prioritisation of the topic, its importance when it comes to regulation and questions of trade, and its own claims to represent "the European approach", it seems logical to focus on the EU as the main actor when trying to find out about Europe's take on AI and future plans. However, any analysis of Europe's thinking on AI needs to be complemented by the view from the member states.

There are several reasons one cannot just 'take the EU's word for it'. For one, there are only a few areas in which the EU has exclusive competences, such as in trade, whereas in others the EU can only act when member states agree to delegate powers to it, and when the member states agree on policy directions. Secondly, there are areas in which the EU does not so far play a role. This is most notably the case with regard to AI in the military sector. Although in recent years, and following the United Kingdom's departure, the EU has begun to strengthen its role in the defence sector, such as through the creation of the Permanent Structured Cooperation (PESCO) and the European Defence Fund, the member states remain by far the more important actors when it comes to defence. Furthermore, even in areas in which the EU has clear competences, member states' views still matter as they influence EU policies. Finally, even for those interested exclusively in the EU's plans and actions, it is important to keep an eye on member states' policies. Around the world, governments as well as experts are trying to get to grips with the technological, (geo)political, economic, and societal implications of AI. This means that a lot is in flux, as ideas get developed, discussed, and rejected or

AI-dedicated fundraising (US$M)



Source: Roland Berger

changed. The same is true for the EU and its member states, whose ideas, plans, and strategies are likely to adjust and change over time, and, importantly, likely to develop in interaction with each other.

The EU is aware of its limitations, and the need to interact with member states, and therefore in the Coordinated Plan it has asked all member states to put in place national AI strategies. As of May 2020, at least 18 of the 27 EU member states have followed this advice and published national strategies, draft programmes, or similar policy documents, namely, Austria, Belgium, the Czech Republic, Denmark, Estonia, France, Finland, Germany, Italy, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Spain, Sweden, and the UK. In addition, there are regional programmes and plans, such as the Declaration on AI in the Nordic-Baltic Region, and the Visegrad Group's thoughts on AI. Several other states have put together expert groups and are in the process of writing their national strategies.

A willingness to work together on a common European AI approach?

If the EU wants to play a coordinating role, and ultimately bring together its member states' plans on AI in a consolidated way, there needs to be an agreement among its members that cooperating on AI is beneficial, as opposed to pursuing national priorities. The Declaration of Cooperation on Artificial Intelligence from April 2018 was a good start to this; through this document, EU member states pledged to collaborate with one another in addressing social, economic, legal, and ethical questions related to AI, as well as to ensure that the EU becomes competitive in the area. The EU's Coordinated Plan, which aimed to establish the EU as a coordinating entity, was also useful as it encouraged member states to draft their own AI strategies. On the other hand, the fact that several EU member states had already published their national AI strategies by the time the EU's Coordinated Plan became public may have undermined its impact somewhat.

Looking at the pronouncements of the European 'big two', France and Germany, on AI one can see that the decision of when to go it alone, when to collaborate with selected partners, and when to delegate power to the EU is not an easy one. In their national AI strategies, the two countries support bilateral or multilateral cooperation and the simultaneous adoption of national and European goals. Their stated motivations for doing so, however, differ. In the German case, the focus on European – specifically, Franco-German – cooperation, appears to be a goal in itself, or the default idea. The French strategy, in contrast, adopts a more pragmatic approach – supporting European cooperation only in areas in which the strategy's authors consider it to be useful.

The French strategy's subheading is "Towards a French and European Strategy" and thus already includes the European angle in the headline. The strategy's foreword notes furthermore that "we cannot conceive AI in a purely national framework". There is a specific reason for France's interest in the EU as an actor: geopolitical concerns surrounding AI. The document notes that: "France and Europe need to ensure that their voices are heard and must do their utmost to remain independent. But there is a lot of competition: the United States and China are at the forefront of this technology and their investments far exceed those made in Europe." The strategy's authors worry that "France and Europe can already be regarded as 'cybercolonies' in many aspects". It is this geopolitical awareness that makes France push for a European rather than exclusively national approach. However, while the French approach sees European cooperation on AI as useful, its focus is on bilateral Franco-German collaboration. The French strategy deals with European cooperation in a practical way, identifying those areas it considers "particularly well suited to integration into a European scheme", such as transport and mobility. The strategy adds, however, that "the other priority sectors (health, defense and environment) do not lend themselves so easily to direct treatment at European level, although it would be useful to get Germany involved." The French strategy mentions Germany, as France's obvious main partner, multiple times. For example, it states that, "to start on [the] development of a European industrial policy on AI, our mission recommends that, initially, work should be carried out within a Franco-German axis." It then includes the other big European player, continuing: "Italy (the north in particular) should also be seen as a possible serious partner, all the more so because of its advances in the field of robotics" – an area in which it goes so far as to speak of a "Franco-German-Italian triptych".

The German strategy's subheading is "AI made in Germany", but this does not translate into a nationalist approach. In fact, the German strategy has a clear European, particularly Franco-German, focus. The terms "European", "EU", and "Europe" are mentioned around 90 times, and the stated goal is to make Germany and Europe world leaders in AI. Mirroring France's focus on the Franco-German axis, the German strategy mentions France more often than any other country. It plans to build a "virtual centre" of research and innovation institutes with France. Germany also wants to work on AI with the French Council on Innovation. Whereas the French motivation to collaborate on the European level is clearly founded on concerns over European's geopolitical power and ability to stand up to other actors, in particular the US and China, this approach is largely absent in the German thinking about AI. In fact, for Germany, working with European partners on AI appears more to be driven by a general conviction that this is the right thing to do, rather than a specific consideration. Interestingly, the geopolitical view so prominent in the French thinking is absent in the German take on AI.

France and Germany – how much do they agree?

Given the crucial role that France and Germany play in European politics, and given the states' economic power, as well as expertise and talent in AI and related areas, it is worth looking at the two countries' approaches to AI. Although one has to be cautious about making definitive statements because of the aforementioned provisional nature of AI policies and thinking at the moment, one also has to note that there are significant differences as to how France and Germany approach AI. If these differences persist – or deepen – this could cause problems for a common European approach.

France has shown a lot of interest in AI from early on. AI was made a top-level priority, with President Emmanuel Macron discussing the topic at length in a Wired interview in early 2018, just as France was launching its AI strategy. France's AI ecosystem is considered energetic; a study by Roland Berger found that within the EU France's start-up scene was leading with regard to (foreign) investment. Germany, according to the same study, came just behind France. Policy-wise, however, Germany was initially slow to address AI issues, though it sped up its activities from the second half of 2018 onwards. A commission of inquiry was formed, and

the national AI strategy was published in November 2018, complemented by public and expert hearing and other events.

The first important difference between the French and German approaches to AI, judging from the national AI strategies, is the lens through which the countries see AI. Whereas France, as mentioned above, considers AI an important element of geopolitics, and is worried about France's and Europe's position in the world due to AI developments, the German strategy adopts an economic lens. As the German strategy was written under the leadership of the ministries of education and research, economy and energy, and labour and social affairs, it primarily focuses on research, the economy, and society. It concentrates on preserving the strength of German industry – particularly small and medium-sized companies, the famous Mittelstand – by ensuring that AI will not allow other countries to overtake Germany economically. The government's hope is that AI will help the Mittelstand continue to manufacture world-leading products. The German approach to AI is thus markedly driven by fear of losing economic opportunities, causing it to adopt a defensive tone. A poll from 2018 found that 69 per cent of Germans believe that, because of AI, a "massive number of jobs" will be lost (a belief that is particularly prevalent among 16-24-year-olds), while 74 per cent worry that "when machines decide, the human element will be lost".

The contrast in tone is another interesting difference between the two countries. Where the German strategy expresses concern that AI may lead to a loss of economic power, the French strategy adopts a more upbeat tone, calling AI "one of the most fascinating scientific endeavors of our time". Cedric Villani, the French mathematician who led the group that wrote the strategy, in his foreword expresses the conviction that "France – and Europe as a whole – must act synergistically, with confidence and determination, to become part of the emerging AI revolution". This approach seems to accord with French citizens' beliefs: a recent IFOP poll found that 73 per cent of them have a positive or very positive view of AI.

A final area in which Franco-German differences currently appear most pronounced, is on the role AI could play in the military and defence realm. France views the military realm as an important element of its AI development efforts. The French strategy designates defence and security as one of its four priority AI sectors for industrial policy. (One of the authors of the strategy is an engineer from the French defence procurement agency.) The French Ministry of Defence also announced investments in AI research. Most notably, France, in September 2019, became the first European country to publish a military AI strategy, a report written by a team from the Ministry of Defence, with outside expertise. The document outlines France's approach to AI in the military, provides examples of AI-enabled military applications, and announces the creation of several bodies that will help the French military adopt AI. The military AI strategy follows the ideas of France's national AI strategy, adopting a similar geopolitical approach. It describes the US and China as AI "superpowers", and Europe as "an intermediate power in the making". France – together with Canada, Germany, Israel, Japan, Singapore, South Korea, and the UK – are part of the "second circle", in AI. The document repeatedly expresses concern about dependence on other countries (particularly private companies from other states) and adopts "preserving a heart of sovereignty" as one of its directing principles.

The military, security, and geopolitical elements of AI are markedly absent from the German national AI strategy. In fact, the strategy only features one sentence on security and defence, which shifts the responsibility for this area to the MoD. The strategy states: "with regard to new threat scenarios for internal and external security, in addition to research on civil security, the Federal Government [will] promote research to detect manipulated or automatically generated content in the context of cyber security. The research on AI applications, in particular for the protection of external security and for military purposes, will be carried out within the scope of the departmental responsibilities." Unfortunately, it seems unlikely that the German Ministry of Defence will follow France's example and publish a dedicated military AI strategy, outlining its views on AI in the military realm. Rather, the national strategy seems representative of Germany's generally cautious approach to military AI. A report for NATO's parliamentary assembly argues that, given AI's potential value to the armed forces, NATO's leaders in science and technology – such as France, Germany, the UK, and the United States – must invest in defence-related AI research and development. But the report singles out Germany as lagging in this area, commenting: "it is encouraging to see that all of them are indeed investing substantial resources into defence-related AI, with the possible exception of Germany." So far, the public and political debate on AI in the military in Germany focuses primarily on autonomous weapon systems, and efforts to control them. The Foreign Ministry organised an international conference on the topic in March 2019, and has held a series of follow-up meetings.

The national AI strategy's reference to "departmental responsibilities" could be interpreted as giving the German Ministry of Defence a mandate to develop its own strategy on the military applications of AI. However, given the Ministry of Defence's track record of rarely, if ever, publishing doctrinal documents, it is unlikely that the ministry will do so publicly. (That being said, in October 2019, the unit of the army charged with developing new concepts and ideas for ground forces surprised most experts by publishing a position paper entitled Artificial Intelligence in the Land Forces. However, the paper is somewhat disconnected from other German publications, and has no direct impact on German government or Ministry of Defence actions. Indeed, and, as one of the paper's authors said in a private conversation, the Ministry of Defence was not particularly pleased with its publication. It is unclear what will become of the concepts developed in the position paper.)

Hence, whereas France considers military applications an important element of AI, Germany, for the moment, shies away from the topic. This is likely to make future coordination on the topic difficult. This is particularly noteworthy and concerning given the two big-ticket military projects France and Germany are currently developing jointly – the Future Combat Air System (FCAS) and the Main Ground Combat System. FCAS in particular is expected to feature AI elements.

Ethical AI – the way forward for Europe?

While there are noteworthy differences in how France and Germany approach AI, as outlined above, there are also many areas on which the two countries – and others in Europe – agree. This is most notably the case with regard to 'ethical AI'. The EU has articulated the ambition to become "the world-leading region for developing and deploying cutting-edge, ethical and secure AI." The EU pursues two goals with its focus on ethics. Firstly, it follows the analysis of many experts who have pointed out the importance of including ethical considerations into AI development and application. The EU hopes to not only set standards for its own citizens and companies, but also, though its global regulatory reach (dubbed the "Brussels effect"), to influence foreign actors to follow the European lead. Secondly, and somewhat more contested, the European Commission hopes that this focus on ethical AI may in the long run give European companies a lead. The Coordinated Plan states that for the EU, "[s]pearheading the ethics agenda, while fostering innovation, has the potential to become a competitive advantage for European businesses on the global marketplace." The idea is that as more consumers realise the importance of data privacy, and ethical conduct, European firms following ethical AI rules will be at an advantage.

For both France and Germany, the idea of ethical and trustworthy AI holds a lot of appeal. The German government sees "ethical and legal requirements" as an integral part and a future "trademark", of AI made in Germany. The strategy sets out three major objectives, the third of which is "integrating AI in society in ethical, legal, cultural and institutional terms in the context of a broad societal dialogue and active political measures". The strategy specifically mentions European cooperation on this point: "Greater cooperation within Europe, but also internationally, is essential for many challenges for [...] a human-centered use of AI, especially when it comes to uniform and ethically demanding rules for the use of AI technologies in Europe." Ethics is also the area of discussion with regard to military AI that Germany is most comfortable with, which may present an opening for European deliberations on military AI. The French strategy also has a section on the ethics of AI, which recommends "implementing Ethics by design", i.e. during the development process, as "they cannot be integrated a posteriori." The strategy notes the importance of transparency, inclusivity, and diversity. Related to ethics is the importance of data privacy, which equally plays a crucial role for both France and Germany. Furthermore, on ethics, Europe may also consider working with the UK, which equally has shown a lot of interest in and work on ethical AI.

As AI policies around the world are being devised and in flux, and given that Europe is composed of 27 EU member states, the EU institutions themselves, and numerous other non-EU European countries, it is impossible to define "the European approach to AI" in any finality. Nevertheless, this analysis of the EU's, France's, and Germany's current thinking has shown that there are already interesting and noteworthy differences in how the actors approach AI. More coordination, both bilaterally, and on the European level, is needed in order to soften, rather than deepen, these differences.

Project note: In search of Europe’s digital sovereignty

Carla Hobbs

Europe’s Digital Power Project coordinator, European Council on Foreign Relations

Over the past five years, Europe has become a global trailblazer in digital policymaking – to both the admiration and exasperation of many. Ditching its previous laissez-faire attitude to tech regulation in favour of an assertive approach, the European Union has actively intervened to raise privacy standards, levy landmark antitrust fines on tech companies, and shape the debate on issues such as online harms and ethical artificial intelligence. And by the looks of things, it is just getting started.

This shift took place under the Juncker commission amid mounting realisation that Europe had to protect its values, interests, and citizens in a digital space that was gradually becoming a geopolitical and geoeconomic battleground. Lacking the tech credentials to compete with China and the United States as a digital player, the EU instead began to shape the digital ecosystem by exercising its regulatory power to introduce extraterritorial rules binding all those who wished to interact with its single market and consumers. As EU internal market commissioner Thierry Breton said, “it is not us that need to adapt to today’s platforms. It is the platforms that need to adapt to Europe.”

The result is that today the EU is the world’s leading digital regulatory power. But is regulatory power enough to protect Europe’s interests and vision for the internet and digital technologies? If so, what comes next after the milestone 2016 General Data Protection Regulation? How can we ensure regulation does not damage the internet´s essence and founding values, or make it less attractive, profitable, or useful? Must the EU continue to work unilaterally on digital issues or is there scope for transatlantic or other alliances?

It was with these questions in mind that ECFR launched the ‘Europe’s Digital Power’ project in collaboration with Telefónica in 2019. This essay collection forms a major part of that project. The team hit the road, travelling to London in May 2019, Berlin in September, Washington, DC in October, and – virtually – Brussels in June 2020 to pose them to over one hundred policymakers, regulators, tech giants, academics, and others in a series of workshops. (The conclusions of each workshop are publicly available at ecfr.eu/digitalpower).

Several key messages and recommendations emerged from these discussions. On the question of regulation itself, while there was significant divergence of opinion on the scale and methods to be employed, most of interlocutors agreed that a measure of government intervention is necessary to mitigate the harmful effects of the internet. Regulation should be agile and flexible, developed via an iterative process that mirrors the dynamism of the industry it seeks to shape. Regulation should also be proportional and nuanced, aimed at creating a safer system overall in which freedom of speech and innovation can still flourish.

To achieve this, Europe will need informed and sufficiently resourced policymakers and judges who can deal with the scale, complexity, and jurisdictional challenges posed by internet regulation. Here, the tech community has an important role to play in educating them and sharing essential data to reduce information asymmetries. This links to the question of private-public internet co-governance, which interlocutors agreed will be essential moving forward given companies – which own much of world's digital infrastructure – are best placed to enforce rules while regulators can better decide what those rules and limits should be. As such, a continued preference for the multi-stakeholder approach to internet regulation emerged from the workshop discussions. There was also, however, a recognition that the model needs significant improvement if it is to be an effective policymaking and implementing tool given its slow and diffuse operation and lack of incentives for accountability.

In terms of the bigger geopolitical picture, American stakeholders urged their European counterparts to resist viewing the US and EU as equidistant points in a triangle with China. Instead, they argue, these are two allies that share more similarities than differences, such as support for open society values online. This could provide fertile ground upon which to develop a common transatlantic position. This common position would then hold significant sway in defining the norms that govern the digital ecosystem and the direction that pivotal players, such as India, may take.

Lastly, there was overwhelming consensus on one point: that Europe must evolve from a regulatory superpower to a tech superpower if it hopes to truly safeguard its values and interests in the digital space, reap the economic benefits of emerging digital technologies, and keep Europeans safe from disinformation and cyber attacks. Thus far, Europe has been more concerned with writing the rules of the game than playing it, with the bloc continuing to trail behind China and US in developing leading tech solutions and companies. But as one participant pointed out, "referees don't win". The EU must complement its regulatory clout with investments in digital infrastructure, skills, and industry in order to become a digital player in its own right.

If there were any lingering doubts on this last point, the onset of the coronavirus pandemic in Europe has vanquished them, instilling a new level of awareness in societies, governments, and businesses about the critical importance of digital technologies for Europe's economic and health resilience. Europeans' complete dependence on technology to not only sustain the economy as millions worked from home during lockdown, but to even combat the virus itself, overnight made Europe's digital transformation a question of existential importance. Rising tensions and digital decoupling between China and the US during the pandemic added an additional element of urgency, with Europe no longer able to simply spectate but instead forced to pick a lane or define its own.

This is not to say that Europe's digital transformation was not a priority before the pandemic. In fact, "Making Europe fit for the digital age" ranked third among the European Commission's list of objectives for 2019-2024, a prioritisation evidenced by a raft of legislative initiatives on artificial intelligence, data, and other areas, all published just a month before European lockdowns began. Indeed, EU officials were quick to point out during the Brussels workshop that the pandemic experience had validated the EU's digital policy agenda and will strengthen the case for increased financial resources to back it up.

Yet while the motive, money, and mindset might be there, that leaves the method – which is by no means the easy part. Participants in the Brussels discussion argued that Europe might have missed the first generation of digital transformation, but it could position itself to compete in the forthcoming wave of technology, such as edge computing, in which European companies have several competitive advantages. The EU can also continue to shape the digital environment by exercising its regulatory power via, for example, creating a European cloud federation that requires those seeking admission to adhere to EU standards. Lastly, it can also export its model to like-minded democracies around the world and build an alliance with them to increase backing for it.

The challenges are still undeniably many, ranging from member state disunity on tech issues to the unhappy marriage between Europe's rules-first approach and its bid to boost homegrown tech solutions and innovation. But what had become apparent by the end of the project was that Europe was determined to surmount these challenges, its digital resilience and sovereignty no longer a question of 'if' and 'when' but 'how' and 'now'.

It was in this context that this essay collection was born. ECFR invited selected stakeholders who had participated in the four workshops to share their thoughts on how the EU can enhance its digital sovereignty in a post-coronavirus context in areas ranging from 5G to broadband, and cloud computing to disinformation.

I hope that the recommendations prove helpful for readers, and that the collection's central message inspires policymakers, businesses, and civil society alike. Europe has a unique opportunity to turbocharge its digital transformation and achieve greater technological independence and resilience. It cannot afford to miss out.

About the authors

This essay collection that was originally published in July 2020 is the result of the collaboration between the European Council on Foreign Relations (ECFR) and Telefonica that began with the celebration of a series of workshops in London, Berlin, Washington, and Brussels followed by a public event in Madrid. Each workshop brought together approximately 20 to 25 experts and leading professionals from the private sector, academia, government, tech platforms, and civil society to share their views under Chatham House Rule on how Europe can become a relevant actor in the digital arena and safeguard its values and interests in this contested space. These discussions were the origin that led to the publication of the various views on this issue in this work that finally comes to light.

José María Álvarez-Pallete

is chairman and CEO of Telefónica S.A, a position he has held since 2016. He joined the Telefónica Group in 1999 and went on to hold various positions as a general manager of Finance for Telefónica Internacional, and later that same year he became chief financial officer of Telefónica S.A. In 2002 he was appointed chairman and CEO of Telefónica Internacional. Between 2006 and 2011 he was managing director of Telefónica Latin America. He was appointed chairman and CEO of Telefónica Europe in 2011, and was appointed chief operating officer of Telefónica, S.A. in 2012. He holds a degree in Economics from the Complutense University of Madrid, studied Economics at the Free University of Brussels, and holds an International Management Programme from IPADE.

Anthony Giddens

is a Life Fellow of King's College Cambridge and Emeritus Professor at the London School of Economics. He was Director of the LSE from 1997 to 2003, and was made a member of the House of Lords in 2004. Lord Giddens has honorary degrees or comparable awards from more than 20 universities. He co-founded the publishing house Polity Press, which today produces 150 titles a year. Giddens is an ECFR Council Member.

Jeremy Shapiro

is the research director of the European Council on Foreign Relations. Previously, he was a fellow at the Brookings Institution in Washington, DC. Prior to Brookings, he was a member of the US State Department's policy planning staff and the senior adviser to assistant secretary of state for European and Eurasian affairs.

Andrew Puddephatt OBE

is the executive chair of Global Partners Digital's Advisory Board, a company that promotes democracy and human rights online, and chair of the Internet Watch Foundation, a charity that protects children online. He also chairs the Danish based International Media Support and is deputy chair of the Sigrid Rausing Trust. Prior to this, Puddephatt was the Executive Director of ARTICLE 19 among other positions. He has been an expert member of the Council of Europe and the Commonwealth Expert working groups on freedom of information and freedom of expression and is an advisor to UNESCO on media and internet policy. He is an ECFR Council Member.

Janka Oertel

is the director of the Asia Programme for the European Council on Foreign Relations. She previously worked as a senior fellow in the Asia programme at the German Marshall Fund of the United States' Berlin office, where she focused on transatlantic China policy including on emerging technologies, Chinese foreign policy and security in East Asia. Prior to joining GMF, she served as a Program Director at Körber Foundation's Berlin office. She holds a PhD from the University of Jena.

Andrés Ortega Klein

is a senior research fellow at the Elcano Royal Institute, an independent consultant and director of the Observatorio de las Ideas. He was the director of the Department of Analysis and Studies (Policy Unit) at the Prime Minister's Office twice and also worked as counsellor at the Spanish Ministry of Foreign Affairs and Cooperation. He has developed an extensive career in journalism as London and Brussels correspondent and columnist and editorial writer for El País. Ortega Klein holds a BA in Political Science from the Complutense University of Madrid and an M.Sc. (Econ) in International Relations at the London School of Economics. He is an ECFR Council Member.

Frances G Burwell

is a distinguished fellow at the Atlantic Council and a senior director at McLarty Associates. Until January 2017, she served as vice president, European Union and Special Initiatives, at the Council. She has served as director of the Atlantic Council's Program on Transatlantic Relations, and as interim director of the Global Business and Economics Program, and currently directs the Transatlantic Digital Marketplace Initiative. Her work focuses on the European Union and US-EU relations as well as a range of transatlantic economic, political, and defense issues.

Andrea Renda

is a senior research fellow and head of global governance, regulation, innovation, and the digital economy (GRID) at the Centre for European Policy Studies (CEPS). He is currently a non-resident senior fellow at Duke University's Kenan Institute for Ethics, and was Adjunct Professor of Law and Economics at Duke Law School (United States) for Academic Year 2016/2017. Since September 2017, he holds the "Google Chair" for Digital Innovation at the College of Europe in Bruges (Belgium). He is a member of the EU High Level Expert Group on Artificial Intelligence.

José Ignacio Torreblanca

is a senior policy fellow and Head of the Madrid office of the European Council on Foreign Relations and Professor of Political Science at the Universidad Nacional de Educación a Distancia (UNED). He is also a weekly columnist in EL MUNDO as author of the blog "Café Steiner" and a contributor on RNE. Previously, he was Editorial Director of EL PAIS (2016-2018) and prior to that, he was the first director of the ECFR Madrid Office (2007-2016) following the launch of ECFR across Europe. Torreblanca holds a PhD in Political Science from the Complutense University of Madrid (UCM).

Alicia Richart

is the founder and CEO of Digitales, a non-profit start-up that aims to promote the digital transformation of Spain. Prior to this, Richart worked in the Cabinet of the Spanish Minister of Industry, Energy and Tourism as an advisor where she led the Industry 4.0 program and the update of the Spanish General Telecommunications Law (2014). From 2012 to 2014, Richart was the Spanish Digital Champion, appointed by the European Commission. She is an industrial engineer, graduating from the Chemical Institute of Sarrià (1999), and has an MBA from the Esade Business School (2005).

Ulrike Franke

is a policy fellow at the European Council on Foreign Relations and a policy affiliate at the Governance of AI project at Oxford University's Future of Humanity Institute. She holds a PhD in International Relations from the University of Oxford, a BA from Sciences Po Paris and a double summa cum laude MA degree from Sciences Po Paris (Affaires internationales/Sécurité internationale) and the University of St. Gallen (International Affairs and Governance). Her areas of focus include German and European security and defence, the future of warfare, and the impact of new technologies such as drones and artificial intelligence.

Carla Hobbs

Carla Hobbs is the Europe's Digital Power project coordinator and Madrid programme coordinator at the European Council on Foreign Relations. She previously worked at the European External Action Service as a political officer in the Delegation of the European Union to Chile and as a Junior Professional in the Delegation to Trinidad and Tobago. Prior to this, she was a research assistant in the ECFR Madrid Office, directly supporting the head of office José Ignacio Torreblanca. Hobbs holds a joint Bachelor's and Master's degree in History from the University of Edinburgh and a Master's degree in International Journalism from City University London.

Acknowledgements

This essay collection is the product of the Europe's Digital Power project, a collaboration between the European Council on Foreign Relations and Telefónica. We would like to warmly thank Telefónica for their support. We are also grateful to all the participants in the project workshops who shared their expertise and insights on digital affairs with us and to those that partnered with us on project events including the Spanish Embassy in Washington, DC, the Carnegie Endowment for International Peace, and the Centre for European Policy Studies. For their invaluable input and involvement throughout the project, we would like to thank all our colleagues at ECFR.

Telefonica DIGITAL POLICY LAB

This text was originally published by ECFR as a part of an ongoing research project with Telefonica