DIGITALISATION FOR SUSTAINABLE INFRASTRUCTURE: THE ROAD AHEAD

edited by **Carlo Secchi** and **Alessandro Gili**

with the knowledge partnership of

McKinsey & Company

ISPI

DIGITALISATION FOR SUSTAINABLE INFRASTRUCTURE: THE ROAD AHEAD

edited by Carlo Secchi and Alessandro Gili

ISPI

Via Antonio Boselli, 10 – 20136 Milan – Italy
www.ledizioni.it
info@ledizioni.it

Digitalisation for Sustainable Infrastructure: The Road Ahead
Edited by Carlo Secchi and Alessandro Gili

First edition: October 2022

Print ISBN 9788855267908
ePub ISBN 9788855267915
Pdf ISBN 9788855267922
DOI 10.14672/55267908

ISPI. Via Clerici, 5
20121, Milan
www.ispionline.it

Catalogue and reprints information: www.ledizioni.it

This study is an initiative of the ISPI's Centre on Infrastructure, promoted with the knowledge partnership of McKinsey & Company. The Centre on Infrastructure focuses on how geopolitical and economic trends shape and are shaped by investment decisions on infrastructural projects. It aims to analyse global trends (new technologies, mobility, sustainability, etc.) and monitor major projects, also with a view to gauging their complementarity/competition and financing channels. Specific attention is devoted to the role of key economic and political players at all levels – from local to global – including regional and international development banks, whose "political" agenda is often crucial to foster public and private investment.

Table of Contents

PART II - SECTORS

PART III - COUNTRIES

Introduction

In today's tumultuous and fast-changing times, digitalisation and technology are game changers for a wide range of sectors and have a tremendous impact on infrastructure in particular. Roads, railways, electricity grids, aviation and maritime transport are deeply affected by the digital and technological transition, with gains in terms of competitiveness, cost-reduction and safety. But society as a whole is experiencing a profound upheaval: people are having to adapt their consumption, mobility and preferences to the new possibilities offered by transforming digital solutions. The first part of this volume is devoted to the economic and geopolitical implications of the digital race. The digital economy currently accounts for about 15% of global GDP. Since the pandemic, it has grown rapidly, impacting both the private and the public sectors. Areas and companies that have adopted broadband and digital services are now more competitive and have better economic prospects. Moreover, digital infrastructure, artificial intelligence and the Internet of Things are key to promoting the birth of new economic sectors, services and products.

The infrastructure sector is faced with the challenge of rethinking itself digitally and adapting a smart paradigm. Buildings, bridges, roads, and major construction projects could provide feedback on their maintenance or operation status to improve the management of the entire system. Such a new paradigm would be based on IoT (Internet of Things) technologies. Environmental accelerometers, inclinometers

and extensometers, for example, can help monitor the status of infrastructures in real-time and throughout their entire lifecycle. Digitalisation is also a key tool for fostering global commitment to sustainability and green transition: digital technologies can reduce the energy consumption of consumers and companies, reduce traffic congestion, and improve rail and air transport.

The race for digital infrastructure is also a geopolitical one. In the contemporary landscape, significant problems exist when it comes to reconciling the concepts of national sovereignty with the borderless, open and universal nature of the digital space in which data flow. Many countries are trying to achieve digital sovereignty, and this goal could be at the expense of global technological development and market opportunities. Controversy exists among the main global players and a level playing field is far from being agreed upon. The United States and China are the main actors in the global competition for technological and digital leadership. From chips to 5G, from artificial intelligence to supercomputers, the two Great Powers are struggling to lead the industrial and technological race not only within national borders but also abroad. Europe stands in between and, in the recent past, the European Union has had to strike a balance between competitive supplies from China and pressures from the US to ban Chinese digital hardware, particularly that destined for installation in critical infrastructure. More recently, the EU has stressed the importance of progressively becoming a digital and technological powerhouse and a worldwide leader in the development of new standards. The EU Commission has adopted several strategies to increase European strategic autonomy in the field of digitalisation and technology, partly by fostering and strengthening European industry.

Moreover, at the global level, standard setting – once confined to technical bodies – has also acquired a geopolitical dimension and is more and more subject to competition between China, the US and the EU. Against a backdrop of rising geopolitical tensions in the field of technology, securing critical national infrastructure (CNI) is a daunting challenge for policymakers. Recent events, such as the ransomware attack on the Colonial Oil Pipeline

on the US East coast, have demonstrated the vulnerability of strategic infrastructure and the urgent need to address it. Cyber protection strategies have thus been adopted both in the US and in the EU, with the ultimate goal of strengthening the security of strategic infrastructure and ensuring greater resilience.

The second part of this report focuses on the digitalisation of infrastructure and how this will affect different sectors. When it comes to road transport, digitalisation could have a disruptive impact. Advances in smart infrastructure could lead to road networks becoming smarter, greener, more efficient, safer and more resilient. An array of innovative solutions exists today that are readily implementable and can lead to reductions in emissions, delay times, energy consumption and other key indicators, while maintaining or even improving safety levels overall. For railway transport, digitalisation means a denser flow of information on traffic and tracking, easier passenger access to services and information, more efficient use of infrastructure capacity and a higher degree of predictability on timing. Digitalisation is also key to improving the efficiency of air traffic, in order to meet performance targets while building resilience through flexibility and scalability to cope with crisis situations. Introducing new technologies will also improve the way aircraft fly through airspace, reducing fuel emissions on a flight-by-flight basis. Digitalisation is thus key to aviation meeting its decarbonisation commitments and achieving carbon neutrality. At the same time, container port automation is at the core of digital and technological strategies for maritime freight transport and port organisation. Smart port strategies are being adopted around the world to make national ports more efficient and more competitive internationally. The energy sector too is undergoing a steady process of innovation, with smart grids becoming increasingly important. These innovative grids coordinate the needs and capabilities of generators, grid operators, end users and electricity market stakeholders to operate all parts of the system as efficiently as possible, minimising costs and environmental impact while maximising system reliability, resilience, flexibility and stability.

In all sectors, cutting-edge technologies and digitalisation are transforming future outlooks, labour organisation and international competition.

The third part of the report is devoted to the digital and technological strategies adopted by the world's leading nations. The Great Powers are striving to foster the rapid digitalisation of their economies and to make their industries more competitive in a challenging international environment.

The US is pursuing a double-pillars strategy: on the one hand, the country is striving to foster digital transformation for enterprises and households, in order to improve competitiveness and maintain technological leadership; on the other one, the United States is committed to counter China's investment in developing countries, especially in the Indo-Pacific region.

China has identified digitalisation, along with innovation, as pillars of future socioeconomic development. The Digital China strategy – a centrepiece of China's 14th Five-Year Plan (FYP) – envisages a smart information society in which Big Data, AI and other emerging technologies make government and public services such as healthcare and education more efficient and inclusive. Moreover, since 2015 – with the establishment of the Digital Silk Road (DSR) – China has emerged as a major exporter of digital infrastructure, investing billions of dollars in connectivity and digital infrastructure projects abroad, mainly in Asia and Africa. On the African continent in particular, Big Tech companies from the US, Europe, China and Russia are playing a high-stakes game to gain market shares. Challenged by the digital divide and lack of domestic private investments, African countries are eager to welcome foreign investment to improve connectivity and growth potential. Japan, once an undiscussed technological giant, has found itself lagging behind in digital and technological investments compared to China, and is now trying to catch up. Digital transformation (DX) is at the core of the Japanese strategy for industrial and technological development, with increasing investments in industry and infrastructure. Finally, Europe too is trying to reduce its digital and technological dependencies and increase strategic autonomy

in cutting-edge technologies and in the digital sector. This goal is at the core of Next Generation EU (NGEU), the €750 billion plan focused on a sustainable and digital post-pandemic recovery. Indeed, 20% of overall funding will be devoted to the digital transition and to improving internal connectivity within the EU, with benefits for citizens and enterprises. However, NGEU is not the only instrument in the EU toolbox: the Digital Compass, the EU Artificial Intelligence Strategy, the Chips Act, the EU Cyber Resilience Act, and initiatives on super and quantum computers all aim at scaling up digital and technological investments in Europe. However, to be successful, EU strategies need increasing investment and participation from the private sector. The European Investment Bank (EIB) is at the forefront of digital investments in Europe and is increasing connectivity investments in the neighbourhood too, through the NDICI[1] – Global Europe.

It is clearly recognised that digitalisation is a multi-faceted process with disruptive impacts on many aspects of the economy and geopolitics. Infrastructure, industry, and society are all affected as the digitalisation process moves forward. Alongside sustainability, digitalisation is one of the two main pillars that must underpin future economic growth. But investments in digitalisation and technology also entail new geopolitical tensions, as witnessed by the many different digital and technological strategies presently being enacted worldwide. The pandemic and the war in Ukraine have shed further light on the importance of technology and digital infrastructure in the contemporary economy and geopolitics. They also remind us that an agreed set of rules and standards must be reached internationally to allow digitalisation and future technological developments to thrive in an orderly and efficient manner.

C.S.
A.G.

[1] Neighbourhood, Development and International Cooperation Instrument (NDICI).

PART I
TRENDS

1. The Geopolitics of Tech and Digital Space: A Struggle for Future Leadership

Alessandro Gili

In the "age of accelerations" we are living in, technology is increasingly shaping societies, economies and culture. It is undeniable that technology and digital infrastructure have played a key role in the most challenging issues we are facing in our time. From the pandemic to the climate crisis and the war in Ukraine, digital infrastructure and technology are game changers. Digital technologies have become an imperative for working, learning, socialising, shopping and accessing everything from health services to culture. And technology is also changing geopolitics and the determinants of power. In the XIX and XX centuries a large population, good raw materials endowment, a heavy industry and geographic dimension were the main elements for being recognised as a Great Power by the international community. Today, things are progressively and rapidly changing. Technology and digital have entered the geopolitical arena as key enablers of power. Competition in this field is now one of the main components of the struggle for primacy among Great Powers. And the main reasons are crystal clear.

The Economic Dimension

The digital economy is equivalent to 15.5% of global GDP, growing two and a half times faster than global GDP over the past 15 years.[1] In the EU it accounts for 6.5% of GDP and 9% in the US.[2] Global Internet traffic in 2022 will exceed all Internet traffic up to 2016. This trend has been boosted and accelerated in particular because of the pandemic, which had a tremendous impact on Internet traffic when the entire world went online. Against this backdrop, the traditional divide between developed and developing countries remains unchanged and represents a key hindrance to development. Only 20% of people in least developed countries (LDCs) use the Internet, usually with low bandwidth and speed as well as high prices attached. Furthermore, the nature of use is different: for instance, 8 in 10 Internet users shop online in developed countries while that figure is less than 1 in 10 in most of LDCs. Finally, gaps also persist between rural and urban areas, as well as between men and women. An estimated 37% of the world's population – equal to 2.9 billion people – has still never used the Internet, and this constitutes a major obstacle to the full development of affected areas. It is estimated that a 10% increase in mobile broadband penetration in Africa would result in an increase of 2.5% in GDP per capita.[3] In the advanced world, and in Europe in particular, according to the McKinsey Global Institute, half of Europe's workforce will have to cope with a significant transition and almost all workers will gain new skills; as a result, 21 million people will need to change their jobs by 2030[4]. In the US the situation is similar: 47% of American workers will see their work automated by 2040.[5]

---

[1] World Bank, Digital Developments, 20 April 2022.

[2] European Central Bank (ECB), "The Digital Economy and the Euro Area", ECB Economic Bullettin, Issue 8/2020.

[3] International Telecommunication Union (ITU), "Economic contribution of broadband, digitization and ICT regulation", 2019.

[4] S. Smit, T. Tacke, S. Lund, J. Manyika, and L .Thiel, "The Future of Work in Europe: Automation, Workforce Transitions, and the Shifting Geography of Employment", McKinsey Global Institute, 10 June 2020.

[5] C. Frey and M. Osborne, "The Future of Employment: How Susceptible

Digital and tech also mean geopolitics

In the contemporary landscape there are significant problems when it comes to reconciling the concept of national sovereignty and the borderless nature, openness and universality of the digital space where data flow. Many countries are trying to adopt national strategies to compel providers to store data within national borders and this could ultimately lead to a risk of fragmentation in the digital space and on the Internet. This kind of development would result in a suboptimal outcome in economic terms and reduce business opportunities by hampering technological progress, enabling the oligopolistic market structure to emerge and reducing competition.[6] Many countries are trying to achieve digital sovereignty, and this goal could be at the expense of global technologic development. As a result, deep disagreements continue to exist at the international level among the main players, in particular within the G20, and a level playing field in this domain seems still far from being agreed upon.

Today, the digital and technological race is primarily a US-China struggle for primacy. Against the backdrop of a more comprehensive geopolitical and geoeconomic rivalry, the two great powers have elected the technological and digital domain as the core of a broader industrial competition. This is confirmed by ranking of the largest tech companies by market capitalisation. In the top 20, ten are American, four are Chinese, two Japanese, two South Korean, two Taiwanese and none from the EU. American companies still dominate the tech market, but Chinese companies are growing at a fast pace.[7]

The Sino-American technological rivalry accelerated in the aftermath of Donald Trump's election as President of the

---

Are Yobs to Computerization?", Oxford Martin School, Oxford University, 1 September 2013.

[6] United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2021*.

[7] See *Fortune Global 500*.

United States. His predecessor President Obama's "Open Door Policy", aimed at opening up markets and preserving American technological leadership through its tech giants, was rapidly replaced by Trump's "technological decoupling" initiative. The 5G rollout, in particular, was the cornerstone of renewed US-China geoeconomic tension, with significant effects also on allied countries. In May 2019, Trump banned Huawei from US 5G networks, thereafter barring all sales of American technology to Huawei without official authorisation. Simultaneously, US authorities were entrusted with evaluating whether a transfer of any technology could harm critical infrastructure, the digital economy and national security. In particular, when a technology transfer could result in an (even indirect) advantage for a foreign adversary, US authorities had the power to block it. This kind of sanction is built on export control mechanisms aimed at depriving China (and Huawei in particular) of access to the American market and US technological know-how. In 2019 the US was seriously worried about losing its technological edge, since Huawei was the only company with the ability to cover the entire 5G value chain: no other US companies had a similar advantage at the time. By barring Chinese companies from entering the US market, the American Administration restrained Huawei's international expansion and reaffirmed America's ability to strongly influence global economic affairs, including in the technological field. On the other hand, US actions had the effect of strengthening China's state control over tech companies and the perception that even the most globalised and Western-oriented Chinese companies cannot survive without the support of the Communist Party. US sanctions could thus have boosted a secondary trend by encouraging Beijing to foster state-funded innovation and technological self-sufficiency.[8] The Biden Administration, following the path of the Trump Administration before it, is

[8] J. Nocetti, "Europe and the Geopolitics of 5G. Walking a Technological Tightrope", IFRI, January 2022.

committed to maintaining its digital and tech policy towards China and has called on EU allies to ban the installation of Chinese hardware and software in critical infrastructure. One of America's asymmetric advantages in technological competition is its ability to build international coalitions for accelerating innovation, in particular with EU and Indo-Pacific countries.[9]

China, on the other hand, has focused on its Made in China 2025 Plan to develop ten key sectors: Beijing is committed to becoming a leader in ten industrial sectors, among them Artificial Intelligence, the Internet of Things, robotics and machine learning. China stresses the importance of indigenous innovation and has launched an effort to reduce reliance on US technology for its value chain. Most recently, China's Premier Li Keqiang announced that the country will increase its research and development (R&D) spending over the next five years, with the ultimate goal of making major breakthroughs in technology. Accordingly, China's R&D spending will increase by more than 7% per year until 2025.[10] However, in recent years Beijing has often used its State-Owned Enterprises (SOEs) as a trojan horse to take over EU or US high-tech companies and acquire their technology for its national industries. A major example was the takeover of the German robotics maker Kuka by the Chinese enterprise Midea in 2016, followed by many other cases.[11] This also led the EU Commission to adopt a new Foreign Direct Investment (FDIs) screening mechanism in March 2019, fully implemented in October 2020. However, this screening mechanism only aims to foster coordination among Member States, in particular when an FDI could impact the EU single market, but this tool has limited effectiveness due to

[9] Ryan Hass et al., "U.S. - China technology competition", The Brookings Institutions, 23 December 2021.

[10] M Burrows, J. Mueller-Kaler, K. Oksanen, and O. Piironen, "Unpacking the Geopolitics of Technology", Atlantic Council, 2022.

[11] E. Braw, "Cutting-edge tech takeovers are a strategic threat to the west", *Financial Times*, 7 October 2019.

its non-binding nature.[12] Investment screening powers thus remains primarily in the hands of Member States.

Europe faces a tough challenge in the industrial and geopolitical landscape. The Old Continent has been somewhat paralysed in recent years by rising Sino-American tech tensions and torn between increasing tech trade with China (also with associated security risks) and US pressures to phase out any Chinese software and hardware in the digital and tech field, in particular for critical infrastructure and 5G. EU countries have faced challenges when trying to strike a balance between economic competitiveness on the one hand and strategic autonomy and security risks on the other. Moreover, the pandemic and the war in Ukraine – with the massive disruption of global and regional value chains – have demonstrated the urgent need to achieve strategic autonomy, including in the technological, digital and semiconductor sectors, and to reduce critical dependencies. The pandemic crisis exposed the vulnerabilities of the EU's digital space, its increased dependency on critical and often non-EU-based technologies, with reliance on a few tech companies. Moreover, data produced in Europe is generally stored and processed outside Europe, as is its value, which is extracted in other countries. This situation entails high risks in terms of cybersecurity and supply vulnerabilities, as well as possible unlawful access to data by third countries. EU-based cloud providers have only a small share of the cloud market, which leaves the EU exposed to risks and limits the investment potential for the European digital industry in the data processing market.[13]

The EU is now working on this matter and introducing several Strategies to increase its technological and industrial sovereignty. Brussels is striving to attain greater tech sovereignty through the EU Industrial Strategy, the EU Digital Compass, the EU

[12] European Commission, "EU foreign investment screening mechanism becomes fully operational", Press release, 9 October 2020.

[13] European Commission, "2030 Digital Compass: the European way for the Digital Decade", COM(2021) 118 final, 9 March 2021.

Data Strategy, the EU Chips Act and other digital initiatives. Nevertheless, the role of the European Union as a geopolitical actor is often jeopardised by Member States' different positions on several issues. The European Union lags behind when it comes to private investments in disruptive technologies, but it is trying to catch up, with the ultimate goal of taking the lead on responsible digitalisation and addressing the challenges of tech and digital industries through regulation. If successful, the EU could progressively elevate its role as a worldwide standard setter in the digital and tech fields, also outside the boundaries of the single market. As pointed out, some core weaknesses, such as the lack of big European tech companies and insufficient investment in research and development in the Internet and software, remain critical. However, some of these shortcomings will probably be addressed through the Next Generation EU plan, where 20% of the €750 billion fund must be allocated to digital-related investments.[14] Moreover, after the pandemic, something started to change. In the past, the major technological innovations produced within Europe's world-leading academic institutions hardly ever turned into commercial enterprises – partly because of a more conservative investment policy than the more risk-oriented US – and Europe has played a minor role in the biggest technological cycles of the past 50 years (such as the development of the PC, the evolution of software, the growth of mobile technology and Web 2.0). But the European tech ecosystem is steadily improving: in 2021 $93 billion was invested in European startups, a threefold increase from 2020. New unicorns are emerging across the continent, and they are no longer concentrated in core hubs such as Berlin or Paris, but hubs are also emerging in smaller countries such as Estonia. As a result, 28 European tech companies reached unicorn status in the first quarter of 2022, demonstrating that Europe is capable of not only producing high-quality tech and digital research

[14] Council of the European Union, "A Recovery Plan for Europe", last reviewed on 22 June 2022.

in academia but also building world-leading technology companies.[15]

Deployment of 5G in Europe was one of the main battlefields of the US-China tech war, with EU countries assuming different positions in this regard. In Germany, for instance, pressures have arisen from national telecom operators such as Deutsche Telekom to resume talks with Huawei for 5G rollout; other industries, especially the automotive industry, call for the government to adopt a collaborative stance towards Beijing. By contrast, the French Parliament adopted an "anti-Huawei law" in July 2019 to protect French defence and national security interests with regard to mobile radio networks. Even though Huawei and ZTE are not mentioned, the French law has the ultimate goal of hindering Chinese companies from entering the French 5G market, as they will not be allowed to access the core mobile network. In January 2020, the EU Commission itself launched a 5G toolbox, stating that Chinese operators are "high-risk suppliers". This move was aimed at limiting the growth of Huawei's market share in Europe, especially with regard to core networks. However, the EU Commission leaves the final decision concerning national 5G strategies up to Member States, ultimately creating disparities among them.[16] But Europe also has an advantage in this field that the US does not have: Finland's Nokia is the only player – besides Huawei – to be operational in the entire spectrum of 5G technology (it has a 31% share of the European market), and the company is already involved in the EU-funded Hexa-X project that should develop the 6G network by 2030.[17]

Very close to the 5G issue stands the struggle for strategic autonomy on chips. The European Chips Act, in particular, can be defined as both an industrial and a geopolitical tool.

[15] K. Rist, "Europe is Building World-Class Tech Companies. But Can It Close the Gap with the US?", *Forbes*, 27 May 2022.

[16] European Commission, "Secure 5G networks: Commission endorses EU toolbox and sets out next steps", 29 January 2020.

[17] See Nocetti (2022).

Launched in February 2022,[18] it aims to cope with the supply crisis caused by the scarce availability of semiconductors, especially for the EU automotive industry. As is well known, about 80% of semiconductor production is based in Asia (Taiwan is the main producer with TSCM, a company with a global market share of 54%) and, as a result, there have recently been major bottlenecks for the global semiconductor value chain and for the supply to Europe. The EU's final goal is thus to increase EU chip production to 20% of the global market by providing the legal basis for EU Member States to use subsidies to build new foundries and production facilities, as well as for introducing new trade restrictions. Allowing Member States to grant national subsidies could be defined as a cornerstone of EU industrial policy: for the first time, security and geopolitical considerations prevail over competition issues. The EU Chips Act has already brought some results: Intel has recently announced up to $80 billion of investment in Europe, including about €17 billion to build a first gigafactory in Magdeburg, Germany (40% of this production site will be funded by the German government).[19]

In Italy, Intel has announced in August 2022 that the US company is going to build a €4.5 billion advanced semiconductor packaging and assemply plant, which will become operational between 2025 and 2027.[20] Moreover, the Italian-French STMicroelectronics company announced on 5 October that it will build an integrated silicon substrate manufacturing facility in Italy (Sicily), the first-of-a-kind in Europe. This is essential to improve strategic autonomy in chips manufacturing, since SiC substrates have bee in short supply since the start of the global chip crisis. The €730 million investment will be supported

[18] European Commision, "A Chips Act for Europe", COM(2022) 45 final, 8 February 2022.

[19] J. Deutsch, "Intel Bets 17 Billion Euros on a Tech Revival in Eastern Germany", Bloomberg, 6 July 2022.

[20] G. Piovaccari, G. Fonte, "Exclusive: Italy and Intel pick Veneto as preferred region for new chip plant", *Reuters*, 26 September 2022.

financially by the Italian State in the framework of the National Recovery and Resilience Plan.[21]

EU funding for the Chips Act amounts to €43 billion (comprehensive of equity support). However, the EU is not the sole actor aiming to play a more active role in chip manufacturing. A US Chips Act, worth $52 billion of public investment over 5 years was approved by the US Senate in July 2022 and signed by President Biden in August.[22] China, on the other hand, has announced an investment programme estimated to reach $150 billion over ten years.[23] Against this backdrop, the US still holds a considerable advantage in computer chips, also thanks to tech giants such as Intel and Nvidia. In fact, Chinese companies lack expertise and a strong industrial base, in particular when it comes to the most sophisticated components, making chips China's number one import, higher than oil&gas. The trend towards a progressive confrontation between the Western world and China in the digital and technology domain could increase through the establishment of the EU-US Trade and Technology Council (TTC), which will include some form of coordination also in the field of chips. The Council, launched during a European trip by President Biden in June 2021, has the official goal of fostering EU-US trade relations, primarily in the technological field; however, its geopolitical significance in terms of seeking to counter the Chinese race for technological and digital leadership is quite clear.[24]

Most recently, the Biden administration restricted exports of certain equipment and services to Chinese semiconductor companies on 7 October 2022, within the broader framework of the newly released US National Security Strategy.[25]

---

[21] L. Li, "STMicroelectronics to build chip plant in boost for EU supply chain", *Financial Times*, 5 October 2022.

[22] K. Breuninger, "Biden signs China competition bill to boost U.S. chipmakers", *CNBC*, 9 August 2022.

[23] N.F. Poitiers and P. Weil, "Fishing for Chips. Assessing the EU Chips Act", IFRI, 8 July 2022.

[24] F. Fasulo and D. Tentori, "Scambi globali: manovre USA-UE, nel mirino la Cina", ISPI commentary, ISPI, 8 October 2021.

[25] G.C. Allen, "Choking Off China's Access to the Future of AI", CSIS, October

The "chips competition" is linked to another geopolitical, technological and industrial competition: the race for high-computing power, including quantum computers. These kinds of computers have disruptive potential in both the civilian and the military domain, and their deployment has an impact on national sovereignty and soft power. The strategic nature of these assets is demonstrated by the fact that the US and China have closed their respective markets to foreign suppliers and have adopted national strategies since 2015. They are crucial in the development of AI, in medical, climate and science research, as well as in developing new weapons. China and the US lead the race: while in 2000 Beijing did not have a single computer in the fastest 500 ranking, it overtook the US in terms of performance and computing power in 2018, when China had the highest number of computers in the Top500 worldwide (173 Chinese v 126 US), although Chinese machines are not as high-performance as American ones. Nevertheless, the ranking could change rapidly, as demonstrated by the recent operationalisation of Frontier, a new exascale machine in Tennessee.[26] China was also the first nation in the world to operationalise an exascale computer, the most powerful of all, and has pledged to have 10 national exascale computers, with a specific target included in its 14th Five-year-development-plan for 2021-25. The global market for this kind of computer, estimated at €35 billion in 2020, is expected to reach €56.7 billion in 2028. The EU is trying to catch up in this field too by implementing a plan known as the EuroHPC Joint Undertaking (JU) and another named European Processor Initiative (EPI). Launched in 2017 by seven member countries, the EuroHPC initiative was later endorsed by the EU Council through a new regulation and jointly funded by EU Institutions (€3.1 billion) and Member States. No exascale computers are operating in Europe as yet, but five

2022. See also The White House, "National Security Strategy", October 2022.

[26] D. Clark, "U.S. Retakes Top Spot in Supercomputer Race", *New York Times*, 31 May 2022.

petascale and three exascale machines are under construction, and one of them, Leonardo, will be soon operational in Italy.[27]

A Battle for Digital Standards?

Once confined to a technical debate, international standards are rapidly growing in importance as a subject of geopolitics. Digital standards have reflected the normative evolution of the Internet and the digital world and are developed at the domestic and international level with different strategies depending on the individual country. Standards are regarded as commonly accepted benchmarks, generally voluntary and consensus-driven, and are primarily established by standards development organisations (SDOs) that are multilateral (made up of states) or multi-stakeholder (with representatives from industry, government, civil society and academia). National and global adoption of standards is key to ensuring competitiveness and collaboration in the world's business ecosystem: they are crucial to ensure interoperability, cost-effectiveness and good engineering. Today, digital standards have deep social, economic as well as geopolitical implications, since they are the backbone that allows the functioning of crucial infrastructure such as the Internet. The Internet Engineering Task Force (IETF) is the leading international standards body that develops the most important voluntary standards, such as the famous TCP/IP, which allows Internet communications across all hardware devices. When it comes to technical standards, the US maintains the lead in participation in IETF by percentage of attendees (51.64%), followed by the EU (20.1%) and China (5.64%).[28]

[27] A. Pannier, "Europe's Quest for Technological Power", *Horizons*, Issue 20, Winter 2022.

[28] S. Faaborg-Andersen and L. Temes, "The Geopolitics of Digital Standards. Separating Hype from Reality", Harvard Kennedy School Belfer Center for Science and International Affairs, July 2022.

Countries across the world have different strategies when trying to spread national standards at the international level. Historically, the United States, Europe and Japan have dominated standard-setting bodies for technology and data, but nowadays new countries are progressively becoming technology hubs and strive for a greater role in SDOs. China has steadily increased its participation since the 1990s and today Beijing wants to become a major player. In the recent 2020 plan, called China Standards 2035, the country aims to increase its involvement in standard setting by expanding its presence within SDOs where global tech rules are set. Beijing has now become one of the world leaders in telecommunications, space and artificial intelligence, making China a global technology superpower. China thus acknowledges that standards are crucial to influencing technology markets and developing upcoming technologies such as artificial intelligence and digital surveillance. The two key goals of China's plan are to increase the quantity of Chinese-owned international standards and Chinese representatives in leadership positions within SDOs.[29] China Standards 2035 also calls for aligning standards among countries participating in China's Belt and Road Initiative and fostering dialogue on standards within BRICS countries. Moreover, it is clear that the Chinese strategy is far from being market-oriented and encompasses more geopolitical considerations when it calls for a greater role for Chinese industry in supporting the development of state-led standards. In particular, Chinese companies are incentivised to support Chinese proposals in industry-led bodies, even when they are technologically inferior. However, the structure and past work of SDOs indicate that the most successful standards are the best-engineered and most collaborative ones, not those supported by governments.

The US and the EU have different standards strategies from China's, but something is already changing due to

[29] GG. Neaher, D.A. Bray, J. Mueller-Kaler, and B. Schatz, "Standardizing the Future. How Can the United States Navigate the Geopolitics of International Technology Standards?", Atlantic Council, October 2021.

Beijing's assertiveness. Traditionally, the US approach has been based on decentralisation, encouraging private sector, industry and multi-stakeholder participation. In February 2022, the EU, against a backdrop of efforts to gain strategic autonomy, adopted a new standards strategy with the final goal of strengthening the digital single market, fostering the green transition and democratic values and ultimately establishing the continent as a global leader in standard setting. According to the strategy, coordination between the EU Member States, national standardisation bodies and EU stakeholders must be improved to strengthen the EU's voice in global standardisation. This goal must be achieved within a framework of a public-private partnership made up of private companies, non-profit organisations and the European Commission, where the industry takes the lead with a reinforcing regulatory framework enforced by the EU Commission. The EU strategy stresses the importance of maintaining a leading role in Internet standardisation to promote a free, open, accessible, inclusive and secure global Internet. According to the Commission, in recent years international standardisation on Internet protocols has become increasingly politicised, with the risk of limiting the evolution of the global open Internet and hampering the digitisation process across the world. This seems to be a clear reference to the Chinese proposal of an alternative Internet protocol that would replace the universal TCP/IP. This New IP would probably undermine the concept of an open Internet using the same standards and protocols in every country. The Chinese proposal aims to introduce a new system where each country creates its own version of the Internet under the control and surveillance of the state. However, such a goal is very unlikely to gain consensus at the international level.

Instead, the EU focuses on the importance of adopting the Internet Protocol Version 6 (IPv6) in order to improve the existing TCP/IP infrastructure. Its ongoing discussions with the United States on more cooperation within the scope of the Trade and Technology Council (TTC) or future discussions

on standards in the planned Digital Partnerships with Japan, the Republic of Korea and Singapore are good examples of EU standardisation cooperation strategy with international partners. One of the most important tools for the EU to promote its own digital and technological standards is through trade agreements, as well as regulatory dialogues and digital partnerships, with the final goal of cooperating on standardisation with like-minded partners in strategic areas and coordinating positions in international standardisation bodies. The EU will especially promote international cooperation on standardisation through the Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI-GE). Moreover, standardisation projects will be implemented in selected African countries as part of its development cooperation policy and Global Gateway. Finally, the EU will promote key European standards in partner countries with perspectives of accession or closer integration with the EU's internal market, starting from the EU's Neighbourhoods.[30]

The Battle for Digital Leadership in the Developing Countries

The Great Powers have no doubt as to where the battle for digital supremacy and standards will be played out. Developing and low-income countries are the natural market for exporting digital technologies, especially in Africa, South-East Asia and South America, and for applying digital standards internationally. China launched its digital strategy abroad in 2015 with the establishment of the Digital Silk Road, the digital arm of the Belt & Road Initiative (BRI). Since its creation, China has invested about $50 billion in digital infrastructure

[30] European Commission, "An EU Strategy on Standardisation. Setting global standards in support of a resilient, green and digital EU single market", COM(2022) 31 final, February 2022; see also Faaborg-Andersen and Temes (2022).

abroad[31]. But it is not just a race for digital investments between China and US: other actors, such as Russia, Turkey and the EU, are investing in digital infrastructure abroad, especially in the African continent.

As the President of the European Commission said in her 2021 State of the Union address

> the EU will build Global Gateway partnerships with countries around the world. We want investments in quality infrastructure, connecting goods, people and services around the world. We will take a values-based approach, offering transparency and good governance to our partners. We want to create links and not dependencies. And we know how this can work. Since the summer, a new underwater fibre optic cable has connected Brazil to Portugal. In an unprecedented manner, we will invest in 5G and fibre.[32]

In its 2030 Digital Compass, adopted in March 2021, the European Union stressed the importance of international engagement to foster Europe's digital leadership and global competitiveness. The EU focuses on a comprehensive programme including broadband rollout in the Western Balkans and Eastern Partnership. Moreover, Europe will foster connectivity in the Neighbourhood and Africa, especially through submarine cables and a constellation of satellites.[33] In addition, the EU will step up the implementation of the EU-Asia Connectivity Strategy through new Connectivity Partnerships with India

[31] American Enterprise Institute, "China Global Investment Tracker".

[32] European Commission, "2021 State of the Union Address by President von der Leyen", Strasbourg, 15 September 2021.

[33] Submarine cables are e key tool for connectivity and have both an economic and geopolitical goal. about 97% of global internet traffic passes through undersea cables, and financial transactions amounting to about $10 trillion a day are carried out through them. To date, there are 426 undersea cables on the ocean floor totaling 1.2 million km. They have a key geopolitical significance mainly because they physically unite two or more countries, strengthening their economic ties, bilateral transactions, data exchange, and ultimately political and strategic ties as well.

and the Association of South East Asian Nations (ASEAN). A Digital Partnership with Latin America & the Caribbean will complement the launch of the connectivity component of the Digital Alliance with Latin America & the Caribbean, building on the BELLA Cable that will connect Portugal with Brazil.[34] These initiatives will be funded mainly through the recently established Global Gateway, the €300 billion infrastructure plan aimed at boosting connectivity between Europe and the rest of the world, especially with developing countries.[35] The EU's international partnerships primarily aim to align other countries with EU regulatory norms and standards in fields such as data flows, data protection and Internet governance, as well as digital finance and e-government. To foster its digital partnership with emerging economies, the Commission will design and propose digital economy packages. The latter will be financed through Team Europe Initiatives (TEIs) that combine the resources of the EU and Member States.[36] However, the larger share of digital investments abroad will be funded through the Connecting Europe Facility (CEF),[37] especially with respect to the Neighbourhood, and the financial support of the European Investment Bank, in particular through InvestEU and the recently launched €79.5 billion NDICI-Global Europe plan.[38]

---

[34] European Commission, "2030 Digital Compass: The European way for the Digital Decade", COM(2021) 118 final, 9 March 2021.

[35] European Commission, "The Global Gateway", JOIN (2021) 30 final, 1 December 2021.

[36] European Commission, "2030 Digital Compass: The European way for the Digital Decade"…, cit.

[37] European Commision, "Annex to the Commission Implementing Decision on the financing of the Connecting Europe Facility - Digital sector and the adoption of the multiannual work programme for 2021-2025", C(2021) 9463 final, 16 December 2021.

[38] European Union, "Regulation of the European Parliament and of the Council of 9 June 2021 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe, amending and repealing Decision No 466/2014/EU and repealing Regulation (EU) 2017/1601 and Council

When it comes to digital infrastructure investments abroad a key role will be played by submarine cables, which will form the connectivity backbone for the Digital Connectivity Gateways. This infrastructure will be designed in a manner that will ensure international connectivity to EU partners worldwide as a basis for European strategic autonomy. The Digital Global Gateways will support the deployment of backbone connectivity for routes within Member States, between Member States, and between the EU and third countries, including to remote territories where: i) there is a lack of redundancy on a route; ii) existing infrastructure cannot satisfy demand; and iii) the users in the territories suffer from suboptimal services and prices. Furthermore, for strategic and security reasons, non-EU entities will be excluded from investments in the EU and no security-sensitive equipment or services will be procured from third-country suppliers. For infrastructure connecting the EU with third countries, an exception is made for legal entities in that third country where their participation is indispensable for the achievement of the objectives and subject to security guarantees approved by the third country.[39]

Looking at a broader and global picture, especially after the Russian invasion of Ukraine, a Western-led infrastructure initiative could play an increasingly significant role in countering Chinese digital investments abroad, boosting connectivity and financing digital infrastructure in developing countries. First envisaged in 2021 during the G7 Summit in Cornwall, with the establishment of the US-led Build Back Better for the World Plan (B3W),[40] a G7-led $600 infrastructure plan for developing countries was announced during the 2022 G7 Summit in

---

Regulation (EC, Euratom) No 480/2009", *Official Journal of the European Union*, L. 209/1, 14 June 2021.

[39] T. Küppe, "EU Funding for Global Gateways. CEF Digital calls backbone connectivity for Digital Global Gateways", European Commission, Brussels, 28 June 2022.

[40] The White House, "President Biden and G7 Leaders Launch Build Back Better World (B3W) Partnership", 12 June 2021.

Germany.[41] The plan, if correctly implemented, could have disruptive benefits also for digital connectivity. However, there are growing doubts about the plan's financial soundness and it is still unclear how decisions about concrete infrastructure investments will be adopted by the Member States.

The United States is pushing its digital and technological agenda in the Indo-Pacific region too, in a cooperative way with allied countries and with an implicit goal of countering the considerable Chinese digital investment in the region. In March 2021, Australia, India, Japan and the United States gathered in the Quad format, announced that they would "begin cooperation on the critical technologies of the future, to ensure that innovation is consistent with an open, free, inclusive and resilient Indo-Pacific". The Quad stressed the importance of launching an emerging-technology working group to facilitate cooperation on international standards and innovative technologies, with a focus on four core areas: technical standards, 5G diversification and deployment, horizon-scanning and technology supply chains.[42] At the following Quad Summit held in September 2021, the leaders called for the development of open and high standards of innovation, underscoring that technology and digital infrastructure should not be misused for malicious activities such as authoritarian surveillance and oppression or to disseminate disinformation. The Quad countries also agreed to enhance interoperability and resilience of supply chains for hardware and software to avoid vulnerabilities, which have become particularly evident with overdependence on China in the last few years. The Quad leaders decided to create technical standards contact groups with a focus on advanced communications and artificial intelligence. In particular, the group established a cooperative initiative to map capacity, identify vulnerabilities and bolster supply-chains security for semiconductors. During this summit, the Quad also agreed to support 5G deployment and

[41] G7 Germany, "G7 Leaders' Communiqué", Elmau, 28 June 2022.

[42] The White House, "Quad Leaders' Joint Statement: 'The Spirit of the Quad'", 12 March 2021.

diversification, as a way to ensure a diverse, resilient, innovative, competitive and secure telecommunications ecosystem, in particular through the creation of an Open Radio Access Network (RAN). Finally, the member countries decided to set up a Quad Senior Cyber Group aimed at developing shared cyber standards and promoting the scalability and cybersecurity of secure and trustworthy digital infrastructure.[43]

A new Quad Summit in May 2022 stressed once again the importance of the tech focus, promoting the further development of the Open RAN and signing a new Memorandum of Cooperation on 5G Supplier Diversification. The four countries also issued a Common Statement of Principles on Critical Supply Chains aimed at accelerating the pace of cooperation on semiconductors and other critical technologies; finally, to advance cooperation on technology standards they agreed to establish a new body, the International Standards Cooperation Network (ISCN).[44]

What Comes Next After the War in Ukraine?

The war in Ukraine is a game changer for the technological domain and for international cooperation in this field. As Moscow waged war on Ukraine, a digital barricade was immediately raised between Russia and the world. Both Russian authorities and multinational Internet companies built the wall very rapidly. Facebook and Twitter have been blocked. Apple, Samsung, Microsoft, Oracle, Cisco and others have pulled back or withdrawn entirely from Russia and digital payments have been suspended. The decision has inevitably aligned Russia with the Chinese model of strict control over the Internet, and the world has been divided between two different models with

[43] The White House, "Quad Principles on Technology Design, Development, Governance, and Use", 24 September 2021.

[44] The White House, "Quad Joint Leaders' Statement", 24 May 2022; see also R.J. Rajagopalan, "The Growing Tech Focus of the Quad", *ORF*, 9 July 2022.

respect to digital infrastructure and freedom of expression. Moreover, the impact of the tech curtain will be even deeper. Unlike China, where domestic Internet companies have grown in the last few years, Russia does not have a competitive digital and tech industry. Western sanctions on technologies and digital equipment are hitting hard. Already, Russian telecom companies that operate mobile phone networks no longer have access to new equipment and services from companies like Nokia, Ericsson and Cisco. The economic and industrial fallout without Western technologies may be severe. Besides access to independent information, the future reliability of Internet and telecommunications networks, as well as the availability of basic software for industry, public services and government, is at risk. Mobile operators are struggling to continue the 4G network deployment and have been forced to purchase used equipment. Efforts by Russian companies to develop new microprocessors are failing after Taiwan Semiconductor Manufacturing Company (TSMC), which has a global market share of 54%, stopped shipments to Russia.[45] Moscow is highly reliant on imports of high-tech goods, which are worth around $19 billion annually. The largest share (45%) comes from the EU, with 21% from the US, 11% from China and 2% from the United Kingdom. The main import categories are aerospace goods (worth almost $6 billion) and information and communication goods (nearly $4 billion in 2019).[46] The US warned China that tech supplies to Russia – as a means to circumvent sanctions – would have consequences such as secondary sanctions. Chinese digital and tech exports suffered a substantial reduction immediately after the outbreak of the war – with a massive 98% reduction in exports of telecommunications network equipment.[47] Nevertheless,

[45] A. Satariano and V. Hopkins, "Russia, Blocked from the Global Internet, Plunges Into Digital Isolation", *The New York Times*, 7 March 2022.

[46] S. Marcus, N. Poitiers, M. Grzegorczyk, and P. Weil, "The decoupling of Russia: high-tech goods and components", Bruegel Blog, 28 March 2022.

[47] A. Popova, "Tech Sanctions Against Russia Are Working", CEPA, 9 August 2022.

things have progressively changed. China's Huawei resumed exports to Russia in July, like many other Chinese industries, and chip shipments from China to Russia more than doubled in the first five months of 2022 compared with 2021.[48] Against this backdrop, the overall strategy of import substitution has had little success. In fact, China cannot easily substitute fully the technological and digital demand that Russia urgently needs to meet. Beijing itself depends on imports for producing semiconductors and faces the threat of US secondary sanctions. Moreover, Russia is keen to avoid the risk of overdependence on China, and is trying to diversify by using other suppliers such as India and Iran, but the expected results seem far from being achieved.[49]

On the Ukrainian side, digital and technology applications such as SpaceX's Starlink satellites have proved effective in keeping the country online and ensuring people, government but also crucial military connectivity. The country has received more than 10,000 devices since Russia invaded, in part thanks to funding and other help from the US government. The terminals have already become key to the country's response to the war, finding both civilian and military uses.[50] Starlink technology has become key in the battlefield to ensure communications between high commands and troops on the group and coordinate action.[51] The strategic and geopolitical importance of digital infrastructure has also been demonstrated by Russian operations in occupied territories in Crimea. Russian forces have taken over Internet infrastructure in Ukraine and rerouted traffic to Russia-controlled operators, making the Ukrainians' data vulnerable to interception, particularly in the

[48] B. Spegele, "Chinese Firms Are Selling Russia Goods Its Military Needs to Keep Fighti. ng in Ukraine", *The Wall Street Journal*, 15 July 2022.
[49] A. Epifanova, "Russia's Technological Isolation", DGAP German Council on Foreign Relations, 6 April 2022.
[50] T. Simonite, "How Starlink Scrambled to Keep Ukraine Online", *Wired*, 11 May 2022.
[51] L. Cerulus, "UkraineX: How Elon Musk's space satellites changed the war on the ground", *Politico*, 8 June 2022.

Donbas region. In the city of Kherson, a fibre optic cable was taken offline and rerouted to a separatist Crimean operator, with broadband data directed out of Ukraine and into Russian-controlled regions. However, the many network providers that make up Ukraine's Internet (and ensure redundancy) have made the Ukrainian network resilient to Russian military action.[52]

Conclusion

The pandemic and the war in Ukraine have introduced technological and digital sovereignty as buzzwords of contemporary geopolitics. These historical events have accelerated the technological and digital decoupling of value chains and boosted efforts to achieve national strategic autonomy. The digital and Internet space is changing with the global Internet, which is becoming increasingly less global but more fragmented and under growing control by national authorities, especially in authoritarian states. What in the last few years was primarily considered a struggle for technological leadership between the United States and China has turned into a direct confrontation between the Western world and authoritarian states such as China and Russia. The freedom granted by a global Internet and the openness of digital space are increasingly under threat worldwide, as is technological cooperation for the creation of new tech, digital and Internet standards, which is key to foster competitiveness, exploit economies of scale and boost growth at the global level. However, a minimum set of common international rules for the governance of digital space and disruptive technologies such as AI and the Internet of Things is inevitable. And if technical coordination advances in technical and standards bodies with the goal of creating a level playing field for the tech and digital economy of tomorrow, it is possible that cooperation could spread to other domains. But this remains a big question mark.

[52] A. Gross, "Russian forces usurp Ukrainian internet infrastructure in Donbas", *Financial Times*, 5 May 2022.

2. The Economic Impact of Digital Infrastructure: Understanding and Leveraging the Digital Transition

Seth Benzell, Maxwell Means

Miles of cables lie beneath the ground and spool out above our heads. Servers across every nation communicate in ever cleverer codes. Together, these servers and transmission wires are the physical and digital substrate allowing our apps and websites to function. Cellular data and emerging high-speed satellite internet let users access tools and information even when they are apart from our world's massive interconnected system of wires. These technologies define the digital age and its evolution.

And yet, these digital infrastructures are not only interesting networks in and of themselves. They have had a revolutionary impact on economic development. In countless ways, advances in digital infrastructure drive a great amount of economic growth. They have changed the nature of world markets. It is important for policy makers to recognise the importance of these innovations. Using this understanding, they should attempt to build the types of digital infrastructure most conducive to the common good.

In this essay, we predominantly focus on two pieces of internet infrastructure: broadband internet and public application programming interfaces. We evaluate the economic and non-economic impacts of the spread of these networks. We speculate on what the future may hold and suggest prudent digital infrastructure investments.

Broadband Internet – Economic Effects and Government Policies

There is much empirical proof that expansions to broadband access have allowed markets to organise more efficiently due to easier access to information. Using data from job hunters in Germany, Gürtzgen et al. (2021) exploited reasonably exogenous variation in the broadband rollout and found that broadband access improves reemployment rates amongst workers who would otherwise have longer periods of unemployment.[1] Put another way, digital infrastructure in the form of broadband internet access allowed society's labour resources to be reallocated quicker and more efficiently.

Grimes et. al. (2011) analysed company-level data in New Zealand.[2] Though they did not have a particularly "clean" identification strategy, the authors found that broadband adoption boosted company productivity between 7% and 10% after adjusting for confounding factors. Greenstein and McDevitt (2011) analysed the value created by broadband in the US between 1999 and 2006.[3] They found that by 2006, broadband accounted for $28 billion of the US's GDP with between $20 and $22 billion coming from household broadband use alone and they estimated that US consumers enjoyed between $4.8 and $6.7 billion in consumer surplus in contemporaneous dollars. It is likely that further improvements to internet speeds, and additional economic benefits, could be generated by new competitors in the market, additional anti-trust government action, or government subsidies.

---

[1] N. Gürtzgen, B. Lochner, L. Pohlan, and G.J. van den Berg, "Does online search improve the match quality of new hires?", *Labour Economics*, vol. 70, 2021.
[2] A. Grimes, C. Ren, and P.A. Stevens, "The need for speed: impacts of internet connectivity on firm productivity", *Journal of Productivity Analysis*, vol. 37, no. 2, April 2012, pp. 187-201.
[3] S. Greenstein and R.C. McDevitt, "The broadband bonus: Estimating broadband Internet's economic value", *Telecommunications Policy*, vol. 35, no. 7, 2011, pp. 617-32.

Beyond Broadband and Businesses: The Future of Internet Access and Political Economic Impacts

The widespread use of high-speed internet has done more than engender economic efficiency, of course. In 2003, Tolbert and McNeal published an article in Political Research Quarterly that analysed the effects of internet access on voting. They found that internet access increased the likelihood of voting in US presidential elections by 7.5 to 12% and was also generally associated with greater political participation. While some level of political participation is necessary and healthy for a democracy, some reasonably worry that America's rampant political divisiveness started with the internet becoming commonplace. Not all political participation is created equal, and perhaps internet-inspired participation is systemically less useful. Guriev et. al. (2021) found that 3G expansions in Europe were associated with higher perceptions of corruption as well as greater support for iconoclastic populist candidates.[4] They also found that the effect was larger when traditional media sources were censored while the internet remained fettered.

In the *Selfish Gene* (1976), Richard Dawkins formalised the concept of "memes", discrete units of concepts and ideas analogous to genes that spread from person to person.[5] On the internet, memes spread more rapidly than in the analogue world. The diffusion of many successful internet memes is not primarily due to their truth value. It is more directly tied to the ability of those meme to induce someone to recite or spread them to others. Political and religious memes are some of the ones that are most successful, because they often induce a desire to spread them among adherents. It is not therefore unrealistic to expect news sources to become increasingly biased both

[4] S. Guriev, N. Melnikov, and E. Zhuravskaya, "3G Internet and Confidence in Government", *Quarterly Journal of Economics*, vol. 136, no. 4, 2021, pp. 2533-2613.
[5] R. Dawkins, *The selfish gene*, New York, Oxford University Press, 1976.

because there exists a market demand for news that specifically supports ideology and because the writers of news themselves are plugged into the same ideological processes.

How can we make sure that the internet creates a market for truth rather than simply being a selection of vapid tabloids, filled with funny trivialities and political outrages? For the purpose of explicitly testable scientific claims, the peer-review process helps. For business ideas, the profitability of the business can serve as an ultimate reality check. By contrast, our tools for choosing and promoting good political ideas are relatively weak. Clearly, asking the government to restrict communication faces tremendous moral and practical obstacles. Recalling Guriev et al. (2021), perhaps government or social enforcement of speech norms simply leads to a large backlash.[6] And indeed, free speech has brought enormous benefits. The free flow of ideas can create tremendous opportunities as various ideas, principles, and research are combined in novel ways.

One small way in which governments might be able to promote a higher quality of online discourse is by deregulating and subsidizing prediction markets. Prediction markets are spaces where individuals put real or fake money on the line, betting on the probability of different outcomes.[7] Research has suggested that prediction markets can serve at least three important roles: spurring people to seek information, incentivising people to reveal their true beliefs, and promoting tractable information aggregation.[8] By encouraging people to put their skin in the game and make quantitative predictions about the certainty of outcomes, strong predictors (and the cultural memes that they use) will receive a prestige and visibility boost versus persuasive sophists. Prediction markets may also greatly help governments in setting all kinds of policy. As political prediction markets become more established, governments may go directly to them

[6] Guriev, Melnikov, and Zhuravskaya (2021).

[7] C. Graubard and A. Eaddy, "Forecasting, Prediction Markets and the Age of Better Information", *Coindesk*, 4 June 2022.

[8] Graubard and Eaddy (2022).

for policy advice, by posting questions such as "If X becomes government policy, how much will GDP increase?".

An important development is the ongoing deployment of high-speed satellite internet from Starlink and its competitors, allowing high-speed internet to reach places that it never could before reach. Starlink is SpaceX's announced satellite internet service.[9] Starlink would give users access to high-speed internet without potentially destructive land-based infrastructure projects. Given past evidence, rural internetification and emerging satellite internet technologies could prove a great boon to people and firms in some of the poorest and most remote places on earth. Though, perhaps some governments would do well to produce content (or encourage the production of content) that can provide cultural continuity to people suddenly exposed to the whole of the world's thoughts and ideas.

A related challenge is countering foreign propaganda and domestic radicalism. A report from the Oxford Internet Institute found significant evidence for widespread internet propaganda from many governments and political parties around the world.[10] The report estimated there were between 300,000 and 2 million "cyber troops" in China alone and the news has given plenty of attention to the efforts of Russia's "web brigades" in attempting to manipulate international opinion regarding their invasion of Ukraine. More research funding on detecting and stopping the algorithmic portions of mass internet propaganda studies is called for.

Why discuss these political and economic ramifications of digital infrastructure? Well, just as important as the measured, targeted upsides of the internet are the unanticipated, intangible downsides. Governments should anticipate, and prepare for,

[9] R. Crist, "Starlink Explained: Everything to Know About Elon Musk's Satellite Internet Venture", *CNET*, 11 August 2022.

[10] S. Bradshaw and P.N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford University Computational Propaganda Research Project, 2021.

what additional expansions of internet capacity might bring, both in terms of greater speed for existing high-speed internet users and in terms of granting access to more people in more places.

What does the future hold? Well, more reliable internet could mean more effective and efficient remote working and work from home arrangements. Better internet could also make integrated VR projects – such as Mark Zuckerberg's "Metaverse" – potentially more successful and feasible. The concept of the "Metaverse" predates Facebook's "Meta" rebranding and foray into VR, however. The name first appears in the 1992 science fiction novel *Snowcrash* by Neal Stephenson.[11] The "metaverse" in the minds of futurists is essentially an online virtual reality space that houses most of if not all the functionality of the internet. A successful metaverse would see people spending less time outside and less money on physical goods; commensurately, people would be spending more time in the virtual world and more money on virtual goods and services.

From an environmental perspective, this could be a very good thing. The production of digital goods (such as online avatars, virtual spaces, or applications built into metaverse virtual object) will likely require little more than labour, electricity, and the cost of upkeeping server equipment and the like. Potentially, these factors could come together and create a scenario where the total market value of goods and services (GDP) can increase even as society's total demand for limited natural resources falls. Hopefully, these developments will happen along with the growth of green energy technologies, mitigating the negative externalities of metaverse's energy demands. Then again, if widespread VR functionality also decreases travel demand and/or commutes to work, a new virtual economy could still have positive overall effects on emissions.

[11] D. Brown, "What is the 'metaverse'? Facebook says it's the future of the Internet", *The Washington Post*, 30 August 2021.

Application Programming Interfaces – Economic Consequences and Policy Recommendations[12]

However, high-speed internet is not the only important advancement in digital infrastructure. Just as important as the speeds at which computers can communicate is the language in which those computers communicate. Application programming interfaces (APIs) are the software that allows computers to "talk" to each-other. The concept of APIs is often discussed in terms of the "client" such as a home computer or phone and the "server" such as a literal computer server that a company owns. APIs are essentially separate programs running on the client device and the server. The client-side portion of the API sends select signals over the internet to the server hosting the server-side portion of the API which automatically interprets the request and sends back information that is useful to the client-side application.

The economic importance of APIs comes from the fact that they enable a new type of company organisation, in which much of the value is created by outside third parties – a "digital ecosystem". Take Walgreen's "Photo Print" API as an example. This is an API that can control photo printing kiosks at their stores. Walgreen makes this API available to third party app developers so that they can integrate real-world photo printing as an additional functionality of their (say, social media) application.[13] This "inverted firm" strategy is a win-win for both the third-party developers (who get to include a new feature in their applications) and for the focal firm hosting the API (who get a new source of orders for photo printing). Overall, the strategy of creating public APIs enables firms to costlessly recruit third-party complementors to their products. This is an

[12] This section draws heavily from S. Benzell, J.S. Hersh, M.W. Van Alstyne, and G. Lagarda, *How APIs Create Growth by Inverting the Firm*, Working Paper, 2022.

[13] Walgreens Developer Portal | API, Walgreens, https://developer.walgreens.com/apis.

essential advantage given Joy's Law: "No matter who you are, most of the smartest people work for someone else".[14]

APIs are the ideal tool for creating a digital ecosystem. Modular sharing systems are more robust to unanticipated shocks, allowing third parties to trust that the reliability of the source. The modularity of APIs also allows them to be recombined in interesting and exciting new ways. APIs also can allow for permissionless, yet meterable innovation. By permissionless, we mean that public APIs can be interacted with by third parties, and even incorporated into their own products, without needing extensive legal or technical processes. However, a good substrate for a digital ecosystem must be meterable as well. A good public API must make sure that essential company or customer secrets are not revealed, and that any data or services delivered are efficiently monetised.

How does an API achieve these goals? To paraphrase Ofoeda et al. (2019), an API is a set of routines, protocols, and tools that builds standardised software applications compatible with an associated program or database.[15] APIs are codes that control access to information, but they can also be thought of as a kind of contract governing the type and format of calls or communications that an application can make to another associated program.[16] The flexibility of APIs emerges from the fact that the answering program is agnostic about the source of any call and the calling program need not know anything about the internal workings of the answering program. APIs come in two flavours: public and private. Private APIs may help firms share information more seamlessly across departments or better modularise their technology stack to allow for additional

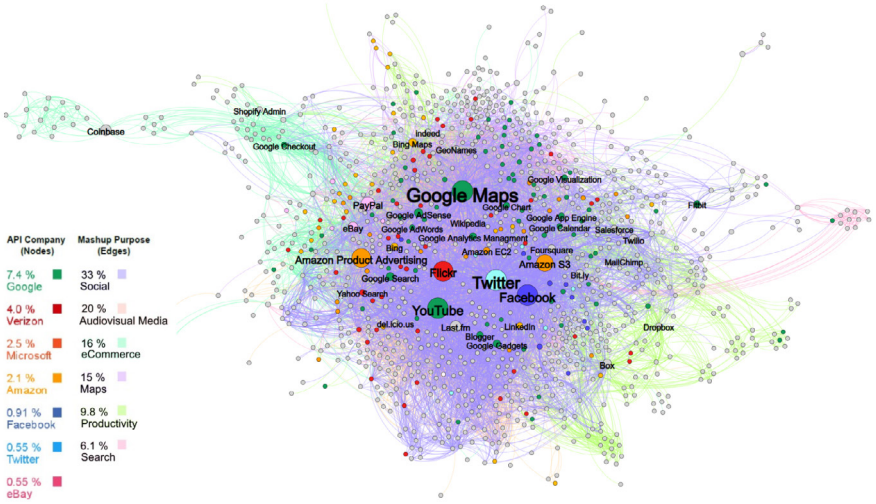
[14] K.R. Lakhani and J.A. Panetta. "The Principles of Distributed Innovation", *Innovations: Technology, Governance, Globalization*, Summer vol. 2, no. 3, 2007.

[15] J. Ofoeda, R. Boateng, and J. Effah, "Application Programming Interface (API) Research: A Review of the Past to Inform the Future", *International Journal of Enterprise Information Systems*, vol. 15, no. 3, 2019, pp. 76-95.

[16] D. Jacobson, G. Brail, and D. Woods, *APIs: A strategy guide*, O'Reilly Media, Inc., 2011.

innovation. While many firms create or commission an API system for their own employees to improve some specific internal processes, other firms manage to create an entire miniature economy of third-party developers creating apps and services that leverage access. Sometimes a private API evolves into a service that is eventually made public, and sometimes public APIs are found so useful that they displace internal productivity tools for the focal firm. "Working Backwards" a book about innovative processes at Amazon has examples of both occurring in that company.

The extent of the interconnectivity created by the network of public APIs and the apps that call them is staggering. The figure below, from Benzell et al. diagrams the internet's connected API platforms.



The network of public APIs and the applications that call them. Nodes correspond to public APIs, are coloured by their owner (grey for "other") and are sized proportionally to their centrality. Edges correspond to applications, or "mashups", that interact with multiple APIs, and are coloured by their purpose. Data is scraped from the public "Programmable Web" repository and has a US and mid-2010's bias.[17]

Benzell et al. (2022) further analyse the benefits of APIs that attract external developers.[18] While on the surface, it may seem counterintuitive to allow outsiders to access your firm's resources, those authors estimated that the value growth of API adopters was 2% higher than otherwise similar firms. Moreover, the authors of the working paper found that the API publisher and their community functioned in a symbiotic way where the growth rate for 3rd party developers also increased. The growth of the API ecosystem is an essential part of digital infrastructure development and is worth encouraging. After all, many companies using one set of servers and code is more efficient than the scenario where each firm must develop their

[17] Benzell, Hersh, Van Alstyne, and Lagarda (2022).

[18] Ibid.

own APIs given that the resources are essentially non-rivalrous. Moreover, extending the resource to outsiders may result in innovative new applications for the same tech resources that the host company may never have happened upon themselves.

While the creation of a public API creates lots of tools for small-scale innovators to incorporate into their apps, it is the large firms at the centre of the network who disproportionately benefit. The nature of digital ecosystems, at least recently, is such that they tend to create natural monopolies at their centre.

Conventional economic wisdom would dictate that such central firms should be allowed to stay large but be regulated so that their market power can be aimed to serve the public good. An alternative approach would be for the government to encourage the development of new APIs but tax at windfall levels those first movers who have benefited disproportionately from the creation of the API network.

Another potential avenue for policymakers to develop a socially beneficial API infrastructure is to think about the data these central API hubs are allowed to collect. Business decisions can be more efficient when informed by data, but a firm that buys data that their competitors do not buy or – for whatever reason – cannot buy may just give the first firm an unproductive strategic advantage over its competitors. This would be a problem like those outlined in "Phishing for Phools" by Akerlof and Shiller (2016), and exact problems in that book could also be exacerbated by these big datasets; namely, firms could use user data to better appeal to irrational impulses rather than improving their products to induce additional "rational" consumption.[19] Perhaps the best future is one in which digital ecosystems are organised around decentralised DAOs and the blockchain, as in some Web 3.0 visions.

[19] G.A. Akerlof and R.J. Shiller, *Phishing for Phools: The Economics of Manipulation and Deception*, Princeton University Press, Princeton, 2016.

Digitalisation and AI Adoption

"Artificial Intelligence" – at least by some definitions – is already here and is already having an effect on the economy. As Argwal et al. discuss in the book *Prediction Machines* (2018), programmers have created learning algorithms that in turn accommodated the invention of products like self-driving cars, automated music recommendation, and facial recognition; in the reckoning of those authors however, AI's greatest change to the global economy may come from making good AI predictions cheaper.[20] Whereas firms previously needed to employ, train, and vet expensive experts to inform management decisions, now firms could perhaps gain predictions of similar quality much more cheaply from "canned algorithms". While this trend will certainly lower the costs of large firms, it could also allow smaller firms with less cash on hand to make better informed decision and thus waste fewer resources "hedging their bets" against less certain predictions. Currently, economists lack especially good data sources with which to disentangle the benefits and externalities caused by the rise of machine learning algorithms, but Argwal thinks that the growth and benefits from machine learning will be similar to the benefits firms saw from adopting personal computing: the effects will not be immediate, but the benefits will become apparent with time as firms learn to integrate the opportunities such programs provide. Brynjolfsson and Rock call this the "J-Curve" effect of new general-purpose technology (e.g. AI) adoption.[21] Fully realising the gains from radically new technology requires large-scale, but hard-to-measure, intangible investments in business reorganisation and other complements. While these investments are being made, the economy will seem to be growing slower than it actually

[20] A. Argwal, J. Gans, and A. Goldfarb, "Prediction Machines: The Simple Economics of Artificial Intelligence", *Harvard Business Review*, 2018.

[21] E. Brynjolfsson, D. Rock, and C. Syverson. "The Productivity J-Curve: How Intangibles Complement General Purpose Technologies", *American Economic Journal: Macroeconomics* , vol. 3, no. 1, 2021, pp. 333-72.

is. However, beneath the tranquil macroeconomic statistics, a behemoth stirs.

But will digital infrastructure, and the bots it enables, take our jobs? Argwal and co. believe learning algorithms could obviate certain positions fairly quickly in certain cases once the price falls low enough relative to wages and so long as regulation does not interrupt the technological transition. Acemoglu et al. (2022) look at the data and find that AI changes the composition of available jobs rather than making human jobs disappear.[22] Using firm-level data on job openings and various proxies for AI automation, that paper found that firms with higher exposure to AI innovations have indeed posted more jobs that require the ability to use AI technologies; moreover, in two parameterisations of their statistical model, they found the expected fall in job openings in other types of job too. Interestingly though, the authors found no associated fall in salary and level of employment for workers in fields with high levels of expected AI exposure. At this moment in history, it is perhaps unclear if this stability should be expected forever.

E-Government

E-Estonia and the "Digital Nations" movement should excite and frighten bureaucrats around the globe. To elaborate, E-Estonia is Estonia's attempt to revolutionise its government through the use of a grand interconnected digital platform.[23] Each citizen is assigned a personal ID card that acts as a digital signature for users and Estonian citizens can now vote, pay taxes, apply for university, and register a business online. Estonia can now administer the government with more efficiency, using less paper and hiring fewer hours of bureaucratic labour. Even

[22] D. Acemoglu, D. Autor, J. Hazell, and P. Restrepo, "Artificial Intelligence and Jobs: Evidence from Online Vacancies", *Journal of Labor Economics*, vol. 40, no. 1, 2022.

[23] N. Heller, "Estonia, the Digital Republic", *The New Yorker*, 18 December 2017.

medical records utilise the same broad platform. Data integrity in the system is secured with blockchain technology so whenever a piece of data is viewed or edited, an ostensibly indelible record of that process is also recorded in the system. Data is housed locally by various businesses and users but transmitted on demand over encrypted pathways. Meanwhile, a backup of the core system is housed on a server in a special embassy in Luxemburg in case the core system fails. The E-Estonia initiative reportedly saves Estonia 2% of its GDP per year in government costs and it could perhaps save even more for larger countries with more cumbersome extant bureaucracies.

The strategy has an attractive sales pitch and obvious – or at least apparent – efforts have been made to shore up a system on which the functioning of the nation depends. Still, this level of centralisation ought to be approached carefully and with scepticism. Some people already worry that sufficient advancements in quantum computing will eventually undermine the mathematical system that validates blockchain data – a prospect which would also scare bitcoin investors.[24] Moreover, a 2014 report on E-Estonia's i-voting system found that it could still be vulnerable to a dedicated cyberattack or be manipulated by government operators.[25] Estonia's technologists assure the public that this assessment was made with incorrect assumptions about the system's architecture, however. Still, countries would be wise to at least make their own earnest assessment about the security of a system like E-Estonia, if only for intelligence purposes. If the system is found to be solid, governments may eventually find it hard to compete without such technological advancements.

[24] I. Barmes, I. Kohn, and C. Soutar, "What Does the Dawn of Quantum Computing Mean for Blockchain?", World Economic Forum, April 2022.

[25] D. Springall et. al., "Security Analysis of the Estonian Internet Voting System", Proceedings of the 21st ACM Conference on Computer and Communications Security, 2014.

Concluding Remarks

As we have established in this chapter, digital infrastructure is quite important for economic growth. Companies and consumers alike stand to benefit from reliable fast internet as well as the apps and services that such information flows allow. As with the invention of the printing press, the largesse created by these new information technologies comes part and parcel with disruption of the world's power structures; firms concentrate and ideologies morph and balkanise.

Governments absolutely have a role in maximising the benefits from these innovations as well as in counteracting the worst of what these developments might bring. In fact, the relative ability of nations to harness and guide these changes may ultimately decide which nations prosper, which nations fail to keep up, and perhaps even which nations are able to survive.

3. Digitalisation for Sustainability: A Twin Challenge

J. Scott Marcus, George Zachmann

There are a large number of linkages between the political goal of limiting the negative environmental footprint of human activity (environmental sustainability) and the increasing penetration of information and communication technology in our society (digitalisation). This chapter seeks to provide a classification of such linkages, to identify both the challenges and opportunities that these linkages offer European citizens, and to provide an initial set of general recommendations for European policymakers.

A Developing Linkage Between Digitalisation and Sustainability

It has long been evident that many of the possible ways in which to enhance sustainability rely on digital technology. In the years 2020 through 2022, however, world events have driven a rapid and dramatic change in our European understanding and approach to sustainability, to digitalisation, and to the relationship between them.

Sustainability has taken on far greater immediacy than in the recent past. The impacts of climate change have become ever more obvious (rising average temperatures) and likely contributed to changing weather patterns that have been connected to extreme heat, droughts, floods, and forest fires.

The European public today accepts, by and large, that climate change needs prompt action – this is an issue that requires action starting now, not something that can be pushed off onto our children or grandchildren.

Russia's brutal and unprovoked invasion of Ukraine has also changed the game dramatically. Reducing our consumption of fossil fuels takes on a very different meaning when there is no longer any assurance that gas will be available in the quantities required. At the same time, shortages and supply chain disruptions that greatly increase the price of gas and oil mean that many measures to reduce consumption that might not have been easy to cost-justify in the past are now easy to cost-justify. This helps to correct for a classic public goods problem, where an investment that would be net beneficial to broader society does not happen because not enough of the benefits flow to the firms or individuals who have to make the investments – at the high prices that we are experiencing today, and the even higher energy prices that we can expect tomorrow, many investments now become directly profitable even in the absence of public policy intervention.

The Covid-19 pandemic has also transformed our understanding. Digital technology played a key role in enabling knowledge workers to work from home,[1] and consumers to shop from home, when the pandemic was at its worst.[2]

The pandemic has also driven an understanding that funds invested in recovery from the pandemic must seek not merely to replace what was there in the past, but also to strengthen and modernise broader society. Furthermore, the vision of a *twin transition* that seeks to promote both sustainability and digitalisation is now solidly anchored in the EU's Recovery and Resilience Facility (RRF), the largest component of Next

[1] J.S. Marcus, "COVID-19 and the shift to remote work", Bruegel, 2022. A version of this Policy Contribution will be published as a chapter in J. Whalley, V. Stocker, and W. Lehr (Eds.), *Beyond the Pandemic? Exploring the impact of Covid-19 on telecommunications and the internet*, Emerald Publishing, forthcoming.

[2] J.S. Marcus et al., "The impact of COVID-19 on the Internal Market", European Parliament, 2021.

Generation EU (NGEU), the European Union's landmark instrument for recovery from the coronavirus pandemic.[3]

Classification

In this chapter, we identify several main linkages between digitalisation and sustainability, which we then expand on in the sections that follow.

- Digital technologies could enable us to reduce our environmental footprint without negatively affecting our standard of living, either by improving the efficiency with which we produce desired goods and services, or by reducing the pollution that we generate for a given volume of goods or services.
- Digital technologies could increase the use of resources.
- Digital technologies could allow new modes of policy-making – including more targeted environmental policies.

Digital Technologies could enable us to reduce our environmental footprint

First, there are many sectors where digital technologies will enable us to produce more from a given amount of input. Satellite data, drones and smart algorithms might allow us to improve the productivity of basic sectors such as agriculture, and reduce the intensity with which we use fertilisers, herbicides and intrusive soil tillage. 3D-printing might reduce materials consumption (compared to subtractive production technologies) as well as transport needs (compared to complex international value chains) for certain products. And digital technology will help us to do a better job of tracking material/product flows in our economy, thus enabling us to recover as much value as possible from a product, even after the end of its economic lifetime. In fact, digital technologies can help to increase circularity (see Tab. 3.1) at almost every stage.

[3] Z. Darvas, J. S. Marcus and A. Tzaras, "Will European Union recovery spending be enough to fill digital investment gaps?", *Bruegel Blog*, 19 July 2021.

Tab. 3.1 - Stages of the Circular Economy

Circular Economy		Strategies	
Increasing circularity	Smarter product use and manufacture	R0 Refuse	Make a product redundant by abandoning its function or by offering the same function with a radically different product
		R1 Rethink	Make a product's use more intensive (e.g. through sharing products, or by putting multi-functional products on the market)
		R2 Reduce	Increase efficiency in product manufacture or use by consuming fewer natural resources and materials
Rule of thumb: More circularity → fewer natural resources consumed and less environmental pressure	Extend lifespan of product and its parts	R3 Re-use	Re-use by another consumer of a discarded product which is still in good condition and fulfils its original function
		R4 Repair	Repair and maintenance of a defective product so it can be used with its original function
		R5 Refurbish	Restore an old product and bring it up to date
		R6 Remanufacture	Use parts of a discarded product in a new product with the same function
		R7 Repurpose	Use a discarded product or its parts in a new product with a different function
Linear economy	Useful application of materials	R8 Recycle	Process material to obtain the same (high grade) or lower (low grade) quality
		R9 Recover	Incineration of materials with energy recovery

Source: RLI 2015, edited by PBL (##)

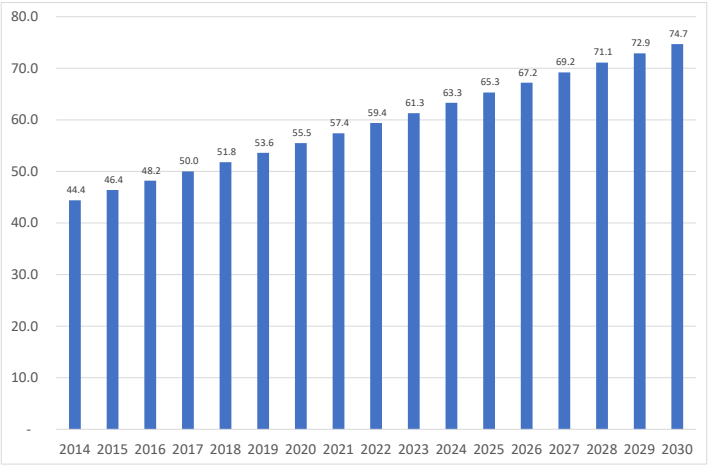
Second, digital technologies might allow a shift to more environmentally friendly production processes – we could produce the same output with less pollution. In particular, the shift from dispatchable fossil power plants to high shares of variable renewables (e.g. wind) is greatly facilitated by digital technologies that are required to adjust demand, and to dispatch and adapt network operation in real-time to fluctuating feed-in of renewable energy. The same holds for electric vehicles, whose large scale deployment will be facilitated by smart charging devices that help to avoid overburdening (local) electricity grids.

This distinction between technologies that increase efficiency, and those that reduce pollution will be important as long as pollution is not properly priced. Technology that increases efficiency might possibly lead to higher pollution, if instead of reducing input, it results in increasing output. Hence, a framework to prevent such negative spill-overs (e.g., pollution pricing) is required. The application of technology to reduce pollution, by contrast, does not entail such risks and can hence be unconditionally supported.

Digital Technologies and use of resources

Information and communication technologies (ICTs) make up a rapidly increasing share of our economies. Accordingly, the specific material and, in particular, energy needs of this sector are growing rapidly. Swift technological progress is leading to a rapid turnover of ICT hardware (e.g. smartphones and computers). Due to the inhomogeneous and composite nature of the materials in obsolete electronic products, they are difficult to recycle. This leads to a growing amount of e-waste. Fig. 3.2 shows the global total in millions of metric tonnes. Figures after 2019 are forecasts, and do not take the Covid-19 pandemic into account.

Fig. 3.1 - Global e-waste (million metric tons - Mt)



Source: United Nations University (2020) Global E-waste Monitor 2020,[4] p. 24, Bruegel calculations

At the same time, electricity is a key input for data processing and telecommunications. While efficiency in terms of computations and data transfer per electricity input have dramatically improved,[5] the even faster increase in demand for computation and communication has led to increasing electricity demand in this sector. For some digital technologies – most notably digital currencies[6] – there are concerns that the energy costs exceed the perceived benefits. This growth in energy consumption by ICTs is obvious in Fig. 3.3; at the same time, the figure illustrates that there are many different scenarios and assumptions that

[4] V. Forti, C.P. Baldé, R. Kuehr, and G. Bel, "The Global E-waste Monitor 2020: Quantities, flows, and the circular economy potential", 2020.

[5] In only 5 years the energy consumption per computation fell by a factor of 5. In June 2013 the most energy efficient supercomputer ("Eurora") achieved 3.2 gigaflops/watt, while in November 2018 the most energy-efficient system was the Shoubu system B with 17.6 gigaflops/watt.

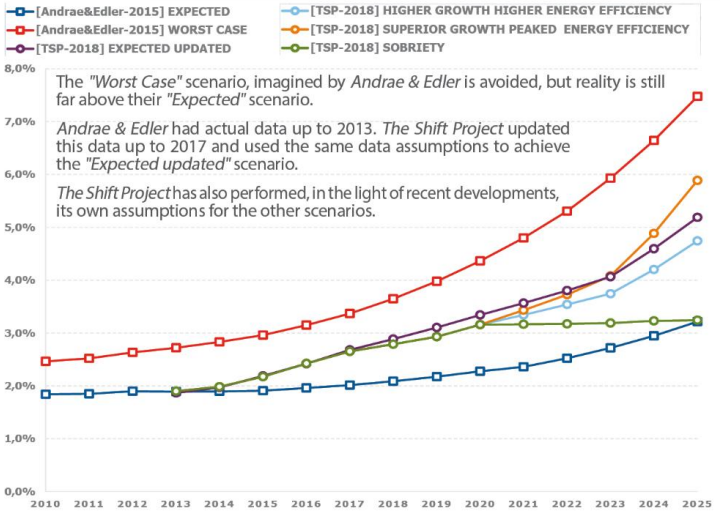
[6] I. Agur et al., "Digital Currencies and Energy Consumption", International Monetary Fund, German Villegas BauerPublication, 7 June 2022.

influence the past and expected future levels of this demand, and considerable uncertainty as to its magnitude.

It is important to bear in mind, however, that the increase in power consumed does not necessarily translate one for one into increased CO_2 emissions. Some of the largest online digital platforms have made substantial investments in order to approach or achieve net carbon neutrality for their data centres. This is one of many instances where firms have voluntarily made investments in green ICTs, presumably not only due to altruism, but also because the initiatives were aligned with their corporate business interests.

The steady improvement in the price/performance of ICTs drives a so-called rebound effect, a point to which we return later in this paper. Less energy is needed to achieve a given quantity of work; however, these technological improvements in resource efficiency make it feasible and economically attractive to do more with ICTs. The net effect is an increase in total energy consumption despite energy efficiency improvements.

FIG. 3.2 - SCENARIOS FOR THE SHARE OF ENERGY CONSUMPTION IN THE DIGITAL SECTOR REMAIN UNCERTAIN



Evolution of global energy consumption of digital between 2010 and 2025, as a proportion of total world energy consumption

Source: The Shift Project (2019), "Lean ICT- Towards Digital Sobriety"

Digital Policy-Making

A last class of linkages is somewhat indirect. Digitalisation enables governments to conduct better-targeted policies (i.e., policies with fewer or smaller negative side-effects). That is, omnipresent sensors, cheaper ubiquitous data transfer, larger data storage and faster processing enable governments to implement policies that were impossible before. Hence, public services can be provided more efficiently, public planning exercises can become more sophisticated, transparency of public decision-making can be increased, laws can be better policed, and the effects of policies can be observed closer to real-time.

This also enables more targeted policies to reduce the environmental footprint. Infrastructure planning based on mobile phone data, granular and real-time control of air quality, targeted incentives and information campaigns are only a few examples of how digital technology enables more sophisticated and efficient policy-making. If digitalisation can allow a society to deploy policies with fewer negative side-effects, this might allow the introduction of more forceful or effective environmental policies.

Challenges and Opportunities in the Light of Europe's Strengths and Weaknesses

Digitalisation will continue to shape our economies and societies irrespective of policy decisions. And Europe stands to benefit.

Capitalising on European capabilities

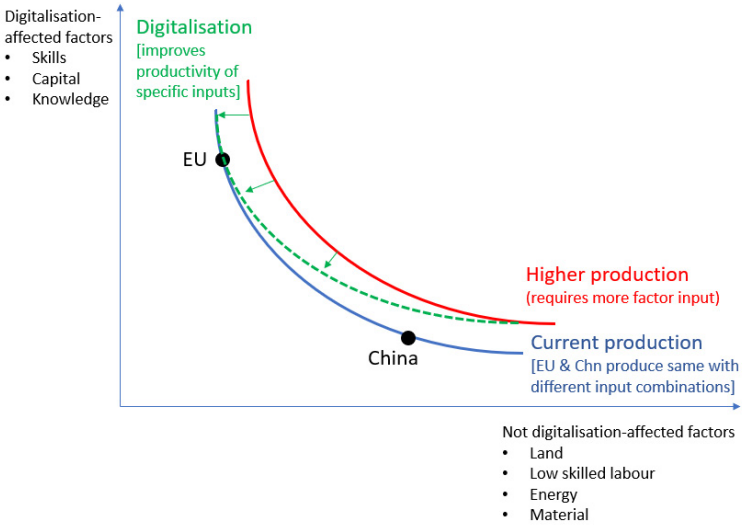
Digitalisation will change the basic production function of an economy:

- increasing the productivity of highly-skilled labour, capital and intangibles;
- while not/less affecting the productivity of energy, materials, land and low-skilled labour.

Intuitively, one should expect that a shift in the production function along these lines would make countries that have a relative advantage in their endowment of those factors for which productivity increases disproportionately better off than countries that are less well endowed with those factors.[7]

If we compare the endowment of these production factors in different regions of the world, it appears likely that the EU could benefit disproportionately from this development. The EU is still doing relatively well in terms of innovation, and it is a large exporter of capital.

FIG. 3.3 - IMPACT OF DIGITALISATION DEPENDS ON FACTOR ENDOWMENT OF AN ECONOMY



Source: Bruegel

[7] A. Goldfarb and D. Trefler, *AI and International Trade*, NBER Working Papers 24254, National Bureau of Economic Research, Inc., 2018.

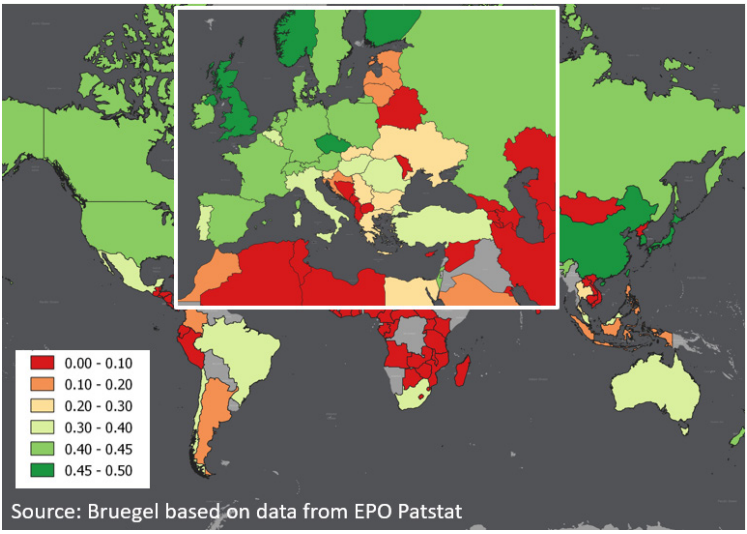
Hence solutions with high use of relatively abundant factors should be favoured. In many services, solutions with very different use of input factors are possible. Recycling, for instance, could be implemented using (1) energy-intensive pyrolysis, (2) resource intensive "thermal recovery", (3) labour intensive sorting, or (4) data/intelligence-intensive sorting approaches. Europe would be more likely to benefit from solutions that rely on relatively abundant factors, notably from data-based approaches.

Europe is strong not only in overall absolute terms (such as number of patents), but also in terms of specialisation in certain digital low-carbon technologies. In terms of energy management technology, European engineers made things possible that had previously been deemed impossible. Around 34% of total German electricity generation in the first half of 2019 was based on wind and solar. But on some days, this generation was close to zero,[8] while on others it represented more than 75% of generation. Managing such volatility in real-time was unthinkable only 15 years ago, when wind and solar accounted for less than 4% of electricity generation. But now, Germany and other countries are able to manage systems with increasing shares of wind and solar with extremely low levels of interruption.

Beyond anecdotal evidence, several EU countries specialise in patenting energy management technologies. Moreover, most EU countries specialise in technologies that are "in the neighbourhood" of energy management technologies; hence, the chances are good they will be able develop comparative advantages in this growing market segment in the future.

[8] E.g., on 24 January 2019 it was 4%.

Fig. 3.4 - Potential comparative technological advantage in energy management tech



Source: Bruegel based on Patstat

Note: the potential comparative advantage indicates whether a country is currently patenting, which has been found to correlate with specialisation in energy management technology (See Kalcik and Zachmann 2017)

The need for nuanced policy responses

Digitalisation will increase the efficiency (output-to-input ratio) of many processes. While efficiency is positive, the net environmental effects are less clear. Increasing the efficiency of certain processes (e.g., machine-learning based searches for new oil-fields) can make polluting activities cheaper and hence lead to more pollution. We noted earlier that the increasing efficiency of ICT operations has led to more consumption of energy, not less, because it became profitable to make progressively greater use of ICTs.

Relatedly, even technologies to reduce the environmental cost of a certain activity might backfire. For example, reducing

the fuel use of airplanes through better airspace management might lower the cost of flying so that the reduced emissions per flight are more than offset by an increasing number of flights. This "rebound effect" also has economy-wide manifestations: if people apply the resources saved through digital technology to more consumer goods, the positive impact of all of these great efficiency enhancing technologies on the environment might well be lost.

It is also important to remember that when it comes to sustainability, interlinkages can be complex and subtle. For example, it is widely assumed that increasing the longevity of a product is positive for sustainability, but this is not invariably the case. A product could be said to pass through three life stages: production, use, and end-of-life. Increasing product longevity is generally positive for the production stage and the end-of-life stage, because fewer units are produced or disposed of. For the use phase, however, the effect can be highly product specific. For a product that is undergoing rapid positive change in terms of energy efficiency and emissions, increasing product longevity might actually have a negative effect in terms of sustainability. For automobiles, for example, increasing product longevity might imply that models with poor mileage stay on the road longer, rather than being replaced by newer, more efficient models with better mileage. These losses in the use stage might offset or even exceed the gains in the production and end-of-life stages.[9]

The challenge of policy-making in the digital age

Governments and administrations can get access to much more granular and close-to-real-time data for their activities. This can be a huge opportunity as it can enable them to reduce

[9] J.S. Marcus, "Promoting product longevity: How can the EU product safety and compliance framework help promote product durability and tackle planned obsolescence, foster the production of more sustainable products, and achieve more transparent supply chains for consumers?", study for the IMCO Committee of the European Parliament, 2020.

negative side-effects of policies. For example, it becomes much easier to understand how people change consumption patterns due to specific environmental taxes. Big data also allows much more experimentation, as different policies might be tested in different regions and the (desired and not-desired) effects on relatively similar household-groups compared.

But this entails two major risks. The first is that administrations might find it very difficult to collect and process such data, and hence might make use of large technology companies that monopolise such data. It is, for example, conceivable that large online digital platform firms might conduct policy planning based on their massive trove of user data.[10] This could be polemically called the US model.

The other risk is that administrations might find it difficult to resist the temptation to collect as much data as possible on their own in order to make their actions as efficient as possible. For example, it might be possible to calculate and regulate individual carbon-footprint based on travel and consumption data. Based on the much-discussed Social-scoring system in China, this approach could be polemically called the Chinese model.

Candidate Measures to Enhance Sustainability

The goal is clear enough – as Europeans, we seek carbon neutrality by 2050. No single "silver bullet" will achieve this, but there are a huge number of individual measures that could potentially help us to reach that goal. Many of those measures are mutually complementary, but others are not, and in any event, there are trade-offs to be made as to the amount of energy and resources to be applied to each instrument.

Broadly, it is possible to distinguish the measures along various dimensions, and across various dichotomies.

[10] Google person finder for crisis management; S. Edelstein, "Waze and Esri Team Up to Offer Traffic Data to City", *The Drive*, 18 June 2019.

- Some affect *consumption* of energy, including not only *residential* consumption, but also *commercial* and *industrial* consumption. The use of ICTs is itself a form of consumption.
- Some are on the *production* side, including *generation*, *transmission* and *distribution* of energy.

Candidate measures on the production side

On the production side, most measures entail shifting the production of energy from fossil fuels to various non-polluting and renewable sources. Digital technology is fundamental to the ability to flexibly shift from one power generation source to another, and to take advantage of a mix of renewable sources and of energy storage (such as, for example, the batteries of electric cars).

In addition to measures that directly work on consumption or production of energy and materials, there are a range of support actions that could be considered, including research activities, and education and training so as to foster sustainability expertise.

Candidate measures on the consumption side

On the consumption side, some measures seek to reduce consumption, while others seek to improve efficiency, and to reduce waste. It is further possible to distinguish between those that seek to reduce or improve the use of energy, versus those that seek to reduce or improve the use of materials (bearing in mind that our use of materials also plays a large role in climate change).[11] These different categorisations on the consumption side can be understood in terms of Figure 3.1.

Our focus here is on measures that benefit from digitalisation, but there are also things that can be done using traditional methods.

[11] Circle Economy and Ecorys (2016) claim that more than "50% of our greenhouse gas emissions are related to material management".

Examples of broad areas where public policy measures that rely on digitalisation might potentially generate gains in terms of energy and materials consumption include:

- Digitalisation of agricultural production and distribution could offer surprisingly large benefits. The FAO (2013) estimates that roughly one-third of all food produced for human consumption in the world is lost or wasted, corresponding to 3.3 billion tonnes of CO_2 needlessly produced per year.[12] In India, development of a farm management platform that provided personalised agricultural advice produced a 64% increase in productivity.[13]
- Continued modernisation and digitalisation of the transport sector so as to favour public transport over the ownership and use of private vehicles saves both energy and materials.
- Collaborative economy services that share vehicles are likewise beneficial. Car sharers cause 13% to 18% less CO_2 emissions.[14] Collaborative economy sharing services could be applicable in many other domains as well.
- Avoiding transportation altogether through increased telecommuting and teleconferencing clearly has a role to play. The Covid-19 pandemic resulted in an enormous increase in working from home. Far more work can be done from home than was done in the recent past. All indications are that a hybrid work pattern, with two or three days per week physically at the office, has become the "new normal" as of 2022.[15]

---

[12] FAO, *Food Wastage footprint impact on natural resources*, Summary Report, 2013.

[13] M. Sawant, M. Urkude, and R. Jawale, Organized data and information for efficacious agriculture using PRIDE model, Int. Food Agribusiness Manage (IFAMA), Rev. 19(A), 2016.

[14] H. Nijland and J. van Meerkerk, "Mobility and environmental impacts of car sharing in the Netherlands", *Environmental Innovation and Societal Transitions*, vol. 23, 2017, pp. 84-91.

[15] Marcus (2022).

- The circular economy is as much a way of looking at the world as a specific measure. It incorporates not only recycling, but also repair, re-use, remanufacturing, refurbishing, and more.
  - Better material tracking and sorting could enhance recycling.
  - Achieving longer product lifetimes is an aspect of the circular economy. Fairly simple measures such as ensuring that mobile device batteries can easily be replaced could be considered. As previously noted, however, extending product lifetimes entails complex trade-offs if the products themselves are becoming more sustainable over time.
  - Circle Economy and Ecorys (2016) estimate that the circular economy could reduce global greenhouse gas emissions by 7 billion tonnes of CO_2 per year.[16]
- Green ICTs represent another candidate set of measures on the consumption side. The information technology (IT) sector consumes approximately 7% of global electricity today, and it is predicted that this share will increase to 13% by 2030.[17] The sector itself has undertaken some initiatives, such as shifting large data centres to make greater use of renewable energy.
- Empowering consumers by providing better information on their consumption of energy and materials at home also has a role to play. In one Chinese study, smart metre installation led to a 9% reduction in monthly electricity consumption.[18]
- Strengthen the monitoring of environmental impacts and loss of biodiversity in order to enable better policy formulation and enforcement.

[16] "Implementing Circular Economy Globally Makes Paris Targets Achievable", *Circle Economy and Ecorys*, 2016.

[17] R. Sadler, Video Demand Drives up Global CO_2 Emissions, 2017.

[18] Xingxing Zhanget al., "Smart meter and in-home display for energy savings in residential buildings: a pilot investigation in Shanghai", *China, Intelligent Buildings International*, vol. 11, no. 1, 2019, pp. 4-26.

Recommendations

Our recommendations here pertain for the most part to process and methodology, rather than to specific policy measures. All or nearly all of the candidate themes for policy measures put forward in the previous discussion probably merit some degree of attention from policymakers.

- In formulating public policy, take a strategic view, and adopt an EU Better Regulation perspective: define problems, identify candidate solution options, provide comparative assessments of options, choose approaches that are most likely to be effective, efficient, and coherent with one another and with other EU policies.
- Do not be afraid to lead: Europeans are passionate about issues of sustainability. Europe has many opportunities to move the global debate forward, and these are not limited to formal negotiations.
- Consider the judicious use of regulation and standards. Europe plays a large role in global markets, both as a producer and as a consumer. GDPR demonstrates that European initiatives can have a global impact. Existing EU rules that cover not only product safety, but also waste and hazardous substances in electrical and electronic equipment already have influence. More could be done. As a concrete example, consider the global impact that might flow from an EU prohibition on the sale of mobile devices for which the user cannot change the battery.
- Consider the judicious use of trustmarks. The CE trustmark could potentially also be a potent tool in promoting sustainable practices. The German BMU plans to develop a trustmark for environmentally compatible AI, and Germany already has a Blue Angel trustmark that encourages the energy and resource efficiency of ICT systems and data centres.[19]

[19] Marcus (2020).

- Enlist the public. It is important to promote social engagement and environmental consciousness. More can be done to facilitate the public's visibility into environmental data, and to make it more comprehensible to Europeans.
- Rethink public subsidies. They should focus on forward-looking and sustainable themes where Europe potentially has a competitive advantage. Subsidies for energy-intensive industries where the EU enjoys no competitive advantage (aluminium being an obvious example) appear to run counter to sustainability goals.
- Expand research on possible ways to use digitalisation to promote sustainability, in terms of energy production and energy consumption by all sectors (including by digital technology itself, i.e. green ICTs).

This broad portfolio of potential policies mirrors the many ways in which digitalisation and sustainability can interact. In each of these areas, the concrete policy response needs to be tailored to the problem. But it is also clear that, while digital technology will provide important tools to increase the sustainability of our economic model, technology alone will not solve the problem. Substantial carbon prices in all sectors remain crucial to push households, government and industry to use these new technologies to actually reduce emissions.

4. Changing the Game: The Role of Technology and Data to Increase Infrastructure Efficiency

Monica Bennett

With at-scale adoption of infrastructure technology (InfraTech), we can achieve our biggest objectives, like hitting net zero and achieving the sustainable development goals. But we're currently a long way from having the type of investment we need to achieve InfraTech adoption at scale. The good news is that momentum is building globally to find innovative ways to develop and finance these solutions among governments, investors, and those involved in planning, financing, delivering, and operating infrastructure.

This chapter aims to be a brief, accessible summary of:

- Key reasons experts believe InfraTech is essential to the climate transition and other global priorities.
- Benefits of investment in InfraTech and some data quantifying these benefits.
- The two strategic-level opportunities to scale up InfraTech investment.
- Practical examples of how to increase InfraTech investment in ways that get the greatest value from the technology.

By collating key threads of others' work and combining these with new analysis and thought leadership from the Global Infrastructure Hub (GI Hub) and our partners, I aim to provide

a paper that can be a practical starting point for understanding the state of InfraTech and advancing it in your sphere of influence. I want to encourage further participation and start to build confidence among the full range of stakeholders who are critical to reaching our biggest collective objectives through InfraTech.

The Benefits of Investment in InfraTech

Many individuals and organisations have effectively made the case for greater investment in InfraTech,[1] and I won't duplicate their work here.[2] At the core of each argument is infrastructure's central role in achieving prosperity in our societies and economies, and InfraTech's ability to deliver efficiencies, transparency, and better quality and outcomes from infrastructure.

"Infrastructure" is not only a collection of physical assets, but also one of the most impactful levers governments have for a resilient and inclusive future. After all, Infrastructure systems have been shown to influence achievement of all SDGs, including up to 92% of targets.[3]

---

[1] For this chapter, we define InfraTech as: Digital and non-digital technologies that can be integrated with physical infrastructure to deliver efficient, connected, and resilient assets and to achieve sustainability and inclusivity outcomes. Within this definition, we note that some "breakthrough technologies" have the potential to rapidly accelerate progress toward digitalisation, use and leveraging of data, and the adoption at scale of specific technological solutions. However, InfraTech has significant potential to drive transformation even without application of individual breakthrough technologies.

[2] A few of the many good resources are: World Economic Forum (WEF), *Infrastructure 4.0: Achieving Better Outcomes with Technology and Systems Thinking*, May 2021; PwC and the Global Infrastructure Facility, *Promoting InfraTech adoption across the Infrastructure lifecycle*, 2021; and McKinsey & Company, "Making infrastructure tech a reality in your portfolio", June 2021.

[3] United Nations Office for Project Services (UNOPS), *Infrastructure for Climate Action*, 12 October 2021.

This transformative potential of infrastructure will remain untapped until we start to integrate emerging practices and technological innovation across the infrastructure lifecycle, and there will be many challenges to this integration of technology. Infrastructure has been called "one of the least digitally transformed sectors of the economy"[4] and the World Economic Forum states that "While infrastructure traditionally moves at a staid pace with projects that take years and assets that last lifetimes, this current technological revolution is outpacing previous ones at an unprecedented speed. Infrastructure is letting this wave of innovation race right by it".[5]

The slow pace of the technological shift in infrastructure is unsurprising, given that both the infrastructure and technology sectors are complex ecosystems that have been evolving independently of each other for decades. The successful integration of the two sectors calls for the creation of a new ecosystem – an "InfraTech ecosystem" that is the convergence of both worlds to address the unique challenges and opportunities for technology in infrastructure.

Another key challenge to the adoption of technology in infrastructure is the insufficient investment going into infrastructure itself. The investment gap in infrastructure could be as high as $40 trillion out to 2030.[6] Large-scale change is urgently needed to bridge this gap, and ensure we get as much value as possible from every dollar spent.

At the GI Hub, we have identified 13 areas where infrastructure can make a significant and positive long-term impact, denoted as "transformative outcomes".[7] They include areas like the low-

[4] World Economic Forum (WEF), *Transforming Infrastructure: Frameworks for Bringing the Fourth Industrial Revolution to Infrastructure*, November 2019.

[5] World Economic Forum (WEF), *Infrastructure 4.0: Achieving Better Outcomes with Technology and Systems Thinking*, May 2021.

[6] Analysis of various data sources including Organisation for Economic Co-operation and Development (OECD), McKinsey, Global Infrastructure Hub (GIH), and International Energy Agency.

[7] Global Infrastructure Hub (GIH), *Transformative Outcomes Through Infrastructure*.

carbon transition, environmental regeneration, affordability and access to services, digitalisation, and disaster and climate adaptation. Our work on transformative outcomes helps encourage a different way to think about planning, financing, and delivering infrastructure, and to consider how infrastructure investments can target one or more transformative outcomes to get more "bang for buck".

For example, long-term goals like the climate transition cannot be achieved just by reducing carbon emissions. To reach net zero, we will need to address multiple transformative outcomes in tandem, including reducing carbon emissions and increasing affordability (e.g. so people can afford to use the "green" infrastructure), inclusive mobility (e.g. to ensure wide adoption of low-carbon modes of transport), disruptive innovation (e.g. to ensure that we are gaining access to the new technologies needed for the transition), and digitalisation (e.g. to ensure that we have transparent data to measure progress against our climate goals). InfraTech can be an effective way to achieve multiple transformative outcomes within a single investment.

This need to address multiple transformative outcomes through infrastructure investment – and InfraTech's role within in doing so – has been recognised by the G20 as a priority especially in the context of the $3.2 trillion of additional and accelerated infrastructure investment announced between February 2020 and August 2021.

Critical Opportunities to InfraTech Investment

Although investment in individual infrastructure technologies and specific infrastructure programs and projects is beneficial, what we need most are international- and national-level approaches that enable at-scale adoption of InfraTech. There are two overarching opportunities to achieving this: the strategies that direct investment to InfraTech, and the capacity to convert R&D investment into commercial adoption (the application/implementation stage). Addressing these barriers will help

ensure greater benefits to infrastructure from technology – and therefore greater advances toward our biggest objectives.

The Strategies that Direct Investment to InfraTech

The greatest positive impacts will come from technology that can be scaled at the regional, national, and international levels using replicable commercial and financial models.

Directing investment to InfraTech projects that are scalable and replicable requires a coordination of efforts and action across all levels of government, and between the public and private sectors. Currently, there are only a few global, national, or regional initiatives driving such coordination.

At the G20 level. In recent years, the Saudi Arabian (2020), Italian (2021), and Indonesian (2022) G20 Presidencies have each given priority to infrastructure technology in their work plans, and supported initiatives related to InfraTech that are relevant to both G20 countries and other countries.

The Saudi G20 Presidency introduced the G20's InfraTech agenda, the *G20 Riyadh InfraTech Agenda*,[8] and notable items produced that year to support the agenda and help G20 countries advance InfraTech included:

- A reference note on InfraTech value drivers, which outlined the potential economic, social, and environmental value to countries from InfraTech adoption, and a framework for evaluating benefits against costs and risks.[9]
- A Stocktake of InfraTech Use Cases, showing about 70 program- and project-level implementations of InfraTech across sectors and countries.[10]
- An InfraTech Policy Toolkit that outlines priority areas and tools for policymakers to implement the InfraTech agenda.[11]

[8] G20, *G20 Riyadh InfraTech Agenda*, 2020.
[9] World Bank Group, *InfraTech Value Drivers*, 2020.
[10] Global Infrastructure Hub (GIH), *Infrastructure Technology Use Cases*.
[11] World Bank Group, *InfraTech Policy Toolkit*, 2020.

The Italian G20 Presidency in 2021 continued the work on InfraTech by seeking to strengthen digital infrastructure and connecting digitalisation to its other objectives like improved maintenance and resilience.[12] It also supported the InfraChallenge, an international innovation competition focused on InfraTech.[13]

This year, the Indonesian G20 Presidency has dedicated a work stream to increasing InfraTech investment. This work stream is a continuation of the *G20 Riyadh InfraTech Agenda,* and to this end the GI Hub is furthering our work on the stocktake of InfraTech use cases and developing an actionable *G20 Blueprint for Scaling up InfraTech Financing and Development*.

Each of these initiatives offers thought leadership, builds knowledge around InfraTech and opens pathways to help inform strategies, whether by suggesting policy frameworks, funding and financing approaches, use cases for technology, collaboration mechanisms, or other solutions. However, G20 initiatives require partners such as individual governments and international institutions like multilateral development banks to operationalise this knowledge and put it into action. In many cases there are still too few linkages between these global initiatives and the operational frameworks at the national and regional levels where they can be actioned and implemented. To date, progress has been slow.

At the national and regional levels. Many countries have national infrastructure strategies that establish their infrastructure priorities, although the level of detail and contents of these plans vary widely. In recent years, more countries have begun updating their plans to incorporate global transition goals related to the SDGs, Paris Agreement, or net zero targets. Our review in 2022 found that 85% of G20 countries are planning to incorporate InfraTech in their infrastructure investments in the long-term. However, only 35% of these countries have plans

[12] More on the Italian G20 Presidency's priorities and deliverables can be found on the GI Hub website at https://www.gihub.org/about/g20-infrastructure-outcomes/.

[13] Global Infrastructure Hub (GIH), InfraChallenge.

with a high degree of maturity (i.e. including detailed targets and investment information). Perhaps as a result of this overall lack of maturity in national InfraTech plans, technology is often deployed on a project-by-project basis with no clear, "joined up strategy". The World Bank, in its *Policy Toolkit*, highlights the need for national approaches that set a vision for the application of technology in each stage of the infrastructure lifecycle and set forth how the government will support adaptation to the changing technology landscape:

> The national approach can be suited to each country's context and national goals, while also ensuring that all segments of society … benefit from InfraTech and are not left behind. The plan can also help identify opportunities for regulatory change and reduce bureaucratic obstacles. Because InfraTech is not limited to national borders, the plan should consider international standards.[14]

One example of a country that has a national InfraTech and digital transformation strategy is Brazil, which successfully garnered up to $1 billion of investment support from the Inter-American Development Bank to implement its Brazil Plus Digital program that aims to finance integration and digital transformation in digital infrastructure, the digital economy, digital government, and enabling factors in digital transformation.[15]

Among entities at the planning level. Often, national strategies are the catalyst for subnational/regional strategies and plans and other policy innovations across the infrastructure lifecycle (in particular in project preparation and procurement), so in the absence of national strategies it is not surprising that regional plans and other policy innovations have also been slow to develop. However, as national plans are developed, regional plans must follow.

---

[14] World Bank Group, *InfraTech Policy Toolkit*…, cit.

[15] Inter-American Development Bank (IDB), *Brazil to boost digital transformation with IDB support*, 2021.

The World Bank emphasises the key role of local governments in InfraTech development (and also cites the example of developments furthered by the creation of smart cities) and recommends that both national and sub-national plans focus on strategic multisector and sector planning. It says strategic multisector and sector planning is fundamental in many ways, but not least because this planning helps ensure "appropriate attention" to InfraTech investments that can benefit multiple infrastructure sectors, help to foster a trusted data sharing ecosystem, and build the local InfraTech entrepreneurship ecosystem.[16]

There are several cohorts working on the integration of InfraTech within the upstream enabling environment for infrastructure. For example, the World Economic Forum established its Infrastructure 4.0 project community in 2020. Infrastructure 4.0 was formed to work across sectors and industries to encourage a more holistic, outcome-focused framing for infrastructure and to share the best strategies for improving the adoption of technology into infrastructure development.[17]

Despite this momentum, the use of InfraTech is not yet a mainstream practice in infrastructure development, and there is currently little evidence available on the effectiveness of these approaches. Without data-evidenced, strategic directions and plans from governments to drive InfraTech, it is incredibly difficult to increase investment either from the public or private sectors. Governments are unlikely to progress a commitment to InfraTech into their budgets without a well-defined strategy, and private sector investors and participants need to see a clear path for a technology to achieve scale and provide a strong return.

[16] World Bank Group, *InfraTech Policy Toolkit*…, cit.

[17] World Economic Forum, *Infrastructure 4.0*…, cit.

The Capacity To Convert R&D Investment Into Commercial Adoption

At the moment, the number of technologies available massively outpaces the number of technologies being adopted in infrastructure at scale. Of course, not all products and inventions become commercially successful,[18] but even for those products with clear potential for impact, there is a critical gap in the industry's capacity to convert R&D investments into a commercially successful product that gets adopted at scale. This gap is often called the "valley of death". This is a problem because the newest (and potentially highly impactful) technologies are not becoming commercially available quickly enough – or, in the case of many technologies, aren't becoming commercially available at all.

This misalignment between technology development and adoption is both a cause and a result of the fact that investment is either directed into technology development or delivery of infrastructure, but not necessarily the integration of both. One source[19] identifies the biggest investment gap during the "first commercial operation" stage of technology development, where the financial investment into a demonstration project could be as high as 50-100 million (Figure 4.1). The problem is not so much the availability of capital but rather the perceived imbalance in the risk/return profile of investing in a new technology.

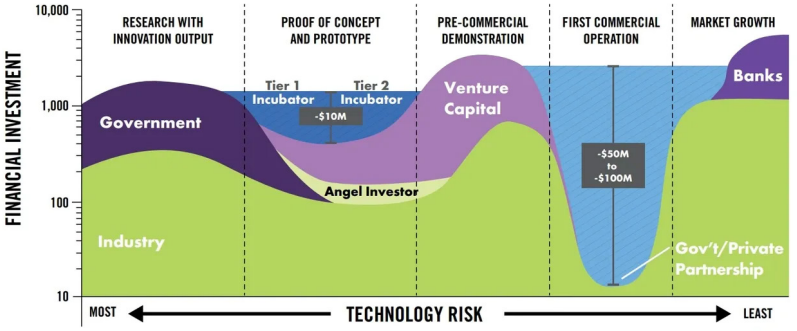
Investment in technology development. As can be seen in Figure 4.1, there is a diverse range of funding sources for early-stage research and development, including venture capital, incubators, governments, and other private companies across

[18] When it comes to commercialising university technologies, globally less than 5% make it to an actual commercial product that generates revenue for both the inventors and the university. See "Commercialising new technologies needs a two-way partnership", *Australian Financial Review*, 2021.

[19] Maryland Energy Innovation Accelerator, *Announcing the Maryland Energy Innovation Accelerator*, 2019.

the industry. This is the domain where R&D groups, start-ups, and small-to-medium sized enterprise (SMEs) conceptualise, prototype, and test technological solutions that are relevant to infrastructure. Through the transformations of the Third and Fourth Industrial Revolutions, this has grown into a robust domain with an entrepreneurial spirit. It generates the innovation, change, and sometimes market disruption that can ultimately be leveraged in infrastructure to realise better and greater outcomes. When it struggles to garner investment, it is usually because of a combination of company and market-related issues, such as the strength (or lack thereof) of the management team, the integrity of the concept/prototype, or uncertainties about the ability to drive adoption of these technologies at scale. These technology companies would benefit from mentoring, partnering, and coaching to instil greater confidence and attract these larger sums of investment.

Fig. 4.1 - Sources of capital across the technology development lifecycle



Source: Maryland Energy Innovation Accelerator (https://mdeia.org/blog/f/announcing-the-maryland-energy-innovation-accelerator)

Investment in infrastructure. Infrastructure programs and projects are developed and financed by governments, multi-lateral development banks, the private sector, or a combination of

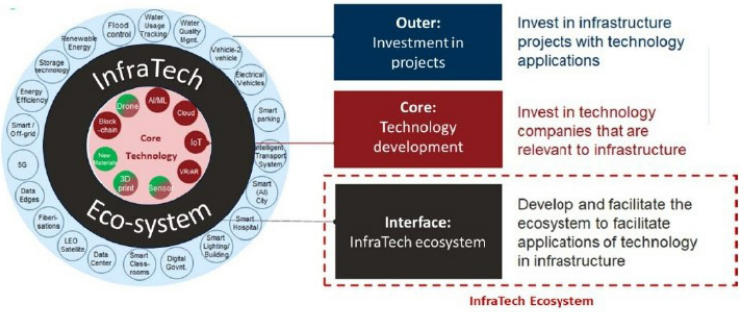
all three. These programs and projects often align with a national strategy or plan for infrastructure as well as the requirement to achieve a public good, which are reflected through our 13 transformative outcomes as mentioned previously. However, the mechanisms by which infrastructure is developed and delivered are highly complex, and in many instances the opportunities to integrate technology into that complex process is overlooked. As a result and as noted above, investment into new technology in the application/implementation stage is progressing slowly, primarily due to perceived risk and cost constraints, but also in some cases due to knowledge or capacity gaps. InfraTech, however, is critical to the quality of infrastructure as it enhances performance, security, efficiency, and cost – but it is also where common constraints like lack of commitment or incentives, lack of data on technology performance, lack of funding, lack of experience/capability, and perceived risk can prevent solutions from being identified and adopted.

Integration of InfraTech in infrastructure development, financing, and delivery. The activities within technology development and in infrastructure investment are well established and underway. However the InfraTech ecosystem, which involves two-way collaboration and communication between technology developers and the financiers of infrastructure projects, is not well-established – nor is it operating in an effective way.[20] Integration of InfraTech is critical to success and can be addressed through an InfraTech ecosystem – a collaborative forum of stakeholders from the public and private sectors who collectively understand policy and regulatory environments, investment drivers, the infrastructure lifecycle, and the research and development environments of technology companies, and can provide a focal point for both strategic leadership and practical advice (Figure 4.2). The goals of the ecosystem are to build public and private sector capacity,

[20] Global Infrastructure Hub and Asian Infrastructure Investment Bank, *G20 Blueprint for Scaling Up InfraTech Financing and Development*, 2022.

knowledge, and confidence in adopting InfraTech to help bridge the "valley of death" for technology companies, and also to support governments and investors to integrate InfraTech into decision-making for infrastructure.

FIG. 4.2 - INFRATECH ECOSYSTEM



Source: AIIB Analysis

As technologies are developed and made ready for adoption, there is a clear need for innovative approaches to de-risk technology investment, and attract investment across both the development and implementation stages to support InfraTech adoption at scale.

Solutions To Attract More Investment into Infratech at Scale

Data to make more informed decisions

The *G20 Riyadh InfraTech Agenda* recognises InfraTech as a key enabler to attracting private investment into infrastructure with a view to closing the ever-increasing infrastructure investment gap. This is primarily linked to its ability to generate data and increase transparency, and can be summarised by two main benefits:

- Enable governments and investors to make better operational decisions by providing better transparency of the day-to-day performance and condition of an infrastructure asset across its lifecycle, and its impact on the environment and society.
- Enable governments and investors to make better strategic investment decisions towards more sustainable infrastructure, by enabling better project prioritisation and by capturing value from their investments through additional revenue streams and realisation of alternative financial benefits.

Yet, we aren't successfully capturing and aggregating such data and making it widely accessible to the industry through a centralised platform. Much of this data is being captured at the localised project level (if it is captured at all). This lack of transparent, accessible, data-based evidence on InfraTech performance is a limiter of investment to InfraTech, but also to infrastructure more broadly as noted above.

In today's world of big data, there are almost limitless ways that government and industry could capture, aggregate, analyse, and improve access to data. In this context, a more global, centralised approach would create transformative impact on the capacity to invest in technology and innovation in infrastructure. Greater coordination on making data available and accessible could be a task for a well-linked InfraTech ecosystem, as described above.

Government policies and national strategies

A detailed exploration of government policies for InfraTech is beyond the scope of this paper, particularly given the comprehensive work done by the World Bank Group in 2020 through the *InfraTech Policy Toolkit.*[21] However, the GI Hub's recent work on InfraTech (including in the *G20 Blueprint*

[21] World Bank Group, *InfraTech Policy Toolkit*…, cit.

for Scaling Up InfraTech Financing and Development) points to two pertinent opportunities in terms of policies: (1) need for national or sectoral InfraTech strategies and the need to involve the private sector in forming these policies to maximise participation and investment, and (2) need for innovative procurement policies and tools that attract and incentivise investment in InfraTech throughout the lifecycle.

Policies and strategies can set the stage for the development of infrastructure programs and projects in partnership with the private sector and multilateral institutions, which allows more innovation and flexibility in funding/financing and risk sharing to maximise investment. These strategies and policies can also incentivise and create formal links between InfraTech start-ups and the infrastructure programs and projects where the start-ups' technologies will be adopted. Similar initiatives have been shown to direct funding to fast-track the development and adoption of InfraTech.[22] Two examples are the Madrid 360 Environmental Strategy and the UAE's Energy Strategy 2050 and Sustainability Strategy. Furthermore, national strategies can also accommodate the creation of "innovation sandboxes" and encourage the embedding of InfraTech within government procurement processes.

Innovative procurement policies and tools are also critical to increasing investment and adoption of InfraTech. Our recent work indicates that there are emerging, innovative approaches in this space but that this area still requires further attention and development. However, governments can apply ideas and learnings from other countries and adapt them for local use. A solution developed in Argentina, for example, could reinvent the way renewable energy is procured in developing countries. Argentina's analytics for renewable energy auctions

[22] Two selected case studies on national strategies that incorporate InfraTech, as collected by the Global Infrastructure Hub (GIH) and the Asian Infrastructure Investment Bank (AIIB) through the G20 Blueprint work, were the Madrid 360 Environmental Strategy and the UAE's Energy Strategy 2050 and Sustainability Strategy.

(AreA) is a novel solution to design and conduct the entire Renewable Energy Procurement Program (REPP) online – which combines an innovative policy with the use of InfraTech itself to transform the way renewable energy projects are being procured nationwide.

By raising awareness and learning how to incorporate innovative elements into their policies and strategies, with participation from the private sector and an eye on increasing InfraTech investment, governments can set the direction for their policymakers to enable the adoption of InfraTech and influence the outcomes positively in each stage, looking beyond their individual roles to achieve better results together.

Innovative Delivery Models

The mainstreaming of InfraTech into infrastructure will require the evolution of infrastructure delivery models to ensure that the right kinds of stakeholders (with their associated knowledge and expertise) are involved in the project and that there is the right balance of risk among stakeholders. As the World Bank has said in its *InfraTech Policy Toolkit*, "Innovation, by its very nature, is agile and involves risks and mistakes".[23] Technologies that bring uncertainty will raise challenges for governments in finding balance and responding in a timely fashion.

The GI Hub has identified, among other solutions, the application of innovative delivery models as a way to ensure a successful and efficient operation of an InfraTech project. An example is the use of concession contracts to delivery energy efficiency upgrades, for example as was done at Ohio State University in the US, which entered into a concession agreement involving a more than $1 billion up-front lease payment to handle the University's energy management including distribution, operating heating and cooling systems,

[23] World Bank Group, *InfraTech Policy Toolkit*…, cit.

optimisation and usage reduction, asset management, and network expansion over a 50-year concession period.[24]

An important element to this commercial shift is to build out the InfraTech ecosystem and ensure that key players are well-equipped with the right skills and knowledge to execute. A more mature ecosystem operating across international, national, and local levels could help improve connections and "matches" between stakeholders, and play a key role in removing the barriers to collaboration. An example of an InfraTech ecosystem is one being operated by the Asian Infrastructure Investment Bank (AIIB). AIIB is developing a holistic platform to scale up InfraTech investments in Asia. Activities are designed to drive Infratech investments tailored to sponsors, investors and financiers: from identifying technology to matchmaking stakeholders, and from capacity building to providing debt/equity financing for InfraTech projects.

Given that there are already many actors operating through ad-hoc and informal linkages, there may be an opportunity to leverage this activity, provide an international focal point for these stakeholders to interact, and build a more mature ecosystem relatively quickly. Activities for the InfraTech ecosystem could include:

- Knowledge-building activities like sharing definitions, taxonomies, or standards for data capture and assessment in InfraTech.
- Development-based activities like creating shared platforms for governments and investors to source and prioritise technologies and commercial approaches.
- Collaborative activities, like working with educational institutions to create a curriculum and upskill future infrastructure professionals in InfraTech. This opportunity is currently in development by a group of international experts and educators.

[24] Global Infrastructure Hub (GIH) case study "Ohio State University Service Concession".

For the industry to evolve and benefit from wide adoption of InfraTech, both governments and the private sector must find ways to accommodate innovation and risk-taking, and build up shared solutions and systems within a robust InfraTech ecosystem.

Technology Integration Solutions

Data is a core opportunity in making the case for scaling up InfraTech, as outlined above. There is also a core opportunity and consideration in how data is made secure and standardised so that it can be utilised to its greatest potential. Two particular strategic opportunities/considerations are worth noting.

The use of digital twins is revolutionising the infrastructure lifecycle and enabling infrastructure to be created, operated, and maintained with exponentially more accuracy, effectiveness, and cost-efficiency. The full potential of digital twin applications in infrastructure is so vast that it deserves a particular focus from governments and investors on learning how best to shape its use cases and to integrate this solution as a standard tool for decision-making across the infrastructure lifecycle. The GI Hub's InfraTech use case library[25] identifies several use cases for digital twins in infrastructure, for example Akselos' digital twins for structural condition assessment of power stations helped increase the overall confidence of the operations team, enhanced operator safety, extended asset life and reduce cost over the project life.[26]

The other strategic area that must be considered is cybersecurity and privacy measures. This is a deep and technical topic which will not be explored in detail for this chapter (and

[25] Global Infrastructure Hub (GIH) use case library available at: https://www.gihub.org/infrastructure-technology-use-cases/

[26] Global Infrastructure Hub (GIH), World Economic Forum (WEF), and Akselos case study available at: https://www.gihub.org/infrastructure-technology-use-cases/case-studies/digital-twins-for-structural-condition-assessment-of-power-stations/

more likely within the realm of digital infrastructure rather than InfraTech specifically) however it should still be noted that security, safety, and ethical concerns in utilising data from infrastructure operations are critical to instil confidence and gain wide user acceptance. The importance of this can be easily seen in examples in digitalisation of public health records or the deployment of autonomous vehicles – where the wrong rules or standards could lead to serious consequences.

Innovative Funding and Financing

As defined by the International Monetary Fund,[27] funding of a project refers to how investment and operational costs are repaid over time; in the case of public infrastructure, this means by users, taxpayers, or a combination of both. Financing refers to money raised up front – through equity or debt instruments – for the design, construction, and early operating costs of an asset.[28]

In the context of this definition, it is therefore important to distinguish funding and financing of technology development from funding and financing of InfraTech-enabled infrastructure (i.e. the implementation of technology within an infrastructure project). As the funding and financing models for InfraTech-enabled infrastructure are likely to be the same as those for infrastructure projects more generally,[29] the focus of this section will be on funding and financing technology development.

There are numerous ways in which InfraTech development can be funded and financed, and some of these were identified above in Figure 4.1. This includes a combination of public and private investment – either through government/corporate

[27] International Monetary Fund (IMF), *PPP Fiscal Risk Assessment Model*, 2019.

[28] Global Infrastructure Hub (GIH), *Innovative funding and financing of infrastructure*, 2021.

[29] At this stage, InfraTech-specific instruments have not yet been identified through the Global Infrastructure Hub's research.

budgets or innovative funds and platforms. The Trial Reservoir (operated globally by Isle Utilities) is an example of this kind of platform.[30] The Trial Reservoir accelerates technology adoption in the water sector through loans for trials, which minimises the risk of piloting new water technology solutions, and Isle Utilities staff provide technical support. The loans are only repaid if the trial is a success.

Alongside innovative funds and platforms is the need to unlock public investment dedicated to InfraTech, and there is evidence that indicates the potential transformative economic impact from public investment into InfraTech. Last year, the GI Hub's InfraTracker examined infrastructure stimulus announcements post-Covid, and linked these to a range of spending types including technology-related fiscal measures. The mapping of infrastructure stimulus across G20 countries to sectors and outcomes found that 17% of the $3.2 trillion announced by G20 governments was attributed to digitalisation or InfraTech.[31] This evidence should ideally open the door for further examination of the role of public investment in scaling up InfraTech investment, including analysis of the impact of InfraTech to close the investment gap and generate cost efficiencies and savings for governments.

Moving Ahead

InfraTech adoption at scale has the potential to be a bridge in the infrastructure investment gap, helping to enable infrastructure to fulfill its potential as a driver of sustainable development and a resilient and inclusive future. InfraTech's contribution is essential, particularly to respond to the climate crisis and economic recovery from Covid-19, and we urgently need to increase investment in InfraTech – particularly at the adoption/implementation stage and particularly in new technologies.

[30] https://www.isleutilities.com/services/trial-reservoir

[31] Global Infrastructure Hub (GIH), *Transformative Outcomes Through Infrastructure*.

The solutions outlined in this paper are actionable at the "individual" level, but by working together as an ecosystem, we can maximise adoption of InfraTech at scale and achieve our biggest objectives. Maturing an InfraTech ecosystem to support adoption of InfraTech at scale should therefore be one of our core focuses.

5. The Internet of Things and Artificial Intelligence to Infrastructure: A Game Changer?

Giovanni Miragliotta, Carlo Negri, Alessandro Perego, Alessandro Piva, Giulio Salvadori, Angela Tumino

The digital revolution is no longer news, yet as it becomes more firmly established, its very nature is changing because of the introduction of innovative technologies and business models to various new sectors and new developments in existing ones. In addition to areas in which the digital transformation has already triggered radical change – as eCommerce has transformed the boundaries and competitive logic of the retail sector – new markets are constantly being impacted by digital technology. Though the pandemic severely tested the economies of many nations and slowed investment in digital technologies by public and private companies, it also expedited the shift towards digital technology in traditional markets and sectors, establishing practices such as smart/remote working, WFH (work from home) and WFA (work from anywhere) in one form or another. Though these new working paradigms had been under scrutiny for some time, they were given a major boost by Covid-19 and soon became consolidated as a new work mode for public and private organisations around the world.

The infrastructure sector also faces the challenge of rethinking itself digitally and adapting a smart paradigm. Buildings, bridges, roads, and major construction projects could provide feedback on their conservation or operation

status to improve the management of the entire system. Such a new paradigm would be based on IoT (Internet of Things) technologies. Environmental accelerometers, inclinometers and extensometers, for example, can help monitor the status of infrastructures in real time and throughout their entire lifecycle. IoT technologies are constantly developing and are already well established in several sectors, from smart homes to smart factories as well as smart metering and agri-food. It is estimated that the global market for IoT could reach $2,465.26 billion in 2029 (Fortune Business Insight). There is also a growing emphasis on value-added services as a means to move away from isolated sales of connected devices to the valorisation of data collected by artificial intelligence. The integration of these two technologies, driven by the trend towards servitisation, could permit predictive maintenance and pre-empt the occurrence of serious structural damage.

Artificial Intelligence and new automated learning technologies such as machine learning and deep learning allow value to be generated from data by identifying correlations between variables and making predictions about the future. An example is the AI-processing of bridge tension, inclination, expansion, and contraction data correlated with weather conditions or camera-detected vehicle transit. Together with advanced analytic or anomaly detection models, deep learning has led to improvements in image analysis. In conjunction with sensors, image analysis can now be used to monitor large structures, especially using data-driven, feature-based techniques that enable image recognition and categorisation. There is even no need to design a feature extraction phase, which can be performed instead by a specific type of neural network, i.e. convolutional neural networks. These deep neural networks are particularly well suited to natural image processing, though their training requires a large amount of appropriately annotated data and results in the loss of the model's interpretability.

Integration between the IoT and AI is becoming so advanced that AI can now operate within connected devices, allowing for

improved functionality and local data processing. Much of the computing power of connected devices can therefore be used to maximise their decision-making powers, so that only pre-processed information is brought into the cloud, thus reducing the amount of data to be managed with a positive impact on data processing times. Edge computing is essential for solutions that require a fast response to external stimuli, such as smart grid applications for network optimisation and demand management. In an energy supply scenario in which users are gradually becoming prosumers, edge computing enhances response and can manage energy storage to cope with peaks in demand and the increasingly pervasive presence of intermittent renewable energy sources.

An additional benefit of AI is the possibility of automating inspections using drones or autonomous robots to conduct visual surveys even under difficult conditions. Both these physical systems can implement complex AI solutions featuring capabilities that permit operation in and interaction with the surrounding area. The use of appropriate cameras could enable regular maintenance inspections to be performed in industrial and civil contexts without human intervention, for the conservation of buildings and infrastructure. Moreover, in future years, AI systems will be able to operate as infrastructure managers, providing support, for example, in smart city traffic control centres to assign the appropriate priority to vehicles, and in factories to monitor manufacturing processes and make autonomous decisions to reorder raw materials or schedule system maintenance.

The digitalisation of bridges, roads, viaducts, buildings and the consolidation of smart infrastructure in general will not only prove useful to improving asset management but will be essential to achieving the green transition and sustainability goals to which the European Union has assigned so much funding. Research conducted in recent months by our Digital Innovation Observatory Research Group shows that digital technologies allow economic and environmental goals to be

achieved in many areas covered by governmental programs, from smart mobility to smart building, and even smart cities.

In the field of smart mobility, the benefits are not only economic and safety-related. A significant improvement can also be achieved in environmental sustainability and in the time spent in congested traffic. CAVs (Connected Autonomous Vehicles) and the societal and personal benefits that derive from them in terms of reduced greenhouse gas emissions and time spent in traffic, are a good example. By developing a simulation model and quantifying the impacts of adopting CAVs equipped with V2V (vehicle-to-vehicle) or V2I (vehicle-to-infrastructure) communication systems, we were able to measure benefits against variations in CAV penetration rates throughout Italy. By way of example, in the case of commuters traveling at peak times, a 70% CAV penetration rate can achieve a saving of 63% in time spent in traffic in a V2V scenario, and 34% with V2I systems. In terms of environmental impact, in Milan alone this would lead to a reduction in emissions of approximately 400 t/year CO_2eq with a V2V solution, and around 2,700 t/year in a V2I scenario.

Moving from smart mobility to the smart management of large buildings, benefits can be achieved through the retrofitting of IoT sensors and AI technologies to existing buildings in order to cut energy consumption. Research conducted into the Italian real estate market considered a 4,000 m^2 building in energy class F, divided into eight floors, four with offices (open plan and professional firms) and the other four divided into residential units of various size (85m^2, 120m^2, and 180m^2). The analysis looked at the cost of purchasing, installing and maintaining IoT energy-efficiency devices such as sensors, actuators, and gateways, and calculated the benefits derived. Results showed a 5.2-year PBT (payback time). This falls to under 4 years with the discounts granted by government incentives (especially Ecobonus incentives). PBT is further reduced if building size increases, due to economies of scale, and in the case of lower energy classes (given the higher initial energy consumption).

In the case of a building in class G, PBT would be between 4.4 and 3.9 years depending on floor space (2,000 m^2 vs 8,000 m^2). Finally, shifting the focus of the analysis from economic to environmental benefits, significant results are achieved even in the "basic" case (energy class F, 4,000m^2), with savings of approximately 200,000 kW h/year for the building as a whole.

Still in terms of sustainability, other important environmental and economic benefits can be achieved by installing connected water meters (smart water metering). These range from remote meter monitoring to greater accuracy in billing, fraud detection, and pipe damage/fault identification. Our Observatory quantified economic benefits based on a 10-year timeframe and two roll-out scenarios with 50,000 or 160,000 meters installed across Italy. Net present value varies under the two scenarios, from 4 to 16 million euros, while payback time varies from 4 to 5 years. In terms of environmental benefits, the amount of water and energy saved is significant, with values for the two scenarios ranging from 0.9 to 3.4 million m^3/year of savings in the case of water, and from 14,000 to 44,000 kW h/year in that of electrical energy.

Looking to the future, it is to be expected that the management of large infrastructures will see greater synergy between the IoT, AI and aspects of the space economy, especially satellite technologies for Earth observation. Closer attention is being paid to two commonly used types of instrument: SARs (synthetic aperture radars), and optical or multispectral sensors. Both these technologies allow specific areas of the Earth's surface to be observed and monitored through the collection of data and images. In the first case, the space infrastructure uses radar measurements that remain effective regardless of local weather or lighting conditions, with no distinction between night and day. In the case of satellites that rely on optical or multispectral sensors, local weather or lighting conditions are decisive: this technology is therefore used mainly in the daytime to provide real-colour images that can be interpreted directly.

Numerous economic activities already make intelligent use of satellite applications for infrastructure monitoring. Such technologies are widespread in the world of energy. They are employed to monitor the growth of vegetation around gas and oil pipelines in order to avoid damage to infrastructure, to monitor leaks and tank levels, and even to identify locations for the development of new plants. Wind and photovoltaic applications are also important. In the field of power lines and hydroelectric infrastructure, satellite technologies are also widely used for structural monitoring to prevent network disruption and failures.

6. Cybersecurity and the Protection of Critical Infrastructure: What is at Stake?

Valentin Weber

Securing critical national infrastructure (CNI) has been a daunting challenge for policy makers. CNI embodies a country's most important assets and yet large parts of it are in the hands of the private sector, whose primary aim is to increase profits. This sometimes comes at the expense of stronger cybersecurity. This financial disincentive of stronger cybersecurity measures has led policy makers to increase regulation of the private sector on both sides of the Atlantic, as will be seen later in this chapter.

The US definition of CNI matches the EU's quite closely. US Presidential Policy Directive 21 from 2013, defines 16 CNI sectors, including dams, the defence industrial base, energy, water and waste water, as well as the food and agriculture sector.[1] The European Commission classifies 10 sectors as essential and several more as important entities.[2] Despite the overlaps in designating energy as a CNI, several differences remain. The EU's definition, for instance, does not include the defence industrial base. Meanwhile the US definition of CNI does not explicitly cover the space sector.[3]

* The author would like to thank Julian Heiss for his research assistance.

[1] G. Dunn, "President Biden Signs into Law the Cyber Incident Reporting for Critical Infrastructure Act, Expanding Cyber Reporting Obligations for a Wide Range of Public and Private Entities", 22 March 2022, all links were last accessed on 18 August 2022.

[2] European Commission, "Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities", 16 December 2020.

[3] S. Magnuson, "ANALYSIS: Acknowledging Space Systems as 'Critical

In the US the primary agency in charge of protecting critical infrastructure is the Department of Homeland Security, which takes on the protection of 10 out of 16 sectors.[4] The others are protected by the Department of Defence, the Department of Energy, the Department of Treasury, and so forth.[5] On the European side it is the role of EU Member States to safeguard their critical national infrastructure and to implement the directive. This is laid down in the European Commission's Network Infrastructure Directive (II).[6]

The designation of what is or is not CNI is also crucial in the international diplomatic arena. Designating a critical national infrastructure means that it is covered by the non-binding voluntary norms of responsible state behaviour drawn up under the UN Governmental Group of Experts in 2015 and agreed upon by all countries in the UN Open-Ended Working Group report of 2021.[7] One of the norms stipulates that

> States should not conduct or knowingly support ICT [information and communications technology] activity contrary to their obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.[8]

Infrastructure"', National Defense, 10 May 2022.

[4] J. de Jong-Chen and B. O'Brien, "A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China", Wilson Center, November 2017.

[5] The White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience", February 2013.

[6] European Parliament, The NIS2 Directive, June 2022.

[7] Congressional Research Service, "The Designation of Election Systems as Critical Infrastructure", September 2019; Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, *Final Substantive Report*, March 2021.

[8] Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2021).

To reinforce these norms, President Biden handed over a list of the 16 entities that the US considers to be part of its CNI during his meeting with President Putin in Geneva in June 2021.[9] But how would a malicious actor know that they were targeting CNI that they are not supposed to attack? Currently there is no clear digital signature that would tell attackers that a target is off limits. Precisely such an idea of a digital emblem has been put forward by the International Committee of the Red Cross, which would show states and cybercriminals that a given target is off limits. This would be like the Red Cross label on cars or buildings that indicates that a certain target is protected by international humanitarian law during times of war.[10] However, by designating some infrastructure as taboo, all other targets could be considered fair game, because they are not covered by the norms/emblems.

This introduction has laid out how the US and EU define CNI, as well as who oversees their protection. It has raised some challenges that will be further elaborated in the core of the chapter. The interaction between the public and private sectors is crucial and will be the leading thread of this chapter. The threats section lays out two primary threats to CNI. These are ransomware and the pre-positioning of malware. The ensuing section "Strategies to Counter Risks" gives a high-level overview of the regulatory environment in the US and EU aimed at protecting CNI. The final section of this chapter investigates key challenges that await those protecting CNI – namely (1) a proliferation of Internet of Things (IoT) devices with poor security and (2) the increasingly blurred boundaries between public and private infrastructure.

[9] S. Lyngaas, "Biden Says He Gave Putin List of 16 Sectors That Should Be Off-Limits to Hacking", *CyberScoop*, 16 June 2021.

[10] T. Rodenhäuser et al., "Signaling Legal Protection in a Digitalizing World: A New Era for the Distinctive Emblems?", International Committee of the Red Cross, September 2021.

Threats to CNI

In recent years the main cyber threats to critical national infrastructure have been ransomware and the pre-positioning of malware.

The first threat is emanating primarily from non-state actors. In 2021, out of the top 10 countries targeted by ransomware, 7 were based in North America or Europe.[11] The United States was the most targeted country, France ranked 4th, Italy 5th, Germany 6th and Spain 7th. The US recorded 1,946 ransomware incidents in 2021 alone. Not all attacks were targeted against CNI, but some notable ones were.

The cyberattack on Marquard & Bahls, a German energy and logistics conglomerate that supplies fuel stations in Germany and international customers with fuel, was discovered on 29 January 2022.[12] The attack targeted only the German subsidiaries of the group – Mabanaft (fuel distribution) and Oiltanking Deutschland GmbH (fuel storage). Both companies declared force majeure as a result, which frees the two companies from obligations toward its customers, such as fulfilling contractual obligations, or paying compensation for damages.[13] The on- and off-loading of fuel stocks was affected in particular as these are largely automated and a manual process is only possible in a limited way.[14] As the ecosystem supplying Germany with fuel involves 26 companies, there was no immediate danger to larger shortfalls in overall supply. The President of the German Federal Foreign Office for Information Security, Arne Schönbohm, mentioned that only 233 fuel stations were

[11] Institute for SECURITY + TECHNOLOGY, "RTF Year Two: New Map; New Data: Same Mission", July 2022.

[12] J. Karabus, "Cyberattacker Hits German Service Station Petrol Terminal Provider", *The Register*, February 2022; Mabanft, "Statement From Oiltanking Gmbh Group and Mabanaft Gmbh & Co. KG Group", January 2022.

[13] C. Scholz, "Wann bei Cyberangriffen höhere Gewalt gilt", *Handelsblatt*, 14 February 2022.

[14] "Cyberangriff auf Zulieferer von Tankstellen in Deutschland", *Der Spiegel*, 31 January 2022.

affected, which translates into 1.7% of all fuel stations in Germany.[15] Nevertheless, even by mid-February Mabanaft had still not managed to restore operations, showing the severity of the disruption.[16] The Black Cat ransomware group is assumed to have conducted the attack.[17] Black Cat is also suspected to be related to the DarkSide ransomware group, which is linked with a major attack on the Colonial Pipeline Co.[18]

On 7 May 2021 Colonial Pipeline Co., headquartered in Alpharetta, Georgia, declared that it was the target of a ransomware attack. This led it to shut down its operations for several days, causing price hikes and runs on fuel stations.[19] Luckily operations were resumed within the week and the disruption did not cause any shortages in fuel supply. Nevertheless, the panic amplified by media reporting had its effects, which led a former CISA employee to declare that "It's more likely that fuel shortages will be a result of panic buying from consumers watching the headlines unfold, as opposed to shortages directly caused by the attack".[20]

In short, when mitigating the effects of cyberattacks, the messaging regarding attacks on CNI is often just as important as the attack itself. During a previous cyberattack on Ukrainian critical infrastructure, Russian malicious actors overwhelmed customer hotlines of the affected Ukrainian energy company. This increased the effects of the cyberattack, since it created uncertainty and fear among the Ukrainian population.[21] If one

[15] D. Knop, "Cyber-Angriff legt Logistikunternehmen Oiltanking lahm", *heise online*, 1 February 2022.

[16] R. Graham, "Germany's Mabanaft Says First Test After Hack Wasn't Successful", Bloomberg, 13 February 2022.

[17] "Staatsanwaltschaft ermittelt nach Cyberangriff auf Ölhändler", *WELT*, 2 February 2022.

[18] R. Gallagher, "Ransomware Attack in Germany Tied to Colonial Pipeline Hackers", Bloomberg, 3 February 2022.

[19] S. Morrison, "How a major oil pipeline got held for ransom", *Vox*, 8 June 2021.

[20] Ibid.

[21] J. Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks", *MIT Technology Review*, 22 December 2016.

goes a step further in this line of thinking, CNI does not even have to be disrupted. The mere belief that malicious actors have compromised financial institutions or a water facility may cause a run on banks or for people not to drink the water in a city and therefore stockpile plastic bottles.

The Colonial Pipeline attack showed that it takes as little as a well carried out ransomware attack to destabilise an entire country. The pipeline operator seems not to have had basic security measures in place, such as multifactor authentication for a virtual private network or a clear separation between its operational technology and data management.[22] What is more, Colonial Pipeline had not prepared sufficiently for a manual restart after incidents. This weakness and non-compliance with federal safety regulations had already been found during an investigation in 2020. Because it had not fixed these weaknesses the Department of Transportation's Pipeline and Hazardous Materials Safety Administration proposed a fine of $1 million in the aftermath of the incident.[23]

The second major threat to CNI has been quieter and concerns the prepositioning of malware, or "preparing the ground" as it is called in national security circles. The goal of this type of cyber operation is to get access to critical national infrastructure and to position malware in foreign infrastructure long before a real conflict arises. Countries such as Russia and China pose a threat to European and American infrastructure and could therefore dissuade countries across the Atlantic from taking action in times of crises, since they would perceive that their CNI is under threat. The most recent such incident was PIPEDREAM, a malware that specifically targets industrial control systems and was discovered in US networks in

[22] D. Sanger and N. Perlroth, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity", *The New York Times*, 14 May 2021; S. Kelly and J. Resnick-Ault, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators", *Reuters*, 9 June 2021.

[23] E. Kovacs, "Regulator Proposes $1 Million Fine for Colonial Pipeline One Year After Cyberattack", *Security Week*, 9 May 2022.

2022.[24] It is an attack framework that targeted the industrial control programmable logic controllers of Omron (a Japanese electronics manufacturer) and Schneider Electronics (a French digital automation and energy management company).[25] If it had not been discovered and mitigated against in time, the malware could have caused disruption, degradation or even destruction.

Strategies To Counter Risks

There are numerous acts and laws on both sides of the Atlantic pertaining to the cybersecurity of CNI. The aim of the paragraphs below is not to provide a comprehensive overview of all regulations, as this would be beyond the scope of this chapter, but merely to highlight the most important pieces of the regulatory environment that assist the overall analysis of this chapter.

European Union

One of the primary strategies in the European Union to protect critical infrastructure has been regulation created with private sector input. A core element of EU regulation is certification. With the adoption of the EU Cybersecurity Act, the European Union Agency for Cybersecurity (ENISA) was positioned as the primary agency responsible for building and maintaining the cybersecurity certification framework.[26] The NIS II Directive [Network and Information Security], for instance, stipulates that certain critical entities must use certified ICT products. As the document simultaneously increases the number of critical entities, this becomes a challenge for Member States and

[24] Ars Technica, "Making Critical Infrastructure Safer", 31 May 2022.
[25] Dragos, Inc., *CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)*, 13 April 2022.
[26] EU DG CONNECT, *The EU Cybersecurity Act*, June 2022.

companies to implement, due to a lack of human resources.[27] CNI operators in the EU also need to report significant incidents within 24 hours and provide an initial assessment of the incident within 72 hours.[28] If a critical entity has been non-compliant, the competent authorities can temporarily relieve the chief executive officer of such an entity from their duties or impose penalty payments of up to €10,000 or 2% of the total worldwide annual turnover. Oddly enough, national parliaments, ministries, central banks, law enforcement and the judiciary are exempt from NIS II, which leaves the EU and its Member States vulnerable.[29] However, recent regulations specify that EU institutions and their delegations abroad must conduct a mandatory cyber risk assessment of their assets and the threats they are exposed to. They also must adhere to minimum cybersecurity standards. These requirements come with no penalties, meaning that implementation morale may be low. These measures likely apply to the COREU network, too, which is used by various EU entities and Member States to allow for secure intra-EU communications. The EU's recent cyber posture also recognises the need for secure communications of such important entities.[30] Considering that the COREU network was hacked in 2018, it is crucial for cybersecurity to be increased in this network environment.[31]

---

[27] T. Sievers, "Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations", *International Cybersecurity Law Review,* 2.2, 2021, pp. 223-31.

[28] Council of the European Union, Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148, June 2022.

[29] J. L. Hardcastle, "Europe Moves Closer to Stricter Cybersecurity Standards, Reporting Regs", *The Register*, 17 May 2022.

[30] Council of the European Union, *Council Conclusions on the Development of the European Union's Cyber Posture*, May 2022.

[31] C. Osborne, "Chinese Hackers Tap Into EU Diplomatic Communications Network", *ZDNET*, 19 December 2018.

United States

Rather than relying on mandatory regulations and obligations, the US has relied very much on issuing voluntary measures to private entities to protect its critical infrastructure. The National Institute of Standards and Technology (NIST) was tasked with compiling a framework to reduce the risk to critical infrastructure entities, with an update being issued in 2018.[32] The purpose of the NIST framework is different from the EU's NIS directive. The former was specifically designed as a set of voluntary standards and best practices aimed at attracting a global following beyond the regulatory environment where it was created. In this vein, the framework was translated into Japanese, Spanish, Hebrew, Portuguese and Arabic.[33] Parts of it were adapted in Israel, Italy and Uruguay.

When it comes to the reporting of critical infrastructure incidents the US is also laxer in its rulebook than the EU, especially in sectors such as information technology.[34] Owners and operators of CNI must report certain cyber incidents within 72 hours and report ransomware payments within 24 hours.[35] However, enforcement appears to be weak as no specific penalties are laid down in the H.R.2471 – Consolidated Appropriation Act, 2022.[36] In the case of non-compliance the CISA director may issue a subpoena. If a company still does not budge, the issue is transferred to the Department of Justice (DoJ) for enforcement.[37]

---

[32] Cybersecurity and Infrastructure Security Agency, "Using the Cybersecurity Framework", n.d.; National Institute of Standards and Technology, "Updating the NIST Cybersecurity Framework – Journey to CSF 2.0", May 2022.

[33] National Institute of Standards and Technology NIST (US Department of Commerce), Cybersecurity Framework – International Resources.

[34] B.E. Humphreys, "The designation of election systems as critical infrastructure", Congressional Research Service, 2019.

[35] Dunn (2022).

[36] US Congress, H.R.2471 - Consolidated Appropriations Act, 2022.

[37] Dunn (2022).

While the US is quite lax in its regulatory environment, compared to the EU, the US is more at ease with using coercive tools to strike back against criminals. This became apparent during the Colonial Pipeline attack. The company had paid a ransom of $4.4 million to a criminal gang.[38] In the aftermath of the attack the DoJ recovered a large portion of bitcoins paid to criminals.[39] In order to do this the DoJ had to obtain the private keys/passwords to access the funds. How it obtained them is unknown to the public, but it may have involved more intrusive techniques. US Cyber Command too has been more aggressive than its European counterparts. The head of Cyber Command stated that his agency conducted cyber operations against cyber criminals to "impose costs".[40] Cyber Command and the National Security Agency also helped the DoJ to recover the Colonial Pipeline ransom. While the immediate gains for the US and costs to cybercrime groups are visible, the medium- and long-term benefits are fuzzier. Cybercriminals are known to rebrand and reappear under a new flag, which makes the post-incident operations more a game of whac-a-mole than a sustainable strategy that would prevent such attacks in the future.[41]

The US is more stringent in the case of federal networks. The presidential Executive Order on Improving the Nation's Cybersecurity, issued in 2021 after the SolarWinds and Colonial Pipeline attacks, obliges federal agencies to implement encryption of data at rest and in transit, as well as multifactor authentication.[42] It also aims to raise private sector cybersecurity levels by requiring suppliers of federal

[38] "The Hackers Who Took Down the Colonial Pipeline", *Slate*, 18 August 2022.
[39] Department of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, 7 June 2021.
[40] J. Barnes, "U.S. Military Has Acted Against Ransomware Groups, General Acknowledges", *The New York Times*, December 2021.
[41] E. Nakashima, "U.S. government denies disrupting Russian ransomware ring that hacked Colonial Pipeline", *The Washington Post*, May 2021.
[42] The White House, "Executive Order on Improving the Nation's Cybersecurity", 12 May 2021.

networks to provide visibility into their software and security data (logging, log retention, log management) for quicker investigation and remediation of incidents.[43] In the words of the White House, "We need to use the purchasing power of the Federal Government to drive the market to build security into all software from the ground up".[44]

The Challenges Ahead for the Protection of CNI

The current attention of the regulators in the US and EU is primarily aimed at improving large and essential infrastructure operators. However, the notion of critical national infrastructure is constantly evolving. One of the recent examples of new entities being added to CNI is the US election infrastructure that the US Department of Homeland Security declared a CNI in 2017.[45] Similarly the notion of CNI will expand in the coming years and decades. This is due to one main factor: the massive proliferation of smart devices across various industries and among citizens.

A case in point is the vast number of smart thermometers that are being installed in homes across Europe and the US. These help to smartly regulate the temperature in homes to save energy. Researchers from Cornell University demonstrated how coordinated thermostat action that is entirely benevolent can already cause strain on the grid.[46] Malicious activity could amplify such pressures. In short, the rise of IoT devices creates new problems for operators of CNI and challenges for policy makers. Making sure that the devices scattered across homes are secure is crucial to national security.

---

[43] Ibid.

[44] The White House, "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks", 12 May 2021.

[45] Humphreys (2019).

[46] B. Friedlander, "Smart Thermostats Inadvertently Strain Electric Power Grids", *Cornell Chronicle*, 12 July 2022.

And even more so, securing IoT devices that are deployed directly *within* CNI will be crucial. One of the major challenges for keeping CNI secure has been the rise of IoT devices. Every second 127 new IoT devices are connected to the internet.[47] They are difficult to patch and often receive and transmit unencrypted data.[48] Due to their long lifespan vendors also do not have the incentive to provide patches over such long time periods. In the healthcare sector IoT risks are especially visible. In 2019, for instance, vulnerabilities in anaesthesia devices would have allowed malicious actors to manipulate the mix of inhaled gases or silence alarms issued by the device.[49]

The EU has taken on the issue of IoT security through its Cyber Resilience Act, which aims to create new cybersecurity rules for vendors and manufacturers.[50] The Act will be published in Q3 2022. The US, for its part, passed the Internet of Things Cybersecurity Improvement Act of 2020, which specifies that NIST and the Office of Management and Budget oversee the improvement of the cybersecurity of IoT devices in federal networks. Here again the US law is laxer than the EU's, as its measures are confined to IoT devices controlled or owned by the federal government. The law requires the devices bought by the federal government to meet NIST standards. If the standards are not met, a contract should not be awarded. In the view of US lawmakers, regulating the private sector more broadly could slow down innovation.[51] Conversely, the US believes that the high standards for government IoT use will trickle down

[47] McKinsey & Company, *What's new with the Internet of Things?*, 10 May 2017.
[48] X. Zou, "IoT Devices Are Hard to Patch: Here's Why - and How to Deal With Security", TechBeacon, n.d.
[49] Cybersecurity and Infrastructure Security Agency, "ICS Medical Advisory (ICSMA-19-190-01) – GE Aestiva and Aespire Anesthesia (Update A)", July 2019.
[50] European Commission, "Cyber Resilience Act – New Cybersecurity Rules for Digital Products and Ancillary Services", n.d.
[51] Thales, "IoT Cybersecurity: Regulating the Internet of Things", June 2021.

to consumer devices.[52] In contrast, the EU's act applies to the market more broadly.[53]

This chapter was not aimed at giving a comprehensive overview of all legislation or regulations covering CNI in the US and EU. Nor was it meant to provide an all-encompassing enumeration of threats to CNI. Rather than taking such a broad view of CNI, this chapter presents the most daunting threats, as well as strategies to meet those threats.

Future research could look further into the cybersecurity challenges arising from large-scale, complex IoT systems, such as smart cities.[54] Cyberattacks disrupting one city may easily affect neighbouring cities, making close cooperation between cities necessary. Another challenge in securing large urban environments is that cities, especially in federally structured countries such as the US or Germany, are often not directly affected by federal-level decisions. Cities are free to choose the supplier they believe fits them best, even if it might pose considerable cybersecurity risks. Finally, researchers could focus on how specific private sector entities, such as the insurance industry, cope with state-backed cyber operations and what challenges this creates for policy makers. Lloyd's, an insurance and reinsurance market, for instance, recently declared that private entities should not cover catastrophic state-backed cyberattacks that affect a country's infrastructure even outside of a war.[55] These new standards set by the private sector raise new definitional challenges, such as what counts as a state-backed cyber operation? And at what point does the state become the ultimate reinsurer?

---

[52] D. George, "New Federal Law Alert: The Internet of Things (IoT) Cybersecurity Improvement Act of 2020 – IoT Security for Federal Government-Owned Devices", *National Law Review*, 10 December 2020.

[53] U.S. Congress, "H.R.1668 - IoT Cybersecurity Improvement Act of 2020", 2020.

[54] V. Weber, "What If Smart Cities Encouraged Stupid Risks?", DGAP Memo No. 1, 13 April 2022.

[55] Lloyd's, *Market Bulletin*, 16 August, 2022.

PART II
SECTORS

7. Smart Roads and Transport Infrastructure

George Yannis, Apostolos Ziakopoulos

7.1. The Way Towards Smart, Green and Efficient Road Transport

In recent years, rapid technological advances in computer science, machine learning and similar quantitative disciplines have led to considerable breakthroughs in communications, sensors and systems, as well as improvements towards the development of more independent Artificial Intelligence (AI). Meanwhile, wide-scale data collection and utilization have been enabled in virtually all technical fields, and the world has become increasingly connected through the Internet of Things (IoT). The transport sector has been in a process of gradual transformation as a result; for instance, driverless and fully autonomous/automated vehicles (AVs) are a major expected development stemming from these advances, but by no means the only one.

As road transport infrastructure will remain a critical component of the transport system, it will inevitably be affected by these developments and its transformation will in turn open new capabilities for road transport systems. Already, a change in scope is being observed for road infrastructure elements, alongside a different philosophy for their management. The rigidity of infrastructure elements is recognised as unfeasible

in the long term, as more uncertainties emerge, frequently in tandem with crises requiring fast interventions.[1] While roads used to be considered as elements mainly providing access and bearing loads for the safe movement of vehicles, they are now examined as means of communication and information exchange, and even energy sources in parallel with their legacy functions.[2]

This prompts the question: what options are there to harness these technological advancements in order to achieve smarter, safer, greener, more efficient and more resilient transport? This paper discusses a variety of technologies and interventions, alongside their potential impacts. It also looks at the barriers to achieving these goals, before drawing appropriate conclusions.

Smart Roads and Adaptive Infrastructure

Under the umbrella of "smart" technological developments, an array of different approaches has become available for road monitoring and improvement. Smart systems are typically dynamic, adaptable and at least partially automated, in the sense that they require little manual intervention to yield their designed output or service. Several of these ideas are largely attainable today and have been implemented in prototypes or pilot studies. They therefore constitute possible starting points from which to transition to smart roads and cities.

Indicatively, smart lighting is an attainable feature of smart roads. By adapting to transport demand, as perceived by the respective sensors, the lighting network can provide targeted illumination when, whereand to the extent that it is needed.[3]

---

[1] E.J. Gilrein et al., "Concepts and practices for transforming infrastructure from rigid to adaptable", *Sustainable and Resilient Infrastructure*, vol. 6, no. 3-4, 2021, pp. 213-34.

[2] E.g. S. Trubia, A. Severino, S. Curto, F. Arena, and G. Pau, "Smart roads: An overview of what future mobility will look like", *Infrastructures*, vol. 5, no. 12, 2020, p. 107.

[3] E.g. G. Gagliardi et al., "Advanced adaptive street lighting systems for smart

This is not only an efficient and energy-saving practice; it allows more harmonious coexistence with flora, fauna and natural human needs, while maintaining safety and quality of life in cities.[4] Furthermore, street lights can offer safe, well-dispersed hosting locations for more sensors, thus improving data collection overall and opening further venues for connectivity applications. For example, security can also be promoted by enabling sensors to detect incidents such as gunshots and allow fast law enforcement response.[5]

AI-based research can yield tools for road maintenance support, such as pothole detection capabilities from user-uploaded images of the area concerned[6] or from social media web scraping.[7] Such approaches can greatly reduce the required workload by city authorities and enable wider coverage of proper infrastructure maintenance through crowdsourcing, thereby reducing neglected areas and the corresponding inequality in fixing network problems.

In addition, extensive research efforts have been dedicated to smart intersections and traffic sign/signal optimisation. These technologies typically include algorithms that operate in real-time or almost-real-time conditions, with the aim of minimising multiple transport indicators such as travel delays, emissions, queue lengths, or similar criteria. Connected vehicle technology of otherwise still human-driven vehicles has improved data collection and reduced transmission times, allowing these schemes to be more refined, although many are

---

cities", *Smart Cities*, vol. 3, no. 4, 2020, pp. 1495-1512.

[4] M. Palmer and R. Gibbons, *Smart lighting for smart cities. In Solving Urban Infrastructure Problems Using Smart City Technologies*, Elsevier, 2021, pp. 485-99.

[5] E.g. M. Scott, "Using streetlights to strengthen cities", Data-Smart City Solutions, 22 August 2016; Gilrein et al. (2021).

[6] V. Bhalla, "SpotholeAI-An Artificial Intelligence (AI) assistant to fix Potholes", The 36th International Conference on Machine Learning (ICML 2019), AI for Social Good Workshop, California, 2019.

[7] S. Agarwal, N. Mittal, and A. Sureka, "Potholes and bad road conditions: Mining Twitter to extract information on killer roads", ACM India Joint International Conference on Data Science and Management of Data, 2018, pp. 67-77.

targeted at fully automated vehicles instead. Some examples include reinforcement-learning algorithms that can account for incidents such as traffic flow incidents, pedestrian jaywalking, and sensor noise, whilst reducing delay times[8] or minimising vehicular emissions alongside delay time by connecting the former to the latter through traffic occupancy in a road segment.[9]

Smart Motorways

Primarily within the UK, Smart Motorways (SMs), as an infrastructure category, comprise three proposed designs that differ from the conventional type. In short, these are **(i)** Controlled Motorways (CM), which add variable and mandatory speed limits to a conventional motorway to control the speed of traffic, while retaining a permanent hard shoulder **(ii)** All Lane Running (ALR) motorways, which apply controlled motorway technology, permanently convert the hard shoulder into a running lane, and feature emergency areas and **(iii)** Dynamic Hard Shoulder Running (DHS) motorways, which apply controlled motorway technology, while sometimes using the hard shoulder as a running lane. SMs are estimated to increase the capacity of busy motorways by up to a third when replacing their conventional counterparts.[10]

---

[8] M. Aslani, S. Seipel, M.S. Mesgari, and M. Wiering, "Traffic signal optimization through discrete and continuous reinforcement learning with robustness analysis in downtown Tehran", *Advanced Engineering Informatics*, vol. 38, 2018, pp. 639-55.
[9] K. Han, H. Liu, V.V. Gayah, T.L. Friesz, and T. Yao, "A robust optimization approach for dynamic traffic signal control with emission considerations. Transportation Research Part C", *Emerging Technologies*, vol. 70, 2016, pp. 3-26.
[10] UK Department for Transport (DfT), Smart Motorway Safety: Evidence Stocktake and Action Plan, 2020.

At present, in the UK alone, SMs cover 488 miles of motorways, with plans to extend the SM network by an additional 300 miles without hard shoulders by 2025.[11] SMs feature mandatory speed control, automatic signal setting in response to traffic conditions and speed enforcement using automatic camera technology. They are managed by Regional Control Centres (RCCs), which can rapidly deploy traffic officers in response to road incidents.[12] SMs have been reported to increase journey reliability by up to 22%.[13] Moreover, SMs appear to reduce environmental impacts, such as global warming potential, especially during the road safety barrier maintenance phase. Gains in environmental impacts are expected to upscale as the annual average daily traffic (AADT) and the platooning percentage of vehicles increases,[14] which are likely future outcomes, thus enhancing the sustainability of SMs.

Despite the aforementioned expected benefits and interconnectivity advantages, SMs have not been without controversy. Drivers have expressed concerns over the absence of hard shoulder coverage, as well as the scarceness and small size of Emergency Refuge Areas (ERAs). Close examination of crash data from the years 2015-18 reveals that road safety levels have not improved uniformly. Specifically, during 2015, 2016 and 2018, SMs were found to perform better than conventional motorways, while in 2017 they saw a higher number of fatalities. Following these concerns, the UK DfT has placed any future SM development on hold while a detailed review is undertaken.[15]

---

[11] Royal Automobile Club (RAC), "Which motorways are smart motorways, and where will new ones be?".

[12] Highways England, *Smart Motorways Programme Environmental Assessment Report*, 2019.

[13] The Royal Society for the Prevention of Accidents (ROSPA), *Road Safety Factsheet – Smart Motorways*, 2021.

[14] M. Guerrieri, B.M.L. Casto, G. Peri, and G. Rizzo, "Smart vs conventional motorways: Environmental impact assessment under realistic traffic conditions", *Science of the Total Environment*, vol. 727, 2020, 138521.

[15] UK Department of Transport (DfT) (2020).

Beyond the United Kingdom, smart motorways are increasingly gaining ground in the European Union. The European Commission, in fact, has developed a strategy to provide European roads with a common infrastructure for smart safety, through the Cooperative Intelligent Transport System (C-ITS). Within this project, C-Roads is a joint initiative that includes most EU Member States and their roads operators (Austria, Belgium, Czechia, Denmark, Finland, France, Germany, Hungary, Italy, the Netherlands, Portugal, Slovenia, Spain, and Sweden), plus the UK and Norway, and is aimed at deploying SMs throughout Europe. Austria has been at the forefront, with tenders launched in 2018 after a study phase and smart roads featuring prominently in the Austrian Road Safety Strategy 2021-30.[16] Italy has followed suit, running a series of technical tests since 2017 on the A22 motorway, which links the country with Germany and Austria, and is a crucial artery for Italian exports. The aim is to develop a system of self-driving trucks in digital connection with the road, by transferring data in real-time on direction, speed and external conditions.[17] Italy is also involved in a similar project on the Salerno-Reggio Calabria motorway, in the southernmost part of the peninsula. The project involves developing a set of smart infrastructures that would provide information and guidance to autonomous vehicles, as well as feature EV charging stations entirely powered by green energy through photovoltaic panels.[18] Finally, in June 2022 the automaker group Stellantis created a circular test track with embedded inductive charging, under the name Arena del Futuro (Italian for Arena of the Future). It was built as part of the A35 Bre-Be-Mi motorway, which

[16] Austrian Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK), "Austrian Road Safety Strategy 2021-2030", 2021.

[17] M. Borsari, "Smart roads to Revolutionize travel", *Warp News*, 24 December 2021.

[18] E. Punsalang, "Salerno-Reggio Calabria In Italy Set To Be Europe's Longest Smart Road", *Ride Apart*, 2022.

links the major Italian cities of Brescia, Bergamo and Milan. The outer lane of the circle is equipped with an embedded Dynamic Wireless Power Transfer (DWPT) system, which enables vehicles such as the electric Fiat 500 used as a test car to drive at highway speeds without actually draining its battery.[19] In addition, widely circulated polls suggest that 25% of drivers have no knowledge of what SMs are and an additional 27% of drivers did not know the rules of driving on an SM, meaning that less than half of drivers are ready to navigate in the growing SM network.[20] This is an absence of critical knowledge, as the safety of any road users and vehicles which are stopped in a running lane depends on correct interpretation of SM signage by drivers. There appears to be uncertainty both in expert knowledge of SM impacts and in public acceptance of SMs.

Systems and Interventions Relating to Automated Vehicles

AI-piloted automated technologies will be adopted on a wide scale in the coming decades, with profound consequences, such as the aforementioned advent of Avs. Several smart infrastructure interventions can be expected to be added to the arsenal of stakeholders when AV technologies reach sufficient penetration levels, especially when connected Avs (CAVs) are seamlessly linked with each other and with smart infrastructure with vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technologies (known as V2X collectively).

In EU countries, a number of C-ITS have been introduced and operate in several pilot trials for participant countries. C-ITS focuses heavily on V2X connectivity and data exchange. At present, such interventions focus on providing support to drivers based on their location, while in the future they are

[19] A. Nedelea, "This Fiat 500 EV Is Charging Wirelessly Through the Road As It Drives", *InsideEvs*, 11 March 2022.

[20] Green Flag & Brake Reports on Safe Driving, *Motorway driving*, 2020.

expected to play a pivotal role in AV integration in transport systems. In several pilot trials within C-Roads, C-ITS have been employed with ETSI ITS-G5 short-range communication technology, which is very similar to WiFi routers. As of 2020, in 18 countries and 7 associated countries more than 100,000 km of motorway are supported in such a manner.[21] It is worth noting that C-Roads and C-ITS have "day-1" potential, meaning that they are readily available to support IAV deployment from the very start. Such systems have the option of serving as an additional layer and source of perception for AV sensors, providing much-needed backup in the event that vehicles become non-operational due to mechanical failure, adverse weather, operational design domain (ODD) exceedance etc., thus increasing the traffic safety of future Avs. Similar developments are happening outside Europe, in the US, Asia and Australia, though fully independent automated vehicles (i.e. SAE level 5 as described in SAE International, 2016) are not yet completely supported.[22]

Accordingly, a multitude of impacts will emerge in the affected transport systems, either from general-traffic AV adoption or from dedicated policy implementations and interventions relevant to Avs. Following Elvik et al. (2019),[23] these impacts can be classified as:

1. Direct impacts: changes that are noticed by every road user on every trip (e.g. travel time).
2. Systemic impacts: changes in transport system boundaries (e.g. modal split).
3. Wider impacts: changes exceeding transport system boundaries (e.g. road fatalities and injuries, emissions).

[21] C-Roads, *Annual pilot overview report 2020*, 26 June 2021; C-Roads, *The C-Roads Platform – An overview of harmonised C-ITS deployment in Europe*, 2020.

[22] SAE International, Standard J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (revised J3016: Sept 2016).

[23] Following R. Elvik, et al., "A taxonomy of potential impacts of connected and automated vehicles at different levels of implementation", Deliverable D3.1, 2019.

It is imperative to anticipate the advent of automation and to analyse and forecast the impacts of automation-based policies proactively. Within the European LEVITATE project, several AV-related infrastructure interventions have been examined. Using a combination of microscopic and mesoscopic simulation, system dynamics, operations research and Delphi questionnaires, a number of anticipated impacts have been assessed.[24] Specifically, the following effects were outlined by Gebhard et al. (2022)[25] for infrastructure interventions, among others:

- Dedicated AV lanes, which according to the Connected Automated Driving Roadmap of ERTRAC (2019),[26] are lanes which only allow vehicle(s) with specific automation level(s) to travel. Conversely, Avs would not necessarily be confined to the dedicated lane. In such cases, this would instead be referred to as a physically separated lane. It is envisaged that where a dedicated public transport lane is in operation, the dedicated AV lane would be shared with the dedicated public transport lane, allowing both types of vehicles (as is the case with current High Occupancy Vehicle (HOV) lanes). Such a dedicated lane may be fixed (dedicated to CAVs at all times), or may be dynamically controlled to vary based according to the traffic situation. Overall, dedicated CAV lanes were predicted to have limited additional impacts on most indicators. Slight benefits were estimated for congestion, vehicle operating costs, vehicle utilisation and occupancy rates, as well as public health.
- On-street parking is the most common option for both paid and unpaid parking along roadsides in urban

[24] A. Ziakopoulos et al., Integration of outputs of WP4-7, Deliverable D8.1 of the H2020 project LEVITATE, 2022.

[25] S. Gebhard et al., Guidelines and recommendations for future policy of cooperative and automated passenger cars, Deliverable D6.5 of the H2020 project LEVITATE, 2022.

[26] ERTRAC Roadmaps, Connected Automated Driving Roadmap, 2019.

cities.[27] While it can contribute to the economy as a form of commercial exploitation of parking space, it can have negative impacts such as congestion, capacity reduction and increases in road traffic accidents. Theoretically, the introduction of autonomous vehicles offers the potential to reduce urban space requirements for roads and parking, as automated vehicles are able to park elsewhere after dropping passengers off at the destination. This gives rise to new opportunities to create more space for high-quality, liveable areas.[28] Replacing on-street parking is associated with a wide range of positive benefits, including large improvements in traffic conditions (reduced travel time and congestion), increased active mode shares, more shared mobility, better development of road safety and reduced demand for parking space. Several impacts are based on the facilities chosen as substitutes for parking space: replacement with public space is particularly associated with societal and environmental benefits (e.g. road safety, public health, energy efficiency) and can be beneficial for shared, public, and active forms of mobility. Conversely, replacement with driving lanes or pick-up/drop-off points is associated with fewer benefits, except for improved access to travel. Pick-up/drop-off points or removing only half of the available spaces also reduces the benefits to congestion due to some of the parking manoeuvres.

- Green Light Optimal Speed Advisory (GLOSA) is a traffic signal application at signalised intersections that

[27] S. Biswas, S. Chandra, and I. Ghosh, "Effects of on-street parking in urban context: A critical review", *Transportation in developing economies*, vol. 3, no. 1, 2017, pp. 1-14.

[28] E. González-González, S. Nogués, and D. Stead, "Parking futures: Preparing European cities for the advent of automated vehicles", *Land Use Policy*, vol. 91, 2020, p. 104010; E. González-González, S. Nogués, and D. Stead, "Automated vehicles and the city of tomorrow: A backcasting approach", *Cities*, vol. 94, 2019, pp. 153-60.

> can be readily available for implementation – a "day-1" measure as noted by Mellegård & Reichenberg (2020).[29] GLOSA utilises traffic signal information and the current position of a vehicle to provide speed recommendations formulated to help drivers reach traffic lights during the green phase, thus reducing the number of stops, fuel consumption and emissions. Stopping distance, signal timing plans and area speed limit profiles are taken into account to calculate the speed recommendation displayed to drivers. The GLOSA service can also be provided to the on-board computer of a connected AV or to a smartphone application. GLOSA is not predicted to have major impacts on most indicators. Slight benefits to traffic conditions are predicted (reduced congestion and travel time), as well as halt reductions in public transport use and reduced vehicle operating costs. Potential negative effects on shared mobility rate, active travel, vehicle utilisation and occupancy rates, access to travel and public health are predicted. These negative effects may be due to a predicted increase in private vehicle travel with the implementation of GLOSA.

Road-use pricing refers to charges for the use of infrastructure, including distance- and time-based fees, road tolls and various charges aimed at discouraging drivers from accessing or remaining in specified areas with their vehicles for long periods. Road-use pricing is expected to increase energy efficiency, halt reductions in public and active transport mode sharing, increase vehicle occupancy rates, and reduce parking demand. On the negative side, road-use pricing is expected to lead to an increase in vehicle operating costs, and lower accessibility to transport overall. While arguably more relevant to transport

[29] N. Mellegård and F. Reichenberg, "The Day 1 C-ITS Application Green Light Optimal Speed Advisory – A Mapping Study, *Transportation Research Procedia*, vol. 49, 2020, pp. 170-82.

policy than to transport infrastructure, smart infrastructure can nonetheless enable fairer, more precise and easier-to-manage road-use pricing calculations.

Discussion and Pending Issues

Naturally, there are several barriers and limitations to the implementation of smart infrastructure solutions. Several of these schemes are largely dependent on data usage, and as such can frequently require liberal data sharing.[30] Conversely, limitations in open data flows can hinder the effectiveness, affordability and feasibility of smart infrastructure and road transformation schemes. A specific example is the "silo effect" that occurs if different commercial data owners and providers are unwilling to share data due to privacy, legal liability, intellectual property, competition, interoperability, cybersecurity or cost-related issues.

Overall, it is reasonable to anticipate more innovative smart road solutions as time progresses; their standardisation and exploitation of possible interactions and synergies are challenges that will have to be tackled subsequently. Of course, systemic resilience has to be a constant consideration. As smooth operation of all smart and connected schemes is related to centralisation of information, sufficient backups and redundancies must be in place against both equipment failures and malicious attacks (i.e. cybersecurity). A closely related issue is the timelesness of smart infrastructure systems. Algorithms will continue improving, but there needs to be a minimum common ground, in the form of stable systems, in order to ensure resilience and to provide a basis for lateral synergy exploitation. Certain regulatory processes can be imposed here by supervisory authorities. Rather than restricting smart solutions, these should be aimed

[30] SuM4All (Sustainable Mobility for All), *Sustainable Mobility: Policy Making for Data Sharing*, Washington DC, License, Creative Commons Attribution CC BY 3.0, GRA in action series, 2021.

primarily at enabling cooperation and embedding of systems and accomodating further advances, so as to create a "future proof" smart road infrastructure.

Policymakers will have to develop digital skills themselves, while cooperating with computer science experts and digital specialists. This is a crucial necessity because problems are becoming too complex, composite and multifaceted to tackle alone. Challenges such as the scalability of smart road solutions need to be addressed to ensure the smooth installation of more reliable infrastructure and smart cities as uniformly as possible. Moreover, concerted efforts are required to increase the fairness and openness of AI systems,[31] and reduce systemic inequalities in transport, exploitative contracting, gentrification effects, societal and accessibility issues and so on – after all, decision-making cannot be solely left with automated black-box processes, especially since fairness may be defined differently for each discipline.[32]

The multidimensionality of the smart road transition is evident as cities have been endeavoring to align with United Nations sustainable development goals.[33] This multidimensionality must obviously include cost-benefit analysis and prioritisation of each element and the overall economic feasibility of transport systems as a whole, together with the required legal frameworks defining the role of each actor in the system, be they supervisory authorities, road infrastructure operators and managers, road users or other stakeholders.

---

[31] E.g. P. Hacker, "Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things", *International data privacy law*, vol. 7, no. 4, 2017, pp. 266-86.

[32] J. Finocchiaro, "Bridging machine learning and mechanism design towards algorithmic fairness", ACM Conference on Fairness, Accountability, and Transparency, March 2021, pp. 489-503.

[33] A.A. Kutty, G.M. Abdella, M. Kucukvar, N.C. Onat, and M. Bulu, "A system thinking approach for harmonizing smart and sustainable city initiatives with United Nations sustainable development goals", *Sustainable Development*, vol. 28, no. 5, 2020, pp. 1347-65.

Conclusion

This section offers a selective examination of several advancements in smart infrastructure, which could prompt the transformation of road networks to become smarter, safer, greener, more efficientand more resilient. An array of innovative solutions exist today that are readily implementable and could lead to reductions in emissions, delay times, energy consumption and other key indicators, while maintaining or even improving safety levels overall. These interventions could take the form of smart lighting or maintenance systems, schemes for data collection through sensors, or traffic signal optimisation. Several IAV-related infrastructure interventions have been outlined as well, which will become deployable as connectivity and automation penetration rates increase. There are numerous barriers to the transition to smart roads and adaptive infrastructure. Broadly speaking, these relate to **(i)** data flow and sharing, **(ii)** transport system robustness, timelessness and scalability and **(iii)** AI fairness and equality. New challenges are largely expected to be multifaceted and multidisciplinary, thus necessitating increased familiarity with new technologies, together with the increased transparency and openness of smart technologies themselves.

7.2. Artificial Intelligence and Mobility: What Is at Stake for Safety?

Road transport is responsible for the majority of transport fatalities, with 1.35 million fatalities worldwide each year. On a global level, almost 40% of road fatalities occur in urban areas, while vulnerable road users account for 70% of road deaths in urban areas. Indicatively, during 2019, about 22,800 road traffic fatalities were recorded in the 27 EU Member States.[34] Despite significant improvements in road safety, the process of minimising crashes and their respective causal factors has markedly slowed during the last decade, with only a 20% reduction in crash fatalities.[35]

In recent years, the shift from traditional reactive road safety approaches towards the Safe System approach has been pursued. The Safe System approach accepts that all humans inevitably make mistakes. When mistakes do happen, all transport system elements must contribute to the avoidance of fatalities and, if possible, injuries. Innovative data-driven solutions can contribute to a holistic, proactive approach to addressing urban road safety problems, and represent a core principle of the Safe System Approach. A famous manifestation of this approach is Vision Zero, originating from Sweden.[36]

It is therefore clear that transport and road safety researchers, industrial practitioners, authorities and all stakeholders must make concerted efforts to further reduce crash numbers and mitigate crash consequences, with the utmost priority of negating losses of life and limb. It is not only important but imperative to exploit the new capabilities offered by artificial intelligence (AI). The rise and wide market penetration of smartphones, sensors and connected objects (whether mobile

[34] World Health Organization (WHO), Global status report on road safety 2018.

[35] European Transport Safety Council, *Ranking EU Progress on Road Safety*, 12th Road Safety Performance Index Report, 2018.

[36] R. Johansson, "Vision Zero–Implementing a policy for traffic safety", *Safety science*, vol. 47, no. 6, 2009, pp. 826-31.

or infrastructure) has increased the availability of analytical and broad-scope transport-related big data, which can now be effectively interpreted thanks to rapid progress in computational power, data science and computer science developments in the forms of advanced artificial intelligence tools.

The sections that follow outline specific advancements and challenges regarding the implementation of AI and big data to increase the safety levels of mobility and transport activities.

Big Data Developments Relevant To Road Safety

The rapidly increasingly connections that characterise the new transport landscapes have yielded a wealth of big data. The multitude of data sources include the following categories (this is a non-exhaustive list):

- Mobile phone data, including sensor-based data (e.g. Google Maps, Here, Waze)
- Cellular Network Data (e.g. mobile phone operators, etc.)
- Vehicular On-Board Diagnostics data (e.g. OEM industry)
- Camera data, including on-vehicle (internal, dashcam and peripheral) and on the road (cameras of cities, network operators, police)
- Data from car sharing services (e.g. Uber, Lyft, BlaBlaCar)
- Data from bike sharing services (e.g. 8D Technologies, Mobike)
- Social Media data (e.g. Facebook, Twitter)
- Telematics companies (e.g. Oseven, ZenDrive, Octo)
- Private agency sensor data (e.g. INRIX, Waycare)
- Travel Card data (e.g. Oyster card, Opal card)
- Public authority sensor or traffic measurement data (e.g. Ministries, Public Transport Authorities, Cities, Regions)
- Weather data (e.g. OpenWeatherMap, AccuWeather, etc.)

- Census data (e.g. Eurostat, National Statistics)
- Digital map data (e.g. OpenStreetMap, Google Maps, etc.)
- Shared mobility data (e.g. GPS, routing, etc.)
- Research-oriented data (e.g. floating car/instrumented vehicles)

This wealth of data sources provides high granularity for analysis, which in turn allows more precise training, predictions and similar calculations of road safety models, or more targeted and specialised analyses. Indicatively, it is now easier for road safety analysts to perform differentiations by road user category, achieve higher spatial and temporal resolution in the data and focus on niche analyses (e.g. interactions with vulnerable road users, particulars of professional drivers, freight vehicles etc.).

Other new developments in computer science, telematics and telecommunications, combined with the spread of connectivity, are also aiding road safety data collection. Most immediately, the rollout of 5G/6G technologies is facilitating data transmission and manipulation, while the Internet of Things (IoT) is progressively bringing new opportunities and possibilities for data acquisition (cross-device connectivity). Furthermore, on-board diagnostic (OBD) systems have become considerably more affordable in recent years. The widespread use of smartphones and social media allow for more users in an increasingly covered percentage of the road network area. In recent years, drones and satellites have complemented the available range of data, thus providing solutions by capturing interactions that were previously harder to observe.

Social media data can be invaluable for pattern analysis in road safety, and can be an excellent source of first-detection and first-response for crashes. Moreover, a proportion of social media data is publicly available, and thus exploitable for research through text extraction and processing, constituting an immense big data source. Increasingly powerful cloud computing, computer hardware and analysis tools have emerged to facilitate

the management and analysis of big data, especially when fused from multiple sources, while technological competition and a wide market enables typically sustainable pricing.

Big Data Challenges for Road Safety Exploitation

Nonetheless, big data can induce big issues for the prospective analyst. To start with, the consequences of using data which is not always representative of the whole population should be assessed and properly corrected. There is undoubtedly bias towards certain user groups as, despite market penetration, younger demographics are more engaged with smartphones and social media interactions. Furthermore, bias can have many dimensions. It is easy to wrongly consider a dataset as unbiased if it covers a specific dimension in detail (e.g. covering different road user categories), while failing in another (e.g. not covering exposure per category). Predominantly, publication biases can also manifest and always need to be considered in research, both in strictly road-safety topics and in the wider economic impact assessment.[37] Even using extensive databases, *a priori* desired conclusions should not drive the research approach or outcomes. Lastly, proper road safety analyses based on big data processing can be costly in terms of data acquisition, overall equipment and human capital. There is a high risk for decision makers to be misled by the opportunistic analysis of seemingly low-cost data in the absence of qualified data scientists and statisticians.

For such applications, the openness of big data is a constant question. A fragmentation of data ownership and a lack of interoperability between datasets and platforms is currently

[37] E.g. R. Elvik, "Effects on road safety of converting intersections to roundabouts: review of evidence from non-US studies", *Transportation Research Record*, vol. 1847, no. 1, 2003, pp. 1-10.; e.g. O. Ashenfelter and M. Greenstone, "Estimating the value of a statistical life: The importance of omitted variables and publication bias", *American Economic Review*, vol. 94, no. 2, 2004, pp. 454-60.

observed, especially in the industry. There are different commercial interests of the various road safety stakeholders in data, creating differing requirements for data access based on acquisition rate, granularity, intended use and so on. An additional layer is introduced by ownership, as several intermediaries have manifested. Data ownership varies depending on which party generates and collects the data. It is possible that they may be not willing to share data due to issues relating to privacy, legal liability, IP, competition, or costs. In other words, road safety data is often ethically or commercially sensitive.

It is important to remember that data is not free, and that all big data-related tasks, from acquisition to processing and provision have several maintenance and physical or digital infrastructure-related costs.[38] The diversity of data sources has undoubtedly been affecting data quality, and that can be discerned in several instances, for instance by examining the frequencies of outliers and/or unreasonable values. This can be quite straightforward to verify, for instance, in cases of traffic volume or weather data. Unavoidably, variations in hardware and software used for collecting data also impacts quality as well, even with well-maintained collection in mind. Last but not least, there is a notable lack of expertise in introducing the road safety context when conducting machine learning, data mining, and data management within the transport domain. A lot of analysts hail strictly from a computer science background and may not necessarily have the essential understanding of proper exposure measurement, road safety analytical design or risk factor and road safety countermeasure causal relationships.

[38] International Transport Forum (ITF), *Artificial Intelligence in Proactive Road Infrastructure Safety Management*, ITF Roundtable Reports, no. 187, OECD Publishing, Paris, 2021.

Surrogate Road Safety Measures

When discussing road safety AI applications, consideration must be given to a critical positive trend in road safety analysis in the form of surrogate road safety measures. These measures are alternative measures that can augment or even substitute the rarer (and less appropriately reported) crash and injury data. Examples of surrogate safety measures include traffic conflicts, harsh driving events, spatial/temporal headways, and many others.[39]

A massive advantage of surrogate safety measures is that they can become readily available for proactive analyses before crashes occur or in areas with limited or no crash data availability. In addition, such measures show less under-reporting and can even aid with crash reporting. More research on the validation of surrogate safety metrics is essential, to reveal which metrics not only correlate with reported crashes but also have accurate predictive capabilities. There is also a need to predict the number of fatalities and/or injuries with good utility and to determine how these metrics can integrate crash participant fragility, physical properties and crash type consequences. The adoption of surrogate safety metrics implies that road safety research is now being conducted across several different indicators, instead of just examining crashes and injuries. This new multidimensionality leads to the review of statistical training needs, so that data is not misused/misinterpreted in relation to what exactly constitutes a safety-critical situation.

Naturally, the collection of surrogate crash measures is becoming increasingly automated and can augment more general-purpose big data. This automated connection is made possible by smartphone sensors (which can be used to obtain data on harsh braking, harsh acceleration, harsh cornering, driving distraction due to cellphone use, speeding, poor road surfaces)

[39] A.P. Tarko, "Surrogate measures of safety", in D. Lord and S. Washington (Eds.), *Safe mobility: challenges, methodology and solutions*, Emerald Publishing Limited, 2018.

or instrumented/floating vehicles. Technologies like automatic crash notification (eCall) and event data recorders enable data-driven responses to post-crash problems. Street imagery, also collected by floating vehicles, supports the assessment of road safety performance, such as the star-rating for roads.[40] With ever smarter vehicles, active safety system activation can also constitute a surrogate safety metric. By monitoring the activation of systems such as Anti-lock Braking System (ABS), Electronic Stability Control/Program (ESC/ESP) and Autonomous Emergency Braking (AEB), reliable information about safety-critical events will flow from increasingly connected vehicles, regardless of their level of automation.

Key Road Safety AI Aspects

With these new options and respective challenges unfolding, AI enters the field to open new advances in all aspects of mobility. It is very difficult to predict all AI uses, or even categorise them using well-defined and distinct labels, but it is reasonable to outline advances in three major areas: **(i)** vehicle technology, **(ii)** driver monitoring and **(iii)** crash risk estimation.

Regarding AI Advances in Vehicle Technology, several new systems have been rolling out and continuously improving. The navigation of complex, non-straightforward road environments becomes more attainable at an increasing rate, as high-end RADAR/LIDAR and sensor technologies stand at the forefront of developments. Through the development of connected and automated vehicles, several traditional road safety risk factors and similar problems are eliminated by RADAR/LIDAR, such as exclusive reliance on lighting and limitations caused by obstructions. On the algorithmic front, the decision-making process is improved and refined by deep learning and complex

[40] Ai-RAP and Automated Coding for iRAP in SuM4All (Sustainable Mobility for All), *Sustainable Mobility: Policy Making for Data Sharing*, Washington DC, License, Creative Commons Attribution CC BY 3.0, GRA in action series, 2021.

algorithms such as advanced convolutional neural networks for perception, localisation, prediction and decision-making. As is typical with high degrees of development, high degrees of specialisation follow, as purpose-made systems are starting to receive purpose-made tools and algorithms, such as grocery delivery or (initially) fixed-route public transport. It is worth noting that most developers design their systems independently and are not reliant on infrastructure adaptations, while over-the-air AI upgrades become a new reality.

Meanwhile, more physical test areas and virtual testbeds are provided and examined and software errors are gradually contained and reaction times are minimised overall. Facial recognition technologies aid commercial company claims with insurance carriers (e.g. Nauto). Vehicle cooperation algorithms are introduced to fleets, aimed at traffic conflict reduction and efficient traffic management. Furthermore, increased connectivity means additional connectivity byproducts: increased parking availability and freight vehicle platooning can mean reduced road safety exposure indicators, as well as increased fuel efficiency. Ambitious flying vehicle (VTOL) concepts are co-considered.

Regarding AI advances in crash risk estimation, an array of new AI methods and machine/deep learning or similar algorithmic models are available to road safety researchers, stakeholders and authorities for real-time crash risk estimates. Big data on crash occurrence and road and traffic characteristics from infrastructure sensors is transformed into multi-dimensional static or dynamic maps of road risk prediction and road & driver star ratings. Crash datasets are imbalanced, rare event cases which give an incentive for the creation of new approaches and venues of analysis through AI methods. Infrastructure assessment frameworks are starting to embrace AI methodologies, such as the i-RAP transition to Ai-RAP.[41] A large number of model configurations show very promising

[41] Ibid.

performance, albeit on specific datasets. Much more research is required on the transferability of AI capabilities to new study areas. The successful performance of a model in one suburb case-study does not guarantee that it will work in another suburb or at city-wide level, so performance is still uncertain.

Regarding AI Advances in telematics & driver monitoring, the insurance industry is heavily investing in telematics, offering reduced premiums for safer driving. AI and data fusion technologies are actively being used in all stages of road safety data collection, transmission, storage, harmonisation, analysis and interpretation from telematics. Personalised feedback can be created and obtained almost instantaneously for participant drivers. Algorithmic route analysis and personalised hotspot detection features based on surrogate safety measures are actively being examined. As far as driver behaviour is concerned, during-trip and post-trip interventions are now possible, and are best administered with gamification and reward systems.

With so many promising new developments, AI and big data applications can be expected to unlock critical road safety advancements, such as attaining Vision Zero safety levels. The most notable venue is that AI facilitates truly proactive management of traffic safety in various ways, such as the following:

- The collection of data on road infrastructure conditions and traffic events through widespread, real-time and broad-scale sensors and systems such as connected vehicle operations and computer vision.
- The identification of high-risk locations through predictive multilayer models before crashes occur.
- Enabled by multiparametric big data, AI pushes the limits of pattern recognition and reaction times beyond human capabilities and may thus uncover new crash-prone road configurations, risky driving behaviour or critical interactions. Essentially multiple in-depth examinations can be conducted per second of analysis.

- Recent developments in the field of explainable AI (XAI) begin to cope with the challenge of the "black box" phenomenon, shedding light on the causal relationships of risk factor, road safety countermeasure and crash causation.

Current Barriers

Needless to say, there are several pending barriers to AI-related developments. Safe, road-worthy AI systems face significant challenges that are only hesitantly tackled. There needs to be a concentration of effort to achieve AI systems with high interface ability with each other, high interoperability across different road networks, timelessness and resilience to ensure a smooth transition of operations and also considerable scalability for reproduction and functionality across areas.

Currently, the absence of monitoring and accountability seriously limits road safety performance. To counter this, public acceptance and trust must be meticulously built and increased by monitoring and reporting AI progress, and conveying the message that AI in road safety is not only for-profit, but also for-society. The neutral ground must be established by the operation of independent tools, such as the AI Incident Database.[42] In addition, legal and operational frameworks are considerably lagging compared to technical developments; self-updating mechanisms are urgently required for them.

While research and innovation efforts on the use of AI in computer vision and risk prediction are very much in the spotlight at present, they require more peripheral support. Thorough arbitration, as well as evaluation and assessment criteria, must be established across platforms, in research and industry, to deliver robust AI vehicular systems that will actively contribute to fatality reductions. Cybersecurity/malicious hacking concerns

[42] S. McGregor, *Preventing repeated real world AI failures by cataloging incidents: The AI incident database*, arXiv preprint arXiv:2011.08512, 2020.

may cause several implications (vehicle manufacturers, software engineers, vehicle owners, automated fleet operators). All these different AI aspects will lead to improvements of road safety interventions and countermeasures. Measuring them via dynamic feedback loops through crash records and surrogate safety measures remains a completely unexplored field.

Naturally, big data applications face their own challenges. At present, large margins remain for road safety practitioners to rapidly gain in terms of data flow by copying best practices for data sharing and privacy protection from other, more free-sharing fields. More secure alternatives to data exchange, such as the exchange of queries and responses can be explored, instead of raw information. On a similar note, multiple-criteria based exploration and decision analysis are needed to determine the most efficient Key Performance Indicators that can be mined or created from the available big data.

In a manner parallel with AI cross-platform operation, the establishment of commonly accepted data harmonisation and fusion protocols would be very beneficial. More investigation is needed on the best approaches to reconciling different data scopes and scales (e.g. country, city, city block, road segment, road user). On a high level, Governments and Road Safety Authorities can mandate the sharing of aggregate vehicle data, or provide financial or similar incentives to industrial partners. Indicatively, a minimum-required dataset can be defined for all vehicle manufacturers to report in an anonymous standard aggregate format. More attention needs to be given on the collection of data on traffic volume, speed distribution, and locations where vehicles' active safety systems (ABS/ESP/AEB) are engaged. Of course, regulatory frameworks for data protection need to be clarified to encompass all aspects of operations in a non-prohibitive manner, while governments should also examine how Freedom of Information laws articulate with data protection laws. Throughout the process, it is essential to observe ethical data sharing.[43]

[43] E.g. Accenture, *Building data and AI ethics committees*, Northeastern University

Road safety remains a complex multifaceted science with its own particularities. It is a given that road safety levels cannot be improved on the basis of on accurate forecasting alone, as causal factors must be determined. Therefore, priorities should include the development of explainable AI (XAI) – "white box" techniques that are more transparent.[44] Emphasis should be placed on collaborations across countries for the integration of all road realities and road safety cultures, which are often overlooked by straightforward analysis. Funding must also be made available to road safety multi-disciplinary professionals to conduct post-intervention assessments and validate or re-calibrate the risk prediction tools.

The creation of new road safety tools must not be a self-serving purpose, but rather a precisely coordinated process, and these new tools need to be aligned with precise policy objectives. Stakeholders should aim to exploit the new technological landscape by commissioning research to assess the availability of surrogate measure data and the generation of risk mapping and road safety assessment tools.

For their part, researchers and practitioners have to develop new skills and a digital infrastructure mentality, and promote a multi-disciplinary approach to road safety that combines expertise from the fields of data science, technology and safety. Estimates of the benefit/cost ratios of interventions can be set to update in a dynamic manner, along with accessible user-friendly interfaces, so that they are readily usable when decisions must be made. Ultimately, all research outputs must be usable, however advanced: for instance, risk mapping tools need to be user-friendly if they are to be adopted by road users.

– Ethics Institute, 2019.

[44] E.g. W. Samek, G. Montavon, A. Vedaldi, L.K. Hansen, and K. Müller (Eds.), *Explainable AI: Interpreting, explaining and visualizing deep learning*, vol. 11700, Springer Nature, 2019.

Conclusion

In conclusion, there appears to be great potential for seamless big-data-driven procedures from safety problem identification to selection and implementation of optimal solutions. There is a newfound net present value in highly granular road safety data, available for (real-time) early problem detection and prompt and customised decision support on every level. Despite this, considerable ground remains to be covered for existing road safety AI applications (vehicle, telematics, crash and driver behaviour analysis). Largely unexplored directions remain in several road safety aspects such as crowdsourcing options, ex-ante and ex-post road safety measure effectiveness, and optimisations regarding data harmonisation. Overall, based on the current potential, big data and Artificial Intelligence can become efficient catalysts for achieving Vision Zero road fatalities in the coming decades.

8. Data and Artificial Intelligence for a Smart Mobility: What's the Way Ahead?

Luca Milani, Stefano Napoletano, Andrea Ricotti, Nicola Sandri

Introduction and Growing Relevance of Data and Artificial Intelligence

Data and Artificial Intelligence are on the verge of disrupting businesses and society. The global Artificial Intelligence software market is predicted to account for $62.5 billion in 2022, reporting an increase of more than 20% from 2021, according to Gartner estimates. Historic growth is also witnessed by rising investments in equity capital of AI startups and increasingly number of AI deals. According to a Gartner's survey, approximately one third of technology and service provider organisations would invest more than $1 million into AI technologies in the next 2 years, recognising the potential AI has to improve business efficiency, create new products and services, expand customer base, ultimately generating new sources of revenue. Furthermore, results from the 2021 McKinsey's *Global Survey on Artificial Intelligence*[1] indicates

[1] The online survey was in the field from 18 May to 19 June 2021. It garnered

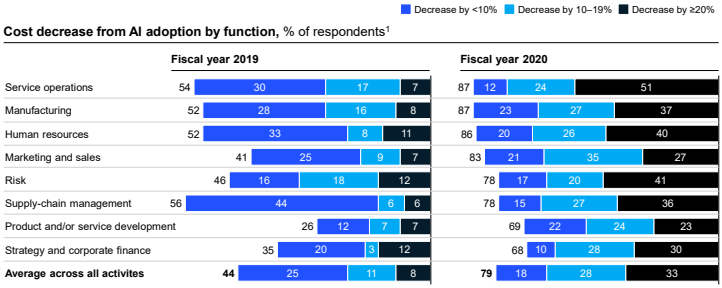
that Artificial Intelligence's adoption is continuing its steady growth:

- 56% of all respondents report AI adoption in at least one corporate function, up from 50% in 2020, with highest increase in companies in emerging economies, including for instance China, Middle East and North Africa.
- Business functions showing the most common adoption of AI are service operations, product and service development, marketing and sales.
- Results also suggest that AI's impact on the bottom line is growing: 27% respondents reported that at least 5% EBIT is attributable to AI in 2021, versus 22% respondents in 2020.
- AI has potential to bring significant cost savings: responding companies reported greater costs savings from AI than they did previously in every function, with the largest year-over-year changes in the shares reporting cost takeout from using AI in product and service development, marketing and sales, and strategy and corporate finance.

---

responses from 1,843 participants representing the full range of regions, industries, company sizes, functional specialties, and tenures. To adjust for differences in response rates, the data are weighted by the contribution of each respondent's nation to global GDP. McKinsey Global Survey, *The State of AI in 2021*.

Fig 8.1 – Cost decrease from using Artificial Intelligence by function



Question was asked only of respondents who said their organisations have adopted AI in a given function. Respondents who said "no change", "cost increase", "not applicable", or "don't know" are not shown.

Source: McKinsey Global Survey, *The State of AI in 2021*

As outlined, data and Artificial Intelligence applications can influence several aspects of companies' day-to-day business, for instance due to increased efficiency in operations. At the same time, these applications can assume a critical role in improving the quality of people's lives, particularly in urban areas, which are becoming increasingly important as the engines of current and future economic growth and development. Indeed, cities are already responsible for the bulk of production and consumption worldwide. According to the World Bank, ~55% of the world's population (equaling to 4.2 billion inhabitants) currently live in cities, with the trend expected to continue: by 2050, nearly 7 of 10 people in the world will live in cities. In addition, more than 80% of global GDP is generated in cities, which are also responsible of two thirds of global energy consumption and account for more than 70% of Greenhouse gas (GHG) emissions. Consequently, it is undoubtedly true that cities will play an increasingly important role for global development, innovations, new ideas, and be the places where data and Artificial Intelligence can play a key role to ultimately increase people's quality of life.

Data and Artificial Intelligence Potential Applications in the Cities of Tomorrow (Smart Cities)

According to McKinsey's Global Institute Report on Smart Cities, there are eight main domains of applications for data and Artificial Intelligence in the cities of tomorrow, including the following examples:

Mobility: shared mobility, allowing access to short-term car, bike, e-scooters use without ownership; congestion charging, applying fees for private car usage in specific areas; Mobility-as-a-System applications, showing information on pricing, time and allowing to purchase one ticket only to travel across multiple modes; intelligent traffic signals; smart parcel lockers; smart parking applications.

Security: wearable audio, video, or photographic recording systems used to record incidents; use of data and analytics to focus inspections of buildings; technologies designed to predict and mitigate the effects of climate change; intelligent monitoring through smart surveillance.

Healthcare: use of analytics direct public health interventions for sanitation and hygiene; integrated patient flow management systems; online care search and scheduling; remote patient monitoring, through collection and transmission of patient data for analysis and intervention by a health-care provider in another location; virtual patient-physician interaction through audiovisual technology.

Energy: systems optimising energy and water use in commercial and public buildings; smart grid technologies to optimise energy efficiency; dynamic electricity pricing; home energy automation systems optimising home energy consumption; smart streetlights.

Water: systems for leakage detection and control; systems leveraging data and information (e.g. weather, soil conditions, plant type) to optimise irrigation; water consumption tracking to increase awareness and reduce consumption; systems for monitoring water quality.

Waste: digitally-enabled pay-as-you-throw systems, including apps and text messages delivered to users to increase awareness and reduce waste; systems to optimise route collection, using sensors to measure trash volume and direct routes of garbage trucks.

Economic development and housing: digitised process for businesses to obtain operating licenses and permits; digital channel for businesses to complete tax filing online; digitisation and automation of application process for land-use and construction permitting; online retraining programs; personalised education, with tailored learning environment.

Engagement and community: digitisation of citizen-facing government administrative services such as income tax filing, car registration, application for unemployment benefits; public engagement in city affairs through digital apps; local connection platforms, as websites or mobile apps helping people to connect and potentially meet others in their community.

Taken singularly or together, the above-mentioned applications bring invaluable economic, environmental and social benefits to all citizens. Indeed, smart city applications can improve key quality-of-life indicators, for example:

Time and convenience: 15-20% reduction in commute time and 45-65% reduction in time interacting with healthcare and government.

Cost of living: 1-3% reduction in citizen expenditures.

Formal employment: 1-3% increase in level of formal employment.

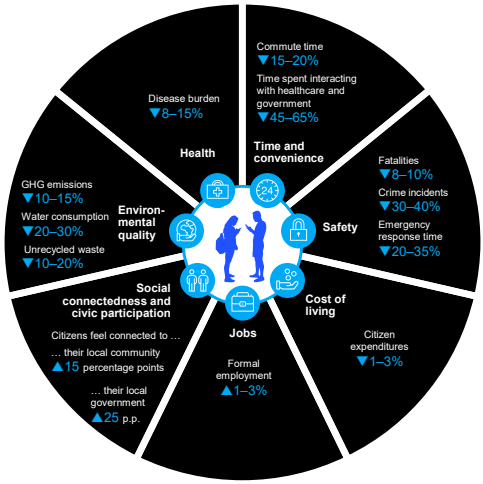
Environmental quality: 10-15% reduction in GHG emissions, 20-30% reduction in water consumption, 10-20% decrease in unrecycled waste.

Health: 8-15% reduction in disease burden.

FIG. 8.2 – SMART CITY APPLICATIONS

Smart city applications can improve some key quality-of-life indicators.

Potential improvement through current generation of smart city applications, from time of implementation



SOURCE: McKinsey Global Institute analysis

The following paragraphs will further deep dive the potential applications of data and Artificial Intelligence in the smart mobility domain in urban areas.

The Role of Data and Artificial Intelligence in Smart Mobility in Urban Areas

Artificial Intelligence is a powerful tool to further drive sustainable transitions to a more efficient, and human centric mobility system, particularly in urban contexts. At the same time, it is undoubtedly true that a holistic approach to urban mobility planning and management needs to be adopted. The following paragraphs investigates few innovative solutions on data and AI usage in smart mobility across the globe, focusing on: self-service electric vehicles rental, Mobility-as-a-Service platforms, on-demand micro transit, traffic control digital infrastructures for congestion charging, and dynamic routing optimisation for last mile delivery.

Self-Service Electric Vehicles Rental

Companies offering self-service electric vehicle rental provides individual users with an application allowing to rent a car in self-service, choosing the pick-up point and the duration of the rental service directly through the app, without having to deal with waiting lines and avoiding human interactions. These operators typically own the EV charging infrastructures and parking facilities across the territory of their operations. These services might also work as a valuable alternative to owning a fleet of cars for employees. Benefits of this AI-based smart mobility solutions are environmental (as only electric cars are used for the service) and economic, constituting a new vehicle ownership model, without the full property, avoiding maintenance and repair costs.

Examples of providers of these services include Ufodrive, an Irish-led EV rental app company, currently operating in 9 countries in Europe, with 150+ thousands connected chargers. The firm offers a completely-digital, EV-only rental service enabling users to rent a vehicle, arrive and the pick-up point and drive the car. Ufodrive offers also the possibility to rent cars for a day, a week or more, allowing to sign for monthly or more subscriptions. For example, subscriptions include free charging for the duration of the renting period, a certain allowance of km per month, insurance and breakdown policies, active route planning technology for driving and charging the vehicle, no additional cost of ownership fees, "Phone-As-A-Key Control (PaaK)" service enabling to unlock the car, connect and disconnect from the charger, check battery level (all from users' phone). Due to its environmental impact, Ufodrive implements also rewarding programs, by providing free ride credit (redeemable against the next booking) at the end of each rental, based on the carbon emissions avoided during the trip with the service.

Mobility-as-a-Service Platforms

Mobility-as-a-Service (MaaS) platforms are new mobility offering combining all transportation modes in a single application, leveraging data and information to integrate planning, pricing, booking, payment and customer service processes. According to degree of integration and geographic coverage, three main operators' archetypes exist within the MaaS landscape:

MaaS pioneers: providers of end-to-end MaaS solutions, integrating all the journey steps (e.g. planning, pricing, payment) in a single application, offering innovative pricing mechanisms (e.g. monthly subscriptions for unlimited use of transport services). These operators are typically locally-focused on one city or area. Examples of these providers include, for instance: Yumuv, BVG Jelbi, Whim.

Focused internationalists: providers of MaaS solutions at national scale, with stronger focus on specific areas. Examples of these operators include: SNCF L'Assistant and Renfe-as-a-Service by Renfe, the latter currently in development.

Information players: providers of information like travel times and distance between point of departure and arrival at global scale. Multiple modes of transport are included (e.g. airplanes, cars, trains, public transit), without actually providing the possibility to book and pay travel tickets. Examples of these operators include: Google Maps, Apple Maps, CityMapper.

As far as ownership is concerned, three main archetypes are observed:

Platforms from Municipalities or urban transit operators: apps directly promoted by the Municipalities or directly-controlled urban transit operators, aiming at integrating different modes of transportation in urban areas. This particularly applies in those urban areas currently experiencing continuous proliferation of mobility operators (e.g. car sharing, bike sharing, scooter sharing), each one with different reservation and booking process. Moreover, these apps are

typically developed in-house or in partnership with suppliers of white label solutions. Examples of players in this regard include the MaaS app Jelbi, launched by BVG in Berlin, in partnership with Trafi, which provides the white label solution.

Platforms from national transport operators: apps promoted by national public transport operators, typically passenger rail operators, to offer integrated mobility services at local or national level, depending on maturity level. Examples of companies in this case include SNCF L'Assistant and Renfe-as-as-Service (RaaS).

Platforms from private technology players: MaaS applications developed by technology companies operating outside the transportation and infrastructure sectors. These companies tend to offer tailored solutions to specific urban contexts, according to priorities and mobility plans of the Municipalities. Whim has been among the first technology companies entering in the MaaS landscape. The app is currently operating in Vienna, Antwerp, Helsinki, Turku, Tokyo, Switzerland (nationwide) and Birmingham.

Several municipalities, transport companies and technology start-up have been investing in the MaaS space due to the fact these digital applications are expected to bring benefits both for passengers and urban areas. The former benefits from full transparency over itineraries and tickets' pricing, with all providers' offerings disposable in a single space. The latter benefits from increasing understanding of people's mobility preferences and decision-making processes, by collecting and analysing travel data and information. Data and information collected via MaaS platforms help the Municipalities both in the short term, by optimising traffic flows, and in the long term by improving the overall transport system, incentivising environmentally-friendly alternatives.

On-Demand Micro-Transit: Across the globe, cities and transit agencies are embracing on-demand micro-transit. This service uses a technology to combine routing and ride scheduling flexibility with the affordability and sustainability of public

transportation. The data algorithm allows to match passengers' demand traveling towards the same direction with a public bus, with trip's time similar to that of a private taxi. One of the most interesting examples of this application is the company Via Transportation, active from 2012 in the space of digital infrastructures for public mobility. Via operates as a Software-as-as-Service (SaaS) company for all forms of transportation, from public transportation planning and operations to non-emergency medical transportation, from logistics and deliveries to school bus fleet routing and autonomous vehicles. Via's algorithm matches multiple passengers heading in the same direction and books them into a single vehicle. Shared services are typically from corner-to-corner to streamline vehicles' routing, requiring passengers to walk to a pickup point indicated on the app. Eventually, the company operates in partnership with local transit authorities, government entities, universities, taxi fleets and private organisations. Among the major benefits of these applications, the service allows to connect riders who live and work far from public transit, bringing convenient and accessible transportation to areas that need it most. In addition, the service creates a flexible, efficient system that maximises use of resources. Finally, it improves the rider experience with booking apps and customisable configurations to meet every rider's need, including wheelchair-accessible vehicles and door-to-door service.

Digital Infrastructures for Congestion Charging Mechanisms

These systems work thanks to a digital technology infrastructure, namely electronic transponder devices for vehicles (e.g. cameras). The successful implementation of congestion charging mechanisms in cities globally, also highlights the environmental benefits and impacts that these applications has on GHG emissions' reduction and decrease in commuting time. As a matter of fact, the mechanism implemented in Singapore

in 1998 led to a 24% reduction in inner-city traffic and a 10-15% reduction in GHG emissions. Evidence from Stockholm proved that successful implementation of congestion charging led to a 30-50% reduction in congestion. Finally, in Milan the Implementation of Area C (i.e. charging fee for access to the historic city centre) helped to reduce average daily entries to the city centre by ~30% in its first year of deployment.

Dynamic Routing Optimisation for Last Mile Delivery

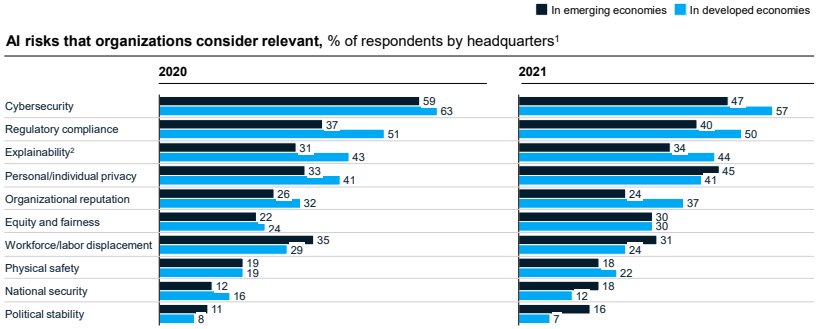
Last mile delivery logistics processes have been becoming increasingly challenging particularly due to increased volumes, as a consequence of e-commerce sales' spike after the Covid-19 pandemic. A dynamic route optimisation tool facilitates cost-efficient planning of itineraries for distribution managers, constituting a valuable tool to tackle the challenges associated with last mile delivery in urban areas. Practically, a dynamic route optimisation helps distribution companies to factor in available resources, determining the most efficient utilisation (e.g., optimising fleet's routes). These tools can also potentially incorporate into routing optimisation external factors, such as weather, traffic, streets' blockage, to adjust routes, ultimately providing delivery drivers with the most efficient path possible.

The US-based Route4me constitutes an example of company providing routing optimisation software for multiple applications and final users. The software is able to evaluate billions of scenarios in seconds to create optimal routes to avoid traffic, construction and other obstacles. Reduction of gas, labour, vehicle costs and insurance are the ultimate benefits of the route optimisation process.

Conclusion

Data applications and digital transformations are currently reshaping the market landscape, with several companies already deploying machine learning and data analytics in their day-to-day operations, particularly in the mobility space. At the same time, risk management is one of the crucial area where many operators have room to improve. According to the 2021 McKinsey's *Global Survey on Artificial Intelligence*, cybersecurity remains the most recognised risk among respondents. Additional concerns are also related to regulatory compliance, the ability to explain how Artificial Intelligence models come to their decisions, personal and individual privacy, organisational reputation, and others.

Fig. 8.3 – The Management of AI risks remains an area for significant improvement, as respondents report a waning focus on cyber



1. "Emerging economies" includes respondents in Association of Southeast Asian Nations. China, India, Latin America, Middle east, North Africa, and Sub-Saharan Africa, and "developed economies" includes respondents in developed Asia, Europe, and North America. Question was asked only of respondentswho said have organisations adopted AI in ≥ 1 business function: Those who answered "don't know" are shown

2. That is, the ability to explain how AI models come to their decisions

Source: McKinsey Global Survey, *The State of AI in 2021*

While revenues from Artificial Intelligence applications have been growing at a fast pace in the last years, the long-term trajectory will depend on enterprises' ability to advance in maturity. Understanding the full potential of data and Artificial Intelligence is crucial for enterprises operating in a dynamic and continuously evolving business and economic environment to improve businesses' performance and people's quality of life in several domains, and particularly in the smart mobility landscape in urban areas.

9. A New Digital Agenda for Rail Transport

Alberto Mazzola, Ethem Pekin, Matteo Mussini

The sustainability and energy-efficiency of railways are undisputed. Rail is the most energy-efficient transport mode and the most effective way to decarbonise transport in large parts of the European Union, as highlighted in the EU Council Conclusions – *Rail at the forefront of smart and sustainable mobility* – adopted by EU Transport Ministers in June 2021.

Transport accounts for 26% of the EU's energy-related greenhouse gas (GHG) emissions. While overall transport emissions continued to grow, the direct emissions of rail transport accounted for less than 0.4% of overall transport emissions in 2019, despite the fact that rail carried approximately 17% of freight and 8% of passenger traffic on inland routes within the EU27. The European Commission Study *Sustainable Transport Infrastructure Charging and Internalisation of Transport Externalities* shows that rail already internalises its external costs much more than any other motorised mode of transport. This situation demonstrates the need for better rules on the internalisation of external costs, and fairer conditions of competition between different modes of transport.

Rail is already Green-Deal-compliant and on target to cut its GHG emissions by 55% compared to 1990 levels by 2030, in line with the EU's "Fit for 55" goals. Rail continues to improve its carbon intensity when calculated according to the well-to-wheel method, which includes the GHG emissions

from producing and distributing fuels, as well as those from using them. According to the European Environment Agency (EEA), furthermore, rail remains closer to zero emissions than any other mode of transport.

Four out of five trains in Europe already run on electricity, one third of which is harvested from renewable sources. According to the International Energy Agency (IEA), railway oil consumption will fall to almost zero by 2050. 90% of the oil currently used for rail traction will be replaced by electricity, and the remaining 10% will be replaced by hydrogen. More traffic on the European railways will mean a substantial drop in transport GHG emissions.

Furthermore, the EU Strategy for Sustainable and Smart Mobility published by the European Commission in December 2020 clearly shows that a large part of the EU's efforts to achieve the climate goals set by the Paris UNFCCC (UN Framework Convention on Climate Change) agreement depends on decarbonising transport and enhancing the role of railways in Europe's mobility.

The European Commission's vision is that, by 2030, high-speed rail traffic will double across Europe and scheduled collective travel for journeys under 500 km should be carbon neutral. By 2050 rail freight traffic will double, and a fully operational, multimodal Trans-European Transport Network (TEN-T) for sustainable and smart transport with high-speed connectivity will be finalised. Such targets will never be reached without new rail infrastructures and further digitisation of the existing infrastructure and rail services. The length of congested rail infrastructure has risen constantly since 2015. This vision forms the basis of the green and digital transition that the European mobility system is currently undergoing, and has visibly affected the way in which Member States can invest funds from the Recovery and Resilience Facility, a financial vehicle created in 2021 to help EU Member States recover from the economic downturn caused by Covid-19, and build back on better, more sustainable foundations.

Railways Play a Very Special Role in Both These Transitions.

While its sustainability already makes rail transport an attractive option for passenger and freight customers, the further digitalisation of the railway system will give the rail industry an opportunity to serve its customers better, increase its capacity and automation, and integrate more effectively with other modes of transport.

The shape of current logistic chains will inevitably change as new technology facilitates the digital integration of different modes, a denser flow of information on traffic and tracking, easier passenger access to services and information, more efficient use of infrastructure capacity and a higher degree of predictability on timing.

Digitalisation will also increase the large amount of data available to railway undertakings and parties currently outside the rail sector: the use of this data, in full compliance with rules on privacy and data ownership, will create opportunities for new business initiatives. Dependable information, such as train timetables, availability of tickets, travel planners, freight terminal data, etc. will all contribute to the realisation of a Single European Rail Area.

Of course, further digitalisation of railways relies on good cooperation both between railways and with telecommunication players. New 5G networks will represent a major opportunity for railways, by empowering the Internet of Things and improving access to real-time information. Proper interfaces between conventional and digital devices will be maintained.

In the paragraphs that follow, we will browse through the tools implemented by the rail sector to digitalise its production processes and relations with customers.

Rail's Digital Agenda

European Rail Traffic Management System

The European Rail Traffic Management System (ERTMS) is a single European signalling and speed control system that ensures interoperability of the national railway systems, thereby reducing the purchasing and maintenance costs of the signalling systems, as well as increasing the speed of trains, the capacity of infrastructure and the level of safety in rail transport.

The European rail sector sees the deployment of ERTMS as a centrepiece of the completion of the market liberalisation that, in terms of regulatory framework, was agreed upon by the European legislators in 2016 (the so-called Fourth Railway Package). However, in the last 20 years, less than 10% of the TEN-T Core network has been equipped with the ERTMS. The pace of deployments needs to be accelerated.

Furthermore, developing the technical and legal framework for the increasing levels of automatic train operation, improved data connectivity along train routes (e.g. through the rollout of 5G technology) and other rail-related digital developments should be on top of the agenda.

CER (Community of European Railway and Infrastructure Companies) has already made its position clear on ERTMS deployment and industrialisation.[1] The immense financial efforts that railways are ready to make (capital investment for track-side ERTMS deployment on the entire TEN-T core network amounts to €80 billion, including digital interlocking plus €11 billion for onboard retrofitting of the entire fleet) must go hand in hand with a clear commitment of public authorities, both in terms of secure and adequate funding, and in terms of strengthened governance of its deployment.

[1] "CER Position - Boosting ERTMS deployment", CER The Voice of European Railways, 27 September 2021.

Firstly, new and appropriate governance for such a large-scale European project is needed to ensure the financial and political commitment to further improve the attractiveness of investing in the ERTMS, and to guarantee legal certainty for private investors. Secondly, 2030 must be kept as the deadline for ERTMS deployment on the TEN-T core network, and 2040 for the comprehensive deployment. This means that the deployment rate will have to increase by a multiple of 10 compared to the last 25 years. Thirdly, co-financing rates of the Connecting Europe Facility[2] for ERTMS should be set at 100%.

Smart technical rail operations

The introduction of the Digital Automatic Coupler (DAC) aims to address the three main challenges of the European rail freight sector – increasing capacity, productivity and quality – which are crucial for a more efficient rail freight system. The ambition for DAC is to successfully achieve the transformation from the current screw-coupling system to the digital automatic coupling system by 2030, thus dramatically reducing the time to assemble a freight train from over 2 hours to just a few minutes.

DAC deployment requires testing over several years under real operational conditions. From February to the beginning of March 2022, the so-called "DAC demonstrator train" (as part of the DAC4EU project) was stopping at four different stations all over Austria and ran through an extensive test programme. The findings and the knowledge gained from operational tests will be taken into account for the further development of the DAC.

[2] The Connecting Europe Facility (CEF) is a key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. It supports the development of high performing, sustainable and efficiently interconnected trans-European networks in the fields of transport, energy and digital services. CEF investments fill the missing links in Europe's energy, transport and digital backbone.

From 2026 on, the DAC could be deployed in stages and be in use throughout Europe by 2030. A pan-European coordinated and funded deployment programme is a precondition for DAC to become a reality.

Automatic Train Operations (ATO) has the potential to enable rail infrastructure managers to use the maximum pathway capacity of existing railway corridors. The consistent implementation of ATO will increase the transport capacity of TEN-T and Rail Freight Corridors by a minimum of 30% by 2040.

Digitalisation in capacity and train path management

European rail infrastructure managers will only be able to make their positive contribution to achieving climate targets if existing infrastructure capacities are managed highly efficiently. This requires the use of state-of-the-art digitalisation technology in all areas of capacity and path management.

Europe's major infrastructure managers and railway undertakings endorsed a Joint Vision for the Sector on Digital Capacity Management.[3] Signed by RailNetEurope, Forum Train Europe, the International union of railways (UIC), the Rail Freight Forward initiative, CER, European Rail Infrastructure Managers (EIM) and the European Rail Freight Association (ERFA), the document outlines the sector's vision for the future of Digital Capacity Management (DCM).

DCM will help free up capacity on congested lines and boost the modal shift towards rail for both passenger and freight traffic. DCM will make it possible to allocate capacity on infrastructure by responding to late demand closer to the market, essentially from freight, and in a much shorter time. Strong demand for investments in Digital Capacity Management highlights the latter's role as a major game changer in terms of reaching the Green Deal targets for the transport sector. DCM is the integral

[3] Joint Vision for the Sector on Digital Capacity Management, DCM/RNE-RFF-FTE-CER-EIM-ERFA-UIC, Vienna, 4 October 2021.

IT-part of the European programme "TimeTable Redesign (TTR) for Smart Capacity Management".

The European TTR programme is already up and running, but funding and resources (both national and international) are essential for its implementation. Implementing DCM will cost a total of €675 million and this needs to be financed by European and national funds. The regulatory framework at European and national levels should be adapted to allow the fully harmonised implementation of TTR.

Digitalisation of customer relations

The possibility of e-ticketing, e-booking, integrated and/or multimodal ticketing, and new offerings from new or incumbent digital platforms all derives from the increased digitalisation of the rail system, which will increase the quantity and quality of data, thus enabling operators to address individual requirements and create door-to-door solutions together with added value for the customer before, during and after travel.

In this new context, Mobility-as-a-Service (MaaS) describes a shift away from personally-owned modes of transport, towards mobility solutions that are consumed as a service. The key concept behind MaaS is to offer travellers door-to-door mobility solutions based on their travel needs. MaaS regards the entire transport system as a single entity, and heavy and light rail, with its low emissions, will be part of the picture.

To improve travel information from departure to destination, and to facilitate the right choice of train and intermodal journeys, as well as through-ticketing, the managers of the European railway companies have agreed to launch a common project called *Full Service Model*, together with leading ticket vendors. This will create an open, plug-and-play IT framework for the distribution of rail tickets in Europe, instead of bilateral IT solutions between distributors and rail service providers.

In the next couple of years, the main focus of railway undertakings will be on improving the booking experience for passengers. Railway undertakings are committed to offering a

seamless user-experience when searching, selecting and buying their railway services. In order to achieve seamless ticketing, sector-based solutions should be supported and considered as the starting point when improving multimodal ticketing, in line with the example of the CER Ticketing Roadmap.[4]

Timetables will have to be more up-to-date, and it will have to be possible to buy train tickets 6 to 12 months in advance, as this is particularly important for tour operators. Tariff exchange systems will also have to be more up-to-date, and enable through-ticketing where applicable. We will have to be able to count on a European-wide standardised API for selling train tickets and increased harmonisation of ticketing conditions, to give passengers greater clarity on ticket conditions of use. Tickets will have to be fully digitalised, with real-time information during the journey and better support during disruptions and delays.

In the past few years, the majority of the rail sector has been working on enablers, creating the respective specifications for train ticket sales that harmonise the different ways of selling tickets (Open Sales and Distribution Model - OSDM), Europe-wide integrated rail timetables (MERITS), and the basis for full ticket digitalisation (ETCD). These enablers will further improve the customer experience when planning, booking and travelling within the EU and internationally by rail.

Railway undertakings are committed to improving international ticketing for rail in the broadest sense. By 2030 passengers will have a seamless user experience when searching, selecting and buying their railway services, including first- and last-mile transport. They will have access to simple, reliable and comprehensive online information regarding timetables, prices, and ticket purchasing for (rail) transport services, both domestic (urban, regional, long-distance) and international. Tickets issued by different railways and ticket vendors will

[4] "CER Ticketing Roadmap", CER The Voice of European Railways, 30 September 2021.

be readily accepted throughout Europe. In the event of travel disruption, passengers will be able to easily obtain information on how to continue their journey, and on their passenger rights.

This will have to be done in a policy context that recognises how data exchange must continue to rely on voluntary contractual agreements and how the rights of data generators should be explicitly recognised in the EU framework on data governance. Data sharing should be based on a level playing field and the principle of reciprocity, while respecting the protection of trade secrets and intellectual property rights.

High-Speed Rail

Only 7% of the distance travelled by passengers in the EU is covered by rail. In order to offer a service that is comparable to aviation in terms of travel time, high-speed rail needs to be made available to European citizens. The Smart and Sustainable Mobility Strategy already sets ambitious targets in terms of the high-speed network: doubling high-speed rail traffic by 2030 and tripling it by 2050. With the current existing high-speed lines, it is not feasible to achieve such targets and double the high-speed rail traffic by 2030 and triple it by 2050. The TEN-T Regulation must promote climate-friendly alternatives like rail and the creation of a European high-speed network that is interoperable, links European capitals and major cities, connects urban nodes and airports and supports the development of international passenger services.

High-speed rail enables passengers to reach city centres rather than airports. For long distances, a high-speed passenger network would free up capacity for freight. Trains could therefore compete with flights on routes of up to 800 km, provided they run at a speed of at least 200 kmh. Flights between Milan and Rome fell by more than half after a high-speed rail line opened in 2007. Nearly 80% of traffic from London to Brussels and Paris has travelled by rail since 2019.

Rail's Energy Agenda: Hydrogen, Batteries and Electricity from Renewables

Due to the high degree of electrification, railways, as the existing green mode of transport, are able to offer almost zero-carbon train operations in Europe. The railway system makes it possible to power trains directly by renewable energy such as solar power. The EU electricity mix continues towards decarbonisation thanks to the carbon price under the EU Emissions Trading System. When combined with large-scale rail electrification, which is underway in accordance with the proposed TEN-T milestones of 2030 for the completion of the core network and 2040 for the extended core network, rail will help the EU to reduce both its imported fossil fuels and its carbon footprint.

The railway sector needs a fully fledged "cultural revolution" to remain a leading player and provide a sustainable transport system in Europe. Hydrogen-powered fuel cell trains (hybrid as bridge technology – hydrogen & battery) have the potential to help the railways in the EU achieve the EU Green Deal goals and overcome the challenges of the ongoing energy crisis. As a matter of fact, whilst it is imperative that railways reduce costs and improve performance in the short run, it is of vital importance that we explore the possibilities in new technologies that, in the longer term, can ensure that railways become increasingly cost-effective, while retaining the lead as the most environmentally beneficial means of powered transport.

Railway undertakings need commercial availability of reasonably priced renewably produced green hydrogen (e.g. reduction of the price of electricity and of the components for hydrogen production via electrolysis).

Two major tasks need to be accomplished before investments can be made in the construction of alternative fuel infrastructure for railways: the first is to achieve wider technical standardisation, and the second is to define safety-related requirements. Furthermore, a strategy has to be set to

increase fuel cell production rates and harmonise the standards applicable to trains and buses at the EU level. This should be done through unified technology standards, unified vehicle interfaces for electricity supply and unified data protocols to support the transition to carbon-free mobility solutions. Research should focus on hydrogen technology and also on batteries for railway applications, so as to increase efficiency. This should include locomotives, infrastructure vehicles and yellow machines.

Conclusion

Digitalisation will offer increasing opportunities to further reduce the environmental impact of our transport system, make collective transport more attractive and easier to use, and make mobility more efficient overall. The concept of Mobility-as-a-Service should lead towards effective multimodality and decreasing rates of individual vehicle ownership.

Collective transport solutions such as rail are of course more energy-efficient than private transport, thus making mobility and the whole economy more resilient to internal and external shocks, including geopolitical tensions and international disruption of energy supplies.

In parallel, European railways are pushing back the technological boundaries of their sustainability: new rolling-stock running on new and more sustainable fuels and making increasing use of electricity from renewable sources will enable the rail system to retain its current competitive edge of low externalities.

Of course, sectoral efforts will not be sufficient. New public policies and other forms of public support will be needed to make the system work.

The current revision of the Regulation on a Trans-European Network for Transport will have to give the Member States a clear set of objectives in terms of infrastructure upgrades, technical specifications and infrastructure development

– particularly when it comes to deploying ERTMS technology and developing a truly European high-speed network.

Financial support via the Connecting Europe Facility must also be secured beyond the current EU Multi-annual Financial Framework and must accompany the progress of the TEN-T project until its finalisation.

With regard to digitalisation and the specific topic of ticketing, European legislators must also recognise the efforts that are being made by the sector to find workable solutions towards the common objective of unleashing the full potential of seamless multimodal mobility. Any external imposition of technical standards or data ownership constraints will foster a sub-optimal ticketing market, where digital gatekeepers could easily abuse their dominant position in the European digital market.

At the same time, urgent policy actions are needed on many fronts to correct uneven intermodal competitive conditions: international air travel is VAT-exempt, whereas rail tickets are not; rail is subject to ETS, whereas the road sector is not and airlines are allocated free allowances; rail operators are charged for every single kilometre of line their trains run on, but the same does not apply to road charging. Last but not least, the social conditions of transport workers vary greatly across modes.

At present, the EU railway sector directly employs more than 1 million people and generates an economic value of over €79 billion. When taking indirect economic effects into account, the rail transport sector supports approximately 2.3 million jobs and generates a total of €170 billion. This corresponds to 1.3% of EU GDP. Furthermore, railways provide secure jobs and the sector is constantly giving rise to new opportunities to hire young people.

The positive spillovers of rail growth are clear, and find expression in a stronger economy and a more cohesive society, as much as in the fight against global warming. In today's world, it would be both irresponsible and self-defeating to overlook the transformative role to be played by railways.

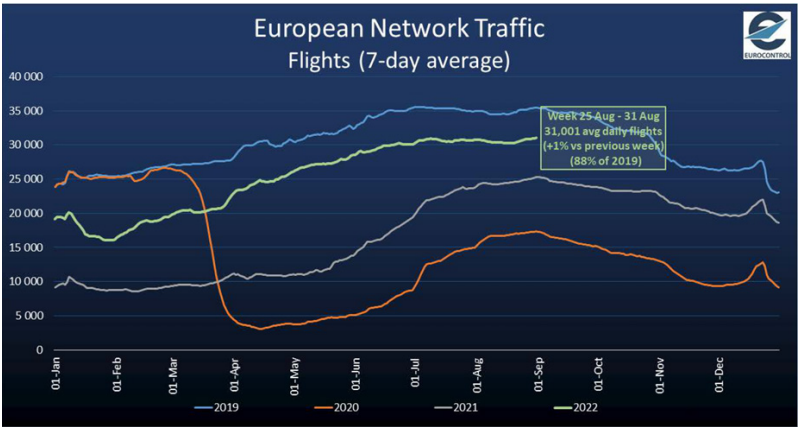
10. Digitalised and Sustainable Infrastructure for Air Traffic Management

Andrew Watt

Air Traffic Management (ATM) exists to ensure the safe and expeditious flow of aircraft, and is essential to the safety, capacity, efficiency and sustainability of the aviation industry. It relies to its core on the expertise, knowledge and dedication of its Air Traffic Control Officers, engineering, technical and administrative personnel.

In 2019, European Air Navigation Service Providers (ANSPs – who provide air traffic control) handled more than 11 million flights, reaching a record 37,228 flights on Friday, 24 June. Less than 12 months later, daily air traffic in April 2020 was barely above 2,000 flights, as Europe locked down to combat the Covid-19 pandemic. Air traffic has recovered in fits and starts and is approximately 12% below what it was in 2019, averaging 31,000 flights per day in August 2022 (Figure 10.1).

Fig. 10.1 - Annual daily flights in EUROCONTROL Network Manager area 2019-22



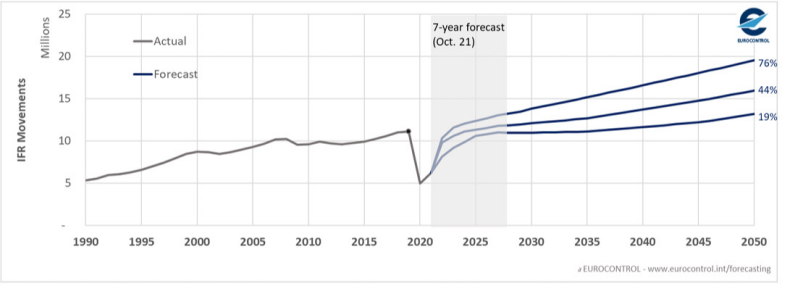
Some of the states with the largest shares of traffic sit at levels between -6% and -21% compared to 2019, whereas Greece has shown a strong rebound to +10% and Turkey only shows a loss of -1%. In eastern Europe, however, the pandemic effect on air traffic has been compounded by the unprovoked Russian invasion of Ukraine. Not only has Ukraine lost 100% of its commercial traffic, but its neighbouring states are also feeling the effects such as Latvia, Finland and Moldova, with traffic down by as much as -38% in Latvia's case. Paradoxically, as traffic flows have had to be reconfigured – and supported by strong growth in certain segments of the market, traffic in the upper airspace (generally above 24,500 feet) is now actually higher than in 2019 in a number of areas, especially in central Europe and across the Mediterranean.

The pandemic is expected to have a long-term impact on air traffic. EUROCONTROL's recently published *Aviation Outlook 2050*,[1] contains traffic and emissions forecasts out to 2050. It concluded that ten years' worth of traffic growth could be "lost"

[1] EUROCONTROL, "2050 air traffic forecast showing aviation pathway to net-zero", April 2022.

due to Covid's impact, in comparison to EUROCONTROL's previous long-term traffic forecast, which predicted in 2018 that the traffic now foreseen for 2050 would have occurred by 2040. The traffic levels of 2019 are not expected to be equalled until the middle of the current decade, with growth being somewhat anaemic thereafter in comparison to previous decades (Figure 10.2).

FIG. 10.2 - EUROCONTROL FLIGHT FORECAST WITH TOTAL GROWTH 2019-2050



ECAC	IFR Flights						
	2019		2050			2050/2019	
	Total (million)	Avg. daily (thousands)	Total (million)	Avg. daily (thousands)	Extra flights/day (thousands)	Total growth	AAGR
High scenario	11.1	30.4	19.6	53.6	23.2	+76%	+1.8%
Base scenario			16.0	43.7	13.4	+44%	+1.2%
Low scenario			13.2	36.2	5.8	+19%	+0.6%

(IFR - Instrument Flight Rules, which cover normal commercial passenger and cargo operations)

The recovery in traffic is patchy. Some airlines, such as Ryanair (+15%) and Wizz Air (+19%), and some cargo and regional carriers are operating above August 2019 levels, but most are not, especially the legacy carriers.[2] Airlines and airports are struggling to find personnel, forcing airlines to modify their schedules over the summer season. The ATM system, also experiencing

[2] EUROCONTROL, "Comprehensive Aviation Assessment, 1 September 2022.

personnel shortages, must cope with this increased volatility, but it needs to become more resilient as demand ticks up.

It was not possible, for example, to stop or resize ATM during the pandemic. Despite the collapse in the number of flights, the entire European ATM system had to provide the public service that is its core mission. Aircraft carrying the precious cargo of Covid vaccines had to fly when and wherever needed, and thus the system had to remain "on" at all times. Airlines could reduce staff numbers and were able to store unused aircraft, but ATM was not very scalable in comparison – obliged to operate a system that can accommodate over 37,000 flights in a day but handling just 5% of that.

ATM is financed through the recovery from airspace users of the costs incurred by ANSPs to provide air traffic control, aeronautical information and aviation meteorological services. Despite the recovery in traffic, approximately 8% less income than in 2019 has been processed back to ANSPs through the EUROCONTROL route charges mechanism this year; parity with 2019 income was only reached in July 2022. This shortfall will impact ANSPs' ability to sustain capital expenditure at pre-pandemic levels.

In parallel, the pressure on the entire aviation industry to reduce its carbon footprint will intensify as the effects of climate change become clearer. ATM is not immune and is similarly under continuous pressure to increase its efficiency over time.

Digitalisation is the key to improving the efficiency of how our ATM system operates, so that we meet our performance targets while building resilience through flexibility and scalability to cope with crisis situations. Introducing new technologies will also improve the way aircraft fly through airspace, reducing fuel burn and emissions on a flight-by-flight basis. It will also lead to a reduction in the energy required to power the ATM system. Digitalisation is thus a key component of aviation meeting its decarbonisation commitments and achieving net zero CO_2 emissions in 2050.[3]

[3] Destination 2050 – A Route to Net Zero European Aviation, published by

Digitalisation

ATM is a technology heavy industry and works on decades-long investment horizons. This is expressed in the European ATM Master Plan, whose ambitious objectives foresee a transition towards the "Digital European Sky" through investing €25-53 billion in the period 2012-50, of which 80% would be invested by 2035.[4]

Digitalisation allows observation – that is, monitoring of performance – and then modification by reprogramming digital equipment to improve operational performance. It works best when everything is connected to a network. Currently ATM deploys external networks to monitor performance, rather than in-built performance monitoring, which is what we wish to move towards. Digitalisation allows for faster reactions and more agility, providing the basis for new digital services.

ATM's digital transition covers the gathering, processing, transporting, sharing and publication of data, as well as the introduction of new, more efficient ground equipment and software-defined radios on-board aircraft. Digitalisation is already happening at pace and is underpinned by three continent-wide programmes covering research, deployment and operations: **(i)** the Single European Sky (SES) ATM Research programme that prepares for the future, **(ii)** the SESAR Deployment Programme established to implement what comes out of the research pipeline, and **(iii)** the "iNM" programme of EUROCONTROL's Network Manager that will replace the operational systems used to organise the flow of traffic through our skies and airports. Three initiatives are highlighted here to illustrate the change: SWIM, NewPENS and iNM.

Airlines for Europe (A4E); Airports Council International (ACI) EUROPE; AeroSpace and Defence Industries Association of Europe (ASD); Civil Air Navigation Services Organisation (CANSO); and European Regions Airline association (ERA), February 2021. Downloadable here https://www.destination2050.eu/

[4] European ATM Master Plan 2020 – Executive View, p. 118.

System-Wide Information Management, or SWIM, is one of six "ATM Functionalities" (AF) within Common Project One (CP1)[5] that is under the responsibility of the SESAR Deployment Manager (SDM). A Common Project is an extraction from the European ATM Master Plan and binds the Member States of the European Union and their operational stakeholders.

SWIM provides the means for the sharing of information. EUROCONTROL has been at the forefront of developing global SWIM standards, through the United Nations' International Civil Aviation Organisation. At an airport, for example, SWIM allows all relevant actors to know when an aircraft is going to land and when it will arrive at the gate. This allows ATC, the airline, the ground handling agents and the airport operator to ensure that all relevant services are forewarned of and prepared for the aircraft's landing, taxiing to and arrival at its gate, covering stand allocation and deciding which taxiway to allocate from runway to stand, as well as passenger disembarkation, aircraft refuelling, cabin cleaning, catering, customs and passport control as necessary, and of course the introduction of a new crew as required.

NewPENS – the digital network for the transport of data throughout the ATM system – is an ultra-resilient IP network for exchanging critical and common aeronautical information reliably, securely, and safely in a cost-efficient way. Its architecture guarantees an increased level of end-to-end control and authority, connecting over 100 locations in 47 countries. It operates with 99.999% availability and includes elaborate cyber-security precautions. It will evolve to meet business needs, providing the backbone on which more SWIM applications will run. NewPENS is supported by a service desk at EUROCONTROL.

[5] CP1 was established to support "effective ATM modernisation, which requires the timely implementation of innovative ATM functionalities, based on technologies that increase the levels of automation, cyber-secure data sharing and connectivity" (Commission Implementing Regulation (EU) 2021/116 of 1 February 2021).

Although EUROCONTROL has been at the forefront of developing SWIM and NewPENS together with the community of ATM stakeholders, we are also experiencing considerable digital transformation ourselves. At the heart of this is the "integrated Network Management" (iNM) programme to replace our core systems which have been successfully ensuring the safe and efficient flow of aircraft across the European airspace every single day, for over 25 years. A whole set of digital and manual processes are in place involving hundreds of airlines, over 40 states and ANSPs, and hundreds of airport operators, with the goal of agreeing how traffic flows will be organised on any given day, considering weather, strikes, military conflict, major sporting and cultural events, as well as seasonal variations in demand.

The iNM programme will deliver a range of innovative digital products enabling EUROCONTROL to maximise the efficiency, safety and sustainability of the European aviation network through a new generation of cutting-edge, resilient and scalable operational systems. The incremental renewal of all of NM's main operational systems will be achieved by 2030, resulting in a new digital architecture enabling NM to deliver ever more integrated business services and products to its stakeholders.

These three initiatives demonstrate the scale of ATM's digital transformation at a macro-level. But at more granular levels, digitalisation is having a profound impact, and the following section looks at this from the perspective of Communications, Navigation and Surveillance (CNS).

Key CNS-Related Deployment Activities

Communications, Navigation and Surveillance together form the central nervous system of ATM. CNS "senses" where aircraft are, the direction in which they are heading, how far they are from their destinations, how high they are flying, whether they are climbing or descending and, critically, if there is any risk of

aircraft coming too close to one another. Data from ground-based, space-based and on-board navigation equipment are combined in an aircraft's flight management system to guide the aircraft. Information is delivered to pilots and controllers in real time so that their situational awareness is always up to date. Our CNS infrastructure has to evolve to meet the safety, capacity, cost-effectiveness and sustainability challenges posed by growing traffic demand. This section highlights several key CNS developments where digitalisation is making a difference.

Communications – Datalink and Future Communications Infrastructure

Datalink is akin to an SMS between Air Traffic Control Officers (ATCOs) and pilots. It complements traditional voice messaging and improves the chances of instructions and acknowledgements being correctly transmitted and received. It is specifically tailored to ATC needs and reduces workload, boosting safety, capacity and efficiency. Although voice communication will always be available, we also see the potential in the emerging Speech-to-Text (STT) technology, driven by Artificial Intelligence, to further digitise controller-pilot communications.

Datalink equipage is required under a 2009 EU law.[6] However, datalink services have already evolved beyond its scope, driven by more sensors becoming available on-board aircraft, enabling provision of new ATM and airline services. There is a concerted drive to automate ATC – the Digital European Sky – to cope with an estimated fourfold increase in air-ground communications demands. Airlines' operational communications (AOC) requirements are also growing

[6] Commission Regulation (EC) No 29/2009 of 16 January 2009 laying down requirements on data link services for the single European sky. It applies to all flights operating as "General Air Traffic" in accordance with instrument flight rules within airspace above Flight Level 285 (FL285 = 28,500 feet). It also applies to air traffic service providers providing services to general air traffic within that airspace.

relentlessly, as more aircraft data are streamed to airline operations centres and into "digital twins". A seven-fold growth in throughput is anticipated.

As both ATC and AOC services use the same Datalink technology, it is being pushed to its limits. At some point in the near future it will not cope, which is why the SESAR Future Communications Infrastructure (FCI) project is now of vital importance.

The FCI Business Case estimates that a lack of ATC datalink capacity costs an estimated €1-1.3 billion annually. The new technologies considered under FCI would provide extra *data* capacity that would allow ATC to boost *airspace* capacity by 11%, enabling the introduction of four-dimensional trajectory management, further improving flight efficiency, and reducing fuel burn and greenhouse gas emissions per flight.

Over 8,500 aircraft would have to have FCI equipment installed by 2029, if 2019 traffic levels are reached in 2024. This subset of the overall fleet represents the aircraft operating 85% of the flights above 28,500 feet – which is the threshold for benefits to kick in. Retrofitting existing aircraft for FCI would accelerate the accrual of benefits and expand the overall benefit pool. Airlines are reluctant to retrofit, unless mandated, but targeted incentives could potentially spur airlines into action.

The industry is converging on "Multimode/multilink" technologies to cover the following FCI equipage options: the new L-band Digital Aeronautical Communications System (LDACS); off-the-shelf technologies that will come on stream in the short-medium term such as new commercial satellite communications constellations (which may not provide services in protected aviation radiofrequency spectrum); and the next generation of Satellite Communications (SATCOM NG). The multilink concept will enable the seamless management of these digital datalink technologies.

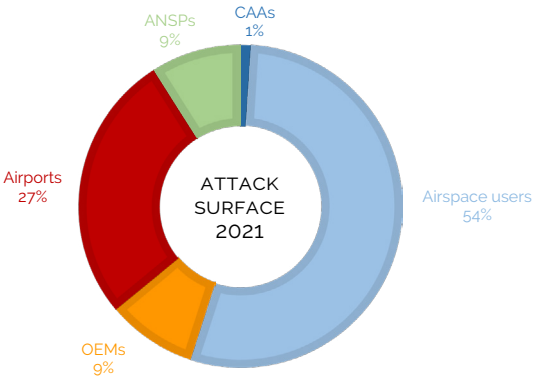
Cyber Security / Public Key Infrastructure (PKI)

Aviation is subject to cyber-attacks. With digitalisation, this risk increases. Entities linked to ATM increasingly need to ensure that greater interconnectivity can be delivered in a secure, resilient and trustworthy manner. The Network Manager already monitors cyber security breaches and brings them to the attention of its stakeholders through its Computer Emergency Response Team (CERT) service. CERT's latest annual report noted that the level of maturity associated with improved means to detect and analyse cyber-events had increased, contributing to more cyber-attacks being reported; this does not mean that the number of attacks has increased.[7] Nevertheless, with increasing automation and digitalisation, cyber security measures will become more important, requiring more sophisticated methods almost certainly based on AI.

In 2019, 200 cyber security "events" were reported by CERT, followed by 1,260 in 2020, and 2,165 in 2021, by when approximately 2.5 aviation-related entities fell victim to a ransomware attack per week versus just over one per week in 2020 (119 and 62 respectively). Airspace users remained the main target of cyber-crime attacks in 2021, mostly through fraudulent activities aimed at stealing money or data. The focus of attacks across the industry is shown below.

[7] EATM-CERT 2022 report on cyber in aviation, June 2022, Classification: TLP-GREEN.

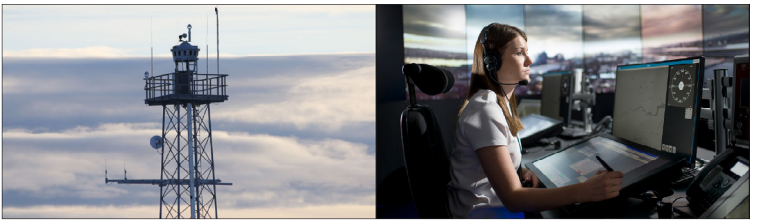
Fig. 10.3 - Distribution of cyber-attacks in aviation



Because SWIM is at the heart of the digitalisation of ATM, it needs to be secured against cyber-attacks. The purpose of a public key infrastructure (PKI) is to facilitate the secure electronic transfer of information for a range of activities on a network. EUROCONTROL and the SESAR Deployment Manager are therefore developing a new service under Common Project One's ATM Functionality 5 to ensure that stakeholders' data and information are transferred securely as sending/receiving parties are identified and authenticated, using a PKI. It will be used where the identities of counterparties involved in the communication and the information transferred must be ensured.

Remote air traffic control towers for airports

The airport tower is arguably the object most readily associated with air traffic control. Thanks to digitalisation, it is now possible to install "remote towers", which allow aerodrome Air Traffic Control and Flight Information Services to be provided from a remote location, while maintaining an equivalent level of operational safety.



Saab on-site camera tower, Sälen
© Saab

London City Digital Tower
© NATS

At Brindisi Airport, ENAV[8] inaugurated its first remotely managed control tower,[9] in June 2022. Air traffic controllers can manage take-off, landing and ground operations from a Remote Tower Module (RTM) located many kilometres from the airport. The exact replication of the 360° panorama visible from a traditional control tower is ensured by 18 fixed cameras whose images are combined on 13 high-definition monitors positioned inside the digital tower. Camera images and other data are integrated into a synthetic view emulating what would be seen in situ. This ensures the accurate detection and traceability of moving objects and vehicles. Air traffic controllers have a better view and use a series of supporting tools for air traffic management, thereby increasing safety and operational efficiency.

Similar developments are taking place at an increasing number of European airports, ranging from London City to remote airports in Sweden. Efficiency gains are particularly attractive when the management of several remote towers can be performed in a single operational centre. An additional benefit is that remote towers have been estimated to consume roughly 70% less electricity than a conventional aerodrome tower.[10]

[8] Ente Nazionale del Assistenza al Volo, Italy's provider of air navigation services.
[9] Enav, "First Remote Digital Tower in Italy Was Inaugurated in Brindisi", 13 June 2022.
[10] EGIS Avia, "Control towers that grow back greener", 9 February 2021.

Artificial Intelligence

The application of Artificial Intelligence (AI) is another example of digitalisation in ATM. EUROCONTROL operates the Maastricht Upper Area Control Centre (MUAC) which manages the upper airspace (from 24,500 to 66,000 feet) above Belgium, the Netherlands, Luxembourg and north-west Germany – one of Europe's busiest and most complex airspace areas. MUAC is Europe's only cross-border civil-military air navigation service provider, building its services around traffic flows rather than national borders.

MUAC's Traffic Prediction Improvements (TPI) project has successfully introduced its own AI algorithms to its integrated Flow Management Position, to reduce uncertainties in trajectory predictions by extracting hidden patterns in historic data. This allows more accurate sector workload predictions and more optimal flow measures. A sector is the volume of airspace under an air traffic controller's responsibility.

MUAC uses AI to predict the actual flight route of an aircraft prior to its entry into MUAC airspace. The route flown can deviate substantially from that planned. The AI algorithm has been in use for 10-15% of MUAC's overall traffic since 2018. It has proved resilient to system changes such as the introduction of new flows or even the global pandemic. This functionality was developed jointly with colleagues from the EUROCONTROL Innovation Hub in Brétigny, South of Paris.

MUAC has also introduced AI to improve its operational performance in four-dimensional trajectory predictions, including recognising "slow climbers" and estimating when and where these aircraft will enter the airspace compared to their flight plans. This helps to pinpoint future zones of flight interactions to which probabilities can be assigned, helping controllers to take mitigating action in advance. AI is also used to improve the prediction of take-off times and so-called "sector skips" when one controller hands an aircraft over from her sector to another controller's sector, but not in the predicted geographical sequence.

Urban Air Mobility, Unmanned Air Vehicles (UAM/UAV) & Drones

The Drone/UAM industry is arguably on its way to achieving early commercialisation. Private investment has been pouring into manufacturing of eVTOL[11] aircraft, with some well on their way to early certification for manned operations (around 2024-25).

The UAM eco-system is as strong as its weakest link – and that is the lack of investment in the physical and digital infrastructure required to fly UAVs and drones in scalable and complex environments. It is only within a digitalised system that we have the possibility of managing a huge number of these new airspace entrants whose interactions risk being highly complex.

"U-Space" is a set of new services relying on a high level of digitalisation and automation of functions and specific procedures, supported by Artificial Intelligence, designed to provide safe, efficient and secure access to airspace for large numbers of unmanned aircraft, operating automatically and beyond visual line of sight.[12] This will accelerate the move of aviation from a human-centric towards an information-centric system.

U-Space, as an unmanned aircraft traffic management solution, will allow the scaling up of the volume of complex drone operations, in environments that are challenging, such as urban areas, or close to airports. Securing public and private investment will require the development and demonstration of fully operational use cases to understand the risks and opportunities presented by the UAM industry.

USpace4UAM, for example, is a large-scale U-Space demonstration project sponsored by the SESAR Joint Undertaking, whose objective is to build confidence in a safe and orderly integration of UAM into everyday air traffic.[13]

[11] Electric Vertical Take-Off and Landing (eVTOL).

[12] European Commission, U-Space, Rolling Plan for ICT Standardization.

[13] SESAR, LARGE SCALE DEMONSTRATIONS PROJECT. Uspace4UAM.

Five demonstration campaigns have already been held in four countries (Czech Republic, Poland, Spain and the UK) covering flights of both drones and eVTOL vehicles in multiple operational scenarios to mimic tailored business use cases.[14] USpace4UAM has helped to mature the technology needed for higher levels of automation and autonomy in UAM operations.

In Sweden, a number of municipalities have come together to develop UAM infrastructure in their cities and regions. They are looking for a "Bus Stop" concept where they connect remote settlements in Northern Sweden with drones flying short distances for cargo delivery, postal delivery, inspection, and surveillance purposes. Passenger transport using UAVs is not yet being considered.

In the UK, the CAELUS project's goal is to "develop a national distribution network to use drones to transport essential medicines, blood, organs and other medical supplies throughout Scotland including to remote communities".[15] One objective is to create the physical and digital infrastructure to support operations, involving the UK's National Air Traffic Services (NATS).

Reducing the Carbon Footprint of ATM/CNS Ground Infrastructure

We are also looking at how to decarbonise the ground infrastructure of air traffic control centres, airport towers, CNS equipment, offices and other ground facilities. A EUROCONTROL Think Paper[16] estimated that Europe's ATM infrastructure consumes approximately 1,140 GWh of

[14] U-Space, *Demonstrating the Everyday Benefits of U-Space. Initial results from SESAR demonstrations (2020-2022)*, European Union-Sesar, 2022.

[15] Care & Equity - Healthcare Logistics UAS Scotland (https://www.agsairports.co.uk/drones).

[16] EUROCONTROL, "Think Paper #13 - Greening European ATM's ground infrastructure", 29 September 2021.

electricity annually, generating an estimated 311,000 tonnes of Scope 2 CO_2 emissions.[17] If all that electricity generation could be decarbonised overnight, then almost 6.2 million tonnes of CO_2 could be saved through to 2050.

ANSPs in Austria, Belgium, Denmark, France, Germany Italy, Switzerland and the UK are reducing their carbon footprints through cloud computing, improved cooling at data centres and the renewal of facilities with more modern and energy efficient equipment. They are moving onto renewable energy contracts, and developing local renewable energy solutions for their facilities, involving solar power, wind turbines and hydrogen fuel cells. Digitalisation, once again, is at the heart of these initiatives.

Several ANSPs are now close to operating as net-zero organisations. ENAV has committed to renewable energy for over 95% of its needs by the end of 2022 and is installing solar power at a mix of remote, airport tower and office facilities. At some locations it may be possible to produce more energy than required, further helping to offset the aviation industry's emissions. The UK's NATS has set climate targets that have been independently validated by the Science-based Targets Initiative,[18] and has twice been recognised as a "climate leader" by the *Financial Times*.[19]

Many of the 6,000 or so CNS ground facilities are located at remote sites, relying on diesel generators for either primary or back-up power. There is scope for developing and deploying off-grid renewable energy installations at these facilities. This has tentatively started with experimental installations in France (Figure 10.4) and Italy, with digitalisation playing a key role in managing power generation and usage.

---

[17] Based on per country average carbon intensity of emissions per kWh of energy produced, using data published by the European Environment Agency.

[18] NATS, "NATS achieves highest science-based validation on net zero target", 14 July 2022.

[19] N. Hawcock, "Europe's Climate Leaders 2022: interactive listing", *Financial Times*, 12 April 2022.

Fig. 10.4 - Sarlat-la CANEDA radio antenna renewable energy emergency power supply

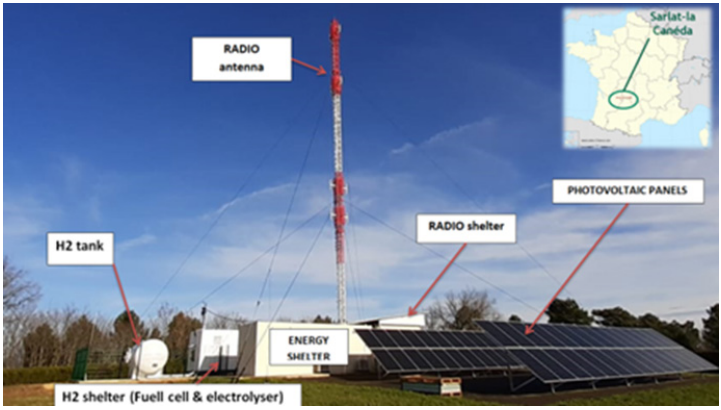


Photo courtesy of DSNA, France

Conclusion

ATM is digitalising rapidly. The introduction of new technologies is key to improving efficiency, capacity and resilience, facilitating better fuel efficiency and less greenhouse gas emissions per flight, and reducing the energy consumption of ATM's ground infrastructure. Through digitalisation, ATM will be able to accommodate the many new airspace entrants currently under development, whose operations will open up new services to businesses and consumers. Change is indeed coming rapidly to an historically conservative industry, but all the signs are that, thanks to digitalisation, ATM will maintain its high levels of safety and service for both its traditional and new customers.

11. Technology and Digitalisation in Maritime Freight and Ports: A Game Changer?

Oliviero Baccelli

The maritime and logistics industry is often considered a traditional industry, more reactive than proactive, mostly due to the long asset cycles involved in shipping and port infrastructure. Over the past decade there has been a shift, mostly driven by the high investments of global players in the container sector, but also by collaborations between port authorities and technology providers, towards a more innovative portscape.

Automation, digitalisation and energy transition are the main drivers of changes that redefine the competitive landscape in maritime and port industries.

The acceleration of the implementation of new technologies and digitalisation is due to infrastructural, organisational and political reasons and it requires a major upskilling of the supply chain workforces.

High financial and environmental costs cause considerable difficulties in building new port and hinterland infrastructures, thus promoting higher efficiency in usage of existing port infrastructures through the implementation of new technologies.

Containerisation is one of the prime examples of such technological development, which transformed the maritime and logistics industry over a relatively short time-span. Containerisation also contributed to the automation of port terminals, although fully automated container terminals do

not yet exist. According to ITF-OECD data, in 2022, across the world, only 53 container terminals are now automated to a certain degree. This represents around 4% of global container terminal capacity. Most automated systems are deployed in the container yard. Only a few terminals have automated the transport between quay and yard. No terminal has completely automated quay cranes. Container terminal automation appears to offer benefits only under certain conditions and thus for a limited group of terminals. Container terminals that face a relatively stable market with guaranteed throughput are more suitable for high levels of automation because of their regular cargo flows. In contrast, terminals with fluctuating throughput are better served by less automation as this maintains greater flexibility. Container volumes are more volatile in transhipment terminals, so more flexibility and low levels of automation are advantageous. Gateway terminals, by contrast, generally have a certain level of captive container volumes, so they tend to be more suitable for automation. Consolidation of carriers, the market power of alliances and the rise of mega-ships have increased peak loads, volatility of cargo flows, and transhipment. These developments require terminals to be more flexible to assure ship-to-ship connections. They make the case for automation less convincing and flexible arrangements for port labour more appropriate, provided enough labour is available. Increasing vertical integration between port terminals and shipping companies and new forms of agreement to share productivity gains with workers will facilitate the introduction of automation in high-wage contexts in the years to come.

According to an International Transport Forum (ITF) study entitled "Container Port Automation Impacts and Implications" (2022), governments have taken divergent positions on port automation. Several governments have formulated strategies on maritime innovation or maritime clusters, of which port automation forms a part. For example, the 2030 Port Policy and Implementation Strategy of the South Korean government focuses on the establishment of a smart logistics system, which

includes port automation. China's 13th five-year plan (2016-20) promotes the development of smart ports, which includes automation to improve productivity. For some governments, the focus is the safety of workers. In most cases, government strategies and the preferences of port authorities are aligned. Some governments, however, are more concerned about possible job losses related to port automation, which has resulted in legislative action to restrict port automation projects in some US states. In February 2021, for instance, the Senate of the State of Washington adopted a new law, Engrossed Senate Bill 5026, stating that: "moneys available to a port district or a port development authority shall not be used to purchase fully automated marine container cargo handling equipment". While the new law eliminates purchases of automated equipment by a "port district or a port development authority", that does not necessarily prevent purchases by port tenants such as the operator of a terminal. Therefore, the bill does not ban port automation but intends to make sure that port automation projects are not facilitated by federal or state subsidies.

Moreover, interest in autonomous and remote-controlled ships is growing fast. Enabled by recent developments in sensor technology, connectivity at sea, and analysis and decision support software and algorithms, the first commercial projects are ready for launch in the near future. The field is a wide one, with many different automation applications and concepts that could benefit the maritime industry. From completely unmanned ships to vessels controlled remotely from land-based virtual bridges, and support systems that give crews advance warning of impending collisions or help to optimise operations. In Norway, government agencies and industry bodies established the Norwegian Forum for Autonomous Ships (NFAS) to promote the concept of unmanned shipping. Since 2021 the Norwegian fertiliser company Yara has been carrying out the first pilot project with an autonomous and electric container ship of 120 TEU capacity named Yara Birkeland. On completion of the pilot project in 2024, the

zero-emissions vessel could set the standard for future short sea shipping. With no need for fuel or a crew, the ship will save up to 90% in annual operating costs compared with similar-sized conventional vessels.

The need for greater transparency towards users and stakeholders, and better control of health and safety, are two other reasons for the acceleration of the implementation of new technologies and digitalisation in the sector. The acceleration of digitalisation of the logistics chain to increase national logistical competitiveness by creating an interoperable digital system between public and private entities for the transport of goods is also a main component of the strategies indicated by the Next Generation EU Programme. For instance, the Italian Ministry of Infrastructure and Sustainable Mobility allocated a specific amount of 250 million euros tor this goal in the Italian National Recovery and Resilience Plan.

Thanks to Automatic Identification Systems (AIS), for instance, everyone is aware of a ship's location, route, speed and cargo. DCSA, the Digital Container Shipping Association established in 2019 by MSC, Maersk, CMA CGM, Hapag-Lloyd, ONE, Evergreen, Yang Ming, HMM and ZIM, is another example. DCSA is currently developing standards and a platform to optimise just-in-time port calls of vessels, promoting a harmonisation of data to streamline timely communication between supply chain stakeholders, with an initial focus on minimising ballasting and waiting times. The final goal is to better coordinate worldwide scheduling of port calls, in order to make slow steaming possible and to increase sustainability. The long-term result could be a practically perfect logistics chain and safe, rapid and traceable door-to-door cargo flows. Another example is 5G-enabled IoT solutions that are being implemented in a variety of terminals and wider port areas. Driven by faster 5G communications, large numbers of sensors are placed on several assets to increase safety and operational awareness. Examples include the tracking of heavy machinery and worker location, tracking of exact vessel locations for quay

wall planning and protection, and smart camera systems for terminal and port access (digital ISPS - International Ship and Port Facilities Security Code).

In the shipping sector, fouling is a major issue for vessels both with regards to maintaining optimal operational speeds and reducing drag through the water. Multiple companies have recently started to work on remotely operated underwater drones that inspect the hull underwater and keep it free from fouling. These types of innovations help high-frequency ships maintain their schedules (RoPax, cruise ship) and help vessels cut their overall fuel consumption and emissions.

Digital infrastructure, mainly in the form of Port Community Systems (PCS), enables smooth data exchange and increased productivity in the maritime and port sector. A PCS enables the intelligent and secure exchange of information between public and private stakeholders by enabling a single submission of data, which becomes available for (selected) third parties to optimise, manage and automate port and logistics processes (e.g. documentation for exports, imports, hazardous cargo, ship manifest information, port health formalities and maritime statistics reporting). Digital infrastructure is therefore aimed at eliminating unnecessary paperwork that can cause delays in cargo handling, improving security, reducing costs and enhancing environmental sustainability, thanks to the reduction of emissions due to better utilisation of assets (e.g. less empty trucking). A PCS also has the ability to act as a National Single Window or to integrate into a National Single Window and is therefore pivotal in the Single Window concept by reducing duplication of data input through the efficient electronic exchange of information. An example is NxtPort, which is a data-sharing platform in the Port of Antwerp. NxtPort collects and shares data across a number of players (including shippers, forwarders, ship's agents, carriers, terminals and insurance brokers, among many others) in order to increase participants' operational efficiency, safety, and revenue. Another example is TradeLens, a new company owned 51% by Maersk and 49% by

IBM. This digital joint venture was created at the beginning of 2018 with the aim of providing a platform connecting a large number of stakeholders in the industry, thereby covering each stage of the transportation process from shippers to ports and terminals, and national authorities. TradeLens is an open and industry-neutral platform aimed at maritime companies based on blockchain technology. The platform aims to make global trade safer and more efficient.

The complex process of achieving net zero emissions in the shipping industry by 2050 is another driver of modernisation of the sector through new technologies and digitalisation. The process is guided by the policy indications of the International Maritime Organisation (IMO)[1] and the European Commission. In particular, new environmental requirements and legislative frameworks have recently entered into force, turning some of the proactive, bottom-up, environmental commitments made by ports into top-down requirements.

The Alternative Fuel Infrastructure Directive[2], the new Port Reception Facilities Directive[3], and the EU Sulphur Directive[4] are examples of this that have already been implemented at EU level. In September 2020, the European Commission adopted a proposal to cut greenhouse gas emissions by at least 55% by 2030 and put the EU on a responsible path to becoming climate-neutral by 2050. To achieve climate neutrality, a 90% reduction in transport emissions is needed

[1] Targets by the IMO are set to reduce carbon intensity of international shipping by 40% by 2030, and 70% by 2050 (compared to 2008). Moreover, the total annual GHG emissions need to be reduced by 50% compared to 2008 across international shipping. As an example, the "IMO 2020" rule limits the sulphur content in fuel oil and resulting in ships needing to use very low sulphur fuel oil (VLSFO) to comply to the new limit.

[2] Directive 2014/94/EU of the European Parliament and of the Council of 22 October 2014 on the deployment of alternative fuels infrastructure.

[3] Directive (EU) 2019/883 of the European Parliament and of the Council of 17 April 2019 on port reception facilities for the delivery of waste from ships.

[4] Directive (EU) 2016/802 of the European Parliament and of the Council of 11 May 2016 relating to a reduction in the sulphur content of certain liquid fuels.

by 2050. All transport modes, including maritime transport, will have to contribute to the reduction efforts and therefore in July 2021 the European Commission presented a proposed Regulation, designated FuelEU Maritime (COM(2021) 562 final), on the use of renewable and low-carbon fuels in maritime transport and amending Directive 2009/16/EC.

FuelEU Maritime is part of the "basket of measures" designed to address emissions from maritime transport, while maintaining a level playing field. It is fully consistent with other measures presented as part of the "Fit for 55" package and builds on existing policy tools such EN 3 EN as Regulation (EU) 2015/757 of the European Parliament and of the Council[5], which establishes an EU system to monitor, report and verify (MRV) CO_2 emissions and other relevant information from large ships using EU ports.

The new legislative framework will enhance predictability by setting a clear regulatory environment for the use of alternative fuels in maritime transport, and stimulate technology development, by encouraging research, innovation and the development of new, advanced types of renewable and low-carbon fuels (RLF) for maritime transport.

The role of technological innovations is extremely important in a market context that do not allow to highlight univocal solutions. The foreseeable scenarios involve a fuel market composed of bio-fuels, liquefied natural gas, electric batteries and hydrogen derivatives such as ammonia and methanol for ships and a more limited mix for port vehicles and the transport of goods to and from ports, also implying a major boost to the modal shift from all road to rail intermodality.

The energy transition will have many direct and indirect effects on the technology used in the maritime and port sectors, because the global decarbonisation agenda is shaping

[5] Regulation (EU) 2015/757 of the European Parliament and of the Council of 29 April 2015 on the monitoring, reporting and verification of carbon dioxide emissions from maritime transport, and amending Directive 2009/16/EC (OJ L 123, 19.5.2015, p. 55).

sectors and industries, and there is a growing trend towards more circular, renewable and locally focused economies. Many seaborne trade volumes are likely to continue growing, but cargo volumes for large vessels transporting virgin materials or fossil fuels over long distances are set to peak within the next 10 years, according to a 2022 study by Danish Ship Finance analysts. Cargoes relating to fossil fuels currently account for roughly 40% of annual seaborne trade volumes. Seaborne trade volumes may increasingly shift towards smaller dry bulk volumes, containerised goods and Ro-Ro cargo. Therefore, decarbonisation of the global economy requires massive changes beyond fuels. More circularity may reduce inefficiencies and give rise to novel solutions that allow more economic activity using fewer resources and demand less transportation of virgin materials and fossil fuels.

The opportunities open to ports in the energy transition include cost savings, securing market share and attracting new cargo and industries, but ports will also have to face new challenges. These include securing funding, strategic planning of land use, regeneration of the areas used for fossil fuel bunkering, stocking and processing, complex operations, collaboration with stakeholders, dealing with technical uncertainty, the societal and political environment and organisation.

Ports will also play a facilitating role in greening the power sector. For instance, ensuring a sustainable and responsible roll-out of offshore renewable technology with respect to maritime and seaport activities is already a priority for most modern European ports. One example is the substantial investment required for adapting to the challenges posed by opportunities for promoting new supply chains in the renewables sector. Offshore windfarms need connections to grids, and the cables, especially seabed cables under the access lanes to and from ports, need careful planning. These developments should consider future needs in terms of port access, anchorage and potential fairway deepening. Moreover, investments in basic port infrastructure (which could also be used to improve the

infrastructure for overall trade) will be necessary to facilitate these types of projects (e.g. adapting quays and port access lanes to larger wind blades).

Ports will also play an important role in energy buffering. With the increased usage of renewable energy, more space for storage capacity will be needed. Many types of renewable energy, e.g. wind-energy, are dependent on an intermittent source. Storage capacity is needed to buffer the volatility of renewables. The port, as a future energy hub, has much potential to use its land as a buffer/battery area to supply the port and the nearby region with energy. This also applies to the re-use of steam from the industry located in the port and the storage of reusable feedstock.

The complex decarbonisation processes directly and indirectly affect demand for substantial new investments in technology and digitalisation, but also for new skills within the private and public port system, on three levels:

1. The new mix of energy carriers requires specific certifications and qualifications in terms of safety and fire prevention for the management of maritime, port, stocking and land forwarding operations;
2. The decision to track, offset and certify the carbon footprint of maritime and land transport requires new skills, in particular to support the most sustainable logistic solutions;
3. The management of new policy tools, such as the European Carbon Border Adjustment Mechanism, will require the management of "environmental duties" by the supervisory authorities, based on big data platforms and trade blockchain solutions.

The accurate identification of future labour-market needs is necessary for a long-term sustainable solution that will require the reform of education and training. Such reform must ensure that the workforce is "future-proofed" in two ways. First, training and education for each specific predicted workforce

expertise must be timely. Second, education and training must equip people with the motivation and ability to be extremely good at learning, re-learning, training and retraining, as often and as much as is needed.

In the maritime freight and port sectors, technology and digitalisation are a game changer only if they are widespread at all professional levels among all supply-chain stakeholders.

Resilience of the Maritime Supply Chain. Mobility and Transport Connectivity; Washington, DC.

12. The Role of Smart Grids for Sustainability

Pablo Gonzalez

Electricity networks are the backbone of a secure and reliable power system and play a critical role in energy transitions. Global investment in electricity networks (including sub-stations, switchgear, metering, digital infrastructure and electric vehicle fast-chargers) has amounted to around $300 billion annually in the last decade, with distribution networks accounting for two-thirds of investment. In addition, the role of smart grids has considerably increased, with growing shares devoted to the digitalisation and modernisation of electricity networks, which now account for more than 15% of total spending in electricity networks.

A smart grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end users. Smart grids co-ordinate the needs and capabilities of all generators, grid operators, end users and electricity market stakeholders to operate all parts of the system as efficiently as possible, minimising costs and environmental impacts while maximising system reliability, resilience, flexibility and stability.

A significant increase in electricity networks spending is required in the short term: the efficient deployment of a grid infrastructure in a timely manner is an essential prerequisite to the successful deployment of other elements of the power system such as variable renewable electricity capacity, storage

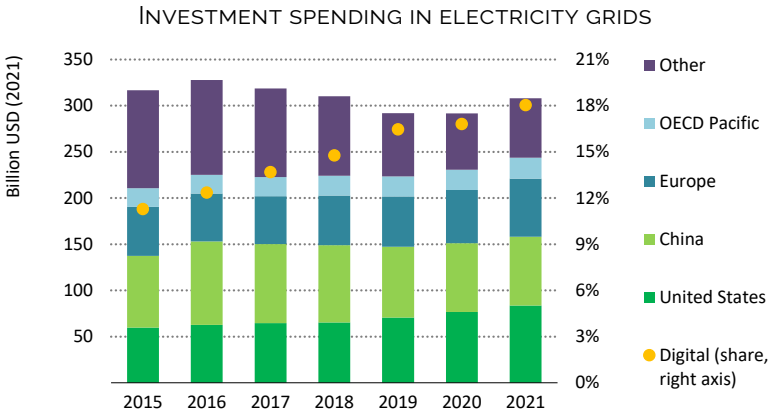
technologies and electric vehicle chargers. However, the current energy crisis, arising from the Covid-19 pandemic and the supply chain disruptions and inflationary pressures caused by Russia's invasion of Ukraine, has placed some network companies under strain, especially in Emerging Market and Developing Economies (EMDEs). This is likely to make it more difficult to finance future grid extensions and upgrades, putting at risk one of the most important enablers for the energy transition.

In this context, the International Energy Agency (IEA) provides a series of recommendations to governments, policymakers and private actors which could guide the investment boost required in smart grids, especially in climate-driven pathways.

State-of-Play

Investment in electricity grids is recovering, with more ambitious network plans to facilitate the electrification of the economy and the integration of renewables

Investment in electricity grids is set to continue recovering in 2022 after a strong increase in 2021, when capital expenditure rose by 6% from Covid-19-affected 2020 levels (the lowest in the last eight years). Advanced economies are leading the way in the electrification of the economy, and investment in these regions rose at a higher speed than elsewhere, accounting for more than 55% of grid spending in 2021 from around 43% in 2015. In addition, spending on electricity networks is being boosted by the fiscal support that governments are providing in response to the economic crisis caused by the pandemic. The IEA has tracked around $20 billion that is due to be spent on transmission and distribution directly by governments through to 2023, which, along with regulatory approval for new assets, is expected to mobilise around $225 billion from the private sector. This support has been boosted in 2022 with the release of the RePowerEU plan by the European Commision and the Inflation Reduction Act in the United States.



Note: Digital includes transmission and distribution automation, networking and communications, analytics (asset performance management, power quality and grid operations), smart meters, advanced distribution management systems, energy management systems, transmission line sensors, vegetation management, dynamic line rating and digitalisation of power transformers and substations.

Source: IEA analysis with calculations from Guidehouse (2022).

Investment in the United States is set to moderate after an increasing trend since 2013 (expenditure in 2021 was 80% higher than that in 2013). Network spending in the country has outpaced electricity demand growth, as increasing capital is devoted to replacing and upgrading equipment and strengthening structures against weather-related damage (only around 30% of investment was devoted purely to expansion in 2021).

China is expected to accelerate investment in 2022, with the State Grid Corporation of China budgeting more than CNY 500 billion for the first time ever and focusing on ultra-high-voltage projects, the upgrading of the distribution network and raising levels of digitalisation of its grids. With 2060 net zero goals on the horizon as well as an ambitious 14th Five-Year Plan for renewables, state-owned utilities' impressive expansion plans are expected to continue triggering investments in the future.

European distribution and transmission system operators are also foreseeing higher investment needs associated with the expansion of the network to integrate more renewables. The focus is particularly on connecting distributed energy resources and offshore wind farms, the modernisation of ageing infrastructure and the digitalisation of grids to allow demand-side load management, electric vehicle charging and the electrification of industry. However, investment levels will not accelerate unless policy makers improve investment frameworks, facilitate access to funds and shorten assessment and permit-granting processes.

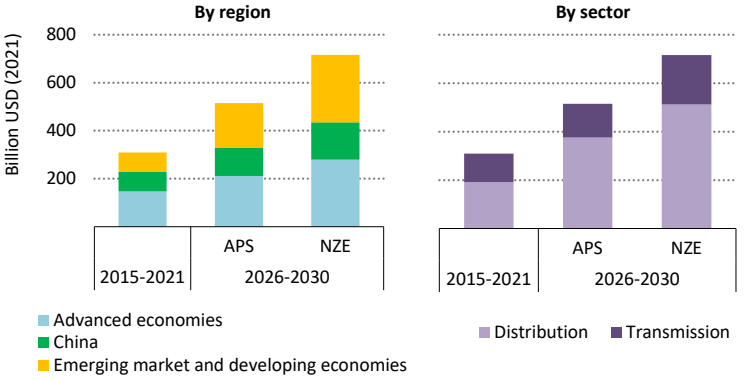
Capital spending on electricity networks in EMDEs stood at around $60 billion in 2021, a similar amount to 2020, and is expected to remain flat in 2022. These are very low levels compared to the $100 billion spent in 2015 and 2016, especially given the transmission and distribution investment needed to keep these regions in line with a net zero trajectory. The weak financial situation of some distribution companies, the lack of adequate investment frameworks (such as performance-based regulation), the lack of least-cost system plans and high operational and commercial losses are among the most important factors that should be tackled in EMDEs to encourage investment.

But investments in electricity grids need to more than double through to 2030 to be on track for net zero, especially in EMDEs

Investments in electricity grids need to considerably increase in the next decade, especially in the IEA's more climate-driven scenarios: the Announced Pledges Scenario (APS) assumes that all long-term emissions and energy access targets, including net zero commitments, are met in time and in full, whereas the Net Zero Emissions by 2050 Scenario (NZE) sets out a pathway for the global energy sector to achieve net zero CO_2 emissions by 2050.

Investments in the APS surpass $500 billion per annum by the late 2020s, with a higher increase coming from the distribution grids. This trend further accelerates in a trajectory consistent with Net Zero emissions by 2050, getting to around $700 billion per annum on average by 2030, more than twice the current investment levels. Hence, capital expenditure would need to increase at a compounded annual growth rate of more than 15% for electricity grids, almost six times the growth rates seen for the sector in the last three years.

AVERAGE ANNUAL INVESTMENT SPENDING IN ELECTRICITY GRIDS



Note: APS = Announced Pledges Scenario. NZE = Net Zero Emissions by 2050 Scenario

The shortfalls are striking on a regional basis, particularly in EMDEs. EMDEs require almost $250 billion per year through to 2030 in the NZE, whereas investment in electricity transmission and distribution in these countries has been only around $80 billion annually since 2015. In advanced economies and China, the annual investment gap in electricity grids is smaller but still significant, at around $150 billion and $60 billion respectively.

Clean, reliable and resilient electricity systems need smart grids more than ever

With around 80 million kilometres of transmission and distribution lines worldwide, electricity networks are the backbone of secure and reliable power systems. Electricity networks also have a central part to play in unlocking flexibility from power plants, energy storage and demand-side resources. Over the coming decade, transmission and distribution grids will capture a growing share of total power sector investment in recognition of their critical role in supporting modern power systems and clean energy transitions.

However, electricity grids are not receiving this necessary recognition in some regions, as the deployment of variable renewables and the electrification of other sectors are growing faster than the construction of smart grids, leading to strains and pressures in their power systems.

For instance, Viet Nam announced at the beginning of 2022 that no new solar or wind projects would be connected for the rest of the year. This occurred after a rapid build-out of more than 20 GW of variable renewables during the last three years (more than 25% of total capacity) which led to frequent grid overload and high renewables curtailment. In China, wind curtailment surpassed 10% in Inner Mongolia and 10% of solar power was wasted in Quinghai in the first half of 2022. As a response, China is accelerating investments in ultra-high-voltage projects and battery energy storage systems.

The Netherlands is experiencing the consequences of a rapid rise of electrification (led by the digitalisation of the economy and the electrification of mobility and heating) without a prior increase in smart grid infrastructure. As a consequence, and despite the expansion of the electricity grid by Transmission System Operators (TSOs) and Distribution System Operators (DSOs), the rapid increase in electricity demand is outpacing the capacity expansion of the grid, and various non-residential consumers are facing limits to accessing electricity at various points in the grid.

Long grid planning and permitting times are leading to insufficient transmission capacity to connect northern to southern Germany, which is leading to higher renewables curtailment and redispatch costs.

Digital infrastructure in smart grids is growing

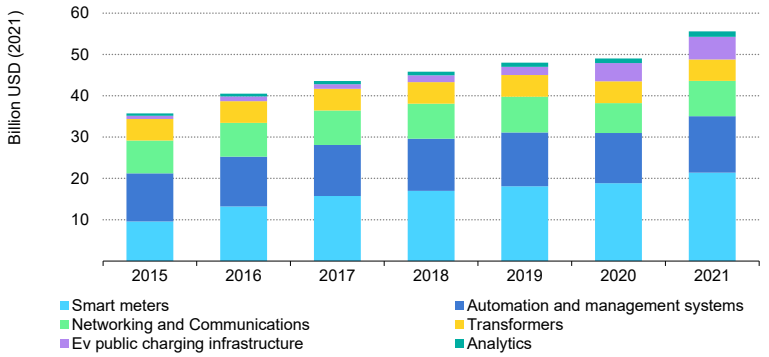
Investment in digital infrastructure in transmission and distribution rose again in 2021 after a slowdown in 2020, and is expected to account for more than 15% of total investment in electricity grids.

The distribution sector accounts for around 75% of all investment in digital, with the rollout of smart meters and the automation of substations, feeders, lines and transformers via the deployment of sensors and monitoring devices. These systems, while improving grid performance and uptime, also provide utilities with dynamic control over fluctuating voltage levels, two-way power flows and intermittent renewable generation. Digital investments in distribution also include network digital twins and non-wire alternatives, such as flexibility services and distributed stand-alone storage systems.

In the transmission business, digital investment is devoted to the digitalisation of power transformers, the automation of substations and the development of flexible AC transmission systems (FACTS) and advanced sensors (e.g. phasor measurement units), allowing for a faster and more flexible operation and improving control, monitoring and optimisation of the power grid.

Finally, investment in public EV charging infrastructure continued to grow in 2021, rising by more than 20%. However, it still comprises less than 5% of total distribution investment.

Investments in digital infrastructure in transmission and distribution electricity grids



Source: Guidehouse (2022)

Large-scale interconnectors are of vital importance for the decarbonisation of certain regions

Large-scale interconnectors remain a principal focus of investment in transmission, with projects under construction or planned in Europe, China, North America, India and Australia. They are a valuable tool to balance supply and demand across regions, access remote energy resources and integrate variable renewables. In the European Union, for instance, the REPowerEU plan proposes additional investment of €29 billion to stimulate the development of interconnectors.

Interconnectors are also important as a tool to boost international power trading and power flexibility, which can allow for efficient resource sharing, particularly for hydropower, solar PV and wind. The Western African Power Pool (WAPP) is a good example, where technical integration of the 14 member countries covered by WAPP is almost complete. In 2021, new transmission lines reached Guinea and Sierra Leone, leaving only Gambia, Guinea Bissau and Liberia to be connected, which is due to occur by the end of 2022. Interconnected

WAPP countries exchanged 6 TWh in 2020, or 8% of total power generated. Trade is expected to double by 2025.

Extreme weather events necessitate power system reliability and security improvements

Around the globe, the extreme weather events of 2021 and 2022 highlighted the energy security risks that climate change is introducing, and the importance of investing in more resilient electricity grids. Winter storms in Texas, cyclones in Fiji and Indonesia, and floods in Germany and China left millions of businesses and homes without power for days and even weeks.

But electricity systems are also struggling to cope with severe strains caused by heatwaves and low rainfall. A range of countries, including the United States, Canada, Iraq, Pakistan and India were severely affected by unusually high temperatures in 2021 and 2022. At the same time, lower than average rainfall and prolonged dry weather are raising concerns about hydropower output in various parts of the world, including Brazil, China, India and North America.

These challenges highlight the urgent need for strong, well-planned policies and investments to improve electricity system security. Electricity systems must be made more resilient to the effects of climate change – and more efficient and flexible as they incorporate larger amounts of solar and wind power, which will be critical to reach net zero emissions in time to prevent even worse climate change impacts.

Recommendations

Improve regulatory frameworks to accelerate investments in emerging market and developing economies

EMDEs are lagging behind in adapting their electricity grids for the energy transition, despite being regions where demand for energy services is expected to grow faster. For example,

Nigeria's national electricity grid has collapsed more than 200 times in the last nine years. These archaic and weak grids suffer from high system losses and lead to inefficient consumption of fossil fuels and frequent power outages.

If bottlenecks in this infrastructure prevent clean energy investment from rapidly picking up in EMDEs, the world will face a major gap in efforts to address climate change and attain other sustainable development goals. Therefore, policymakers have a crucial role to play in setting long-term visions and plans for electricity aimed at ensuring that electricity network expansion and modernisation keeps pace with expanding renewables deployment and new sources of demand.

Investment in many emerging and developing economies is more dependent on public sources; state-owned enterprises account for around three quarters of electricity grid investment in these economies. But public funds are typically scarce, many state-owned utilities are highly indebted and a worsening global economic outlook reduces governments' ability to fund projects. High costs of capital and rising borrowing costs threaten to undercut the necessary investments in electricity grids.

Regulators should tackle the weak financial situation of some distribution companies, the implementation of adequate investment frameworks (such as performance-based regulation), the development of least-cost system plans and sound network tariff designs, and the reduction of high operational and commercial losses. International cooperation can also provide additional financial and technical support, including concessional capital, private sector capital, and inflows from international markets.

Establish adequate remuneration schemes and enhance grid permitting processes

Electricity network regulators, especially in advanced economies, have been trying to avoid the risk of over-investing in the last 20 years, given that electricity demand has stagnated due to gains in energy efficiency. In addition, until recently, expansionary

monetary policy by central banks has led to decreasing costs of capital for utilities.

However, the electricity sector is at the heart of the energy transition, with the electrification of industry, buildings and transport sectors and the deployment of variable renewables. This new paradigm requires an acceleration of investment in electricity transmission and distribution. However, the weakening economic situation is likely to be a barrier to this required acceleration. TSOs and DSOs will be eager to reduce investments based on cost increases of raw materials, such as copper and aluminium, and higher costs of capital due to tightening financial conditions

Furthermore, to avoid grid congestion and ensure the success of clean energy penetration, grid infrastructure additions (grid expansion or enhanced grid flexibility) need to proceed in parallel with variable renewable capacity additions. The challenge for regulators is to resolve the asymmetry of lengthy grid permitting times with the imperative of shorter implementation lags in renewables.

Grid planning and permitting times can be as long as a decade from inception to commissioning of infrastructure. In Germany, for example, the grid planning period of the first Grid Development Plan started in 2011, and was followed by a series of lengthy permitting sequences, while the large interstate connections from northern to southern Germany are to become operational in 2025 at the earliest. Similar observations on permit delays apply to many OECD countries, including the Netherlands, the United Kingdom, Norway, the United States, Spain and France.

Public acceptance of large infrastructure developments is yet another hurdle to grid expansion. Some project developers and authorities have reacted by introducing metrics to limit the visible impacts of grid infrastructure, for example, by insisting on the use of underground cable instead of overhead lines. Nonetheless, project developers need to pay close attention to the needs of local communities and involve them in the process as early as possible.

All in all, legal and regulatory frameworks should develop a change in mindset, avoiding the risks of under-investment and bottlenecks by improving integrated planning processes (for supply, demand and flexibility) and establishing adequate remuneration to incentivise smart grid deployment.

Foster innovation in business

Governments, regulators and utilities should define the roles and operational boundaries of all relevant stakeholders and foster new business models, including those that involve aggregators, virtual power plants and circular solutions, to create a more efficient and sustainable grid.

Governments can collaborate with equipment manufacturers, network owners and operators, utilities and third parties to create "sandbox" environments in which new distributed energy business models can be operated in real-world conditions to identify the least-cost integration options to scale up operations.

It is not just about expanding the grid: modernisation and digitalisation are as important

Power utilities in advanced economies are leading the digitalisation of their transmission and distribution grids, with annual spending ranging between 10 and 20% of total investment. However, this trend needs to accelerate and spread globally. For instance, maintenance and modernisation of existing infrastructure should represent almost a quarter of the total spending in Africa, helping to reduce losses by 30% in 2030 compared with 2020.

TSOs and DSOs should facilitate the adoption of novel assets, including technical options such as distributed energy resource management systems, advanced voltage and reactive power controls, artificial intelligence and drones for more efficient operation and management, closed-loop operations and non-wire alternatives, such as flexibility services and distributed stand-alone storage systems.

Develop roadmaps for standardisation and interoperability

As new services and technology platforms develop, the need for devices to communicate and operate seamlessly across all levels of the grid increases. Central to smart grids is the capability for technologies to be deployed in one part of the energy system and interact with elements in different sectors and geographic areas, and to be used by various stakeholders all along the electricity value chain.

Technical roadmaps that lay out the necessary evolution of standards and interoperability of both digital and traditional electricity infrastructure will be required as the energy system continues to evolve. For instance, in 2021 the European Distribution System Operators (EDSO) for Smart Grids proposed a set of comprehensive indicators to monitor the smartness of grids at the distribution level.

Electricity grids rely on resiliency and sustainability

Extreme weather events and cyber-security challenges highlight the urgent need for strong, well-planned policies and investments to improve electricity system security and resiliency. Power utilities should develop a forward-looking approach for resilience against future potential hazards.

Today, more than 30% of total transmission and distribution investments in the United States are being devoted to adaptation, hardening and resilience purposes. This includes undergrounding power lines, installing concrete poles and elevating or relocating transformers. Nevertheless, TSOs and DSOs should continue developing instruments that can help them better predict and prepare for extreme weather events and wildfires. These include weather predictive services, fire spread modelling, deployment of sensors and high-definition cameras and other real-time or near real-time situational awareness systems.

The growth of network-connected devices, systems and services comprising the Internet of Things in electricity grids

creates significant benefits for the sector. However, the increased interconnectivity of devices entails greater threats from cyber actors. Assessing cybersecurity risk is especially important for new manufacturers, vendors and service providers as they design and implement their devices, systems and services. Security needs should be included in the design process, and initial deployments of new technologies should be closely coordinated with TSOs and DSOs.

Electricity grid operators should embrace the United Nations Sustainable Development Goals and strive to achieve them by reducing the use of raw materials, adopting alternative sustainable materials in grid components, implementing circular solutions for dismantled grid assets, such as recycling and reusing equipment, and protecting biodiversity. These measures can reduce lifecycle environmental footprints and increase safety, especially when critical minerals, notably copper, can become scarce and geographically concentrated.

PART III
COUNTRIES

13. A New Digital and Technological Sovereignty for Europe: Twin Green and Digital Transitions and Twin Challenges in Sovereignty and Security

Annegret Bendiek, Isabella Stürzer

NextGenerationEU as an Accelerator of Sustainable Economic Transition – and European Re-sovereignisation?

Great Power conflict is returning while democracy is threatened, the technological revolution and digitalisation are accelerating, and climate change is escalating: undoubtedly, the global community is facing significant challenges in the still young XXI century. Naturally, the same applies for the European Union, which has been on a promising journey of re-sovereignisation since the Treaty of Lisbon entered into effect in December 2009, but at the same time has been confronted with considerable challenges, from internal disputes in the European Debt Crisis over the first-ever withdrawal of a member, "Brexit", transatlantic discord, and not least the Covid-19 pandemic.

The necessity to respond to the manifold challenges posed (or exacerbated) by the Covid-19 pandemic prompted the EU to introduce the European Union Recovery Instrument,

also known as NextGenerationEU (NGEU).[1] NGEU was first suggested by the European Commission (EC) on 27 May 2020;[2] generally speaking, NGEU is an economic recovery instrument consisting of loan and grant schemes which also serves as a guide to building "a more sustainable, resilient and fairer Europe for the next generation,"[3] as the official communication from the EC puts it. Indeed, more than 50% of the almost €807 billion of NGEU are reserved for availability via specific programs such as Horizon Europe, the EU's R&D funding scheme, the Just Transition Fund and the Digital Europe Programme, which shall foster innovations bolstering the "twin green and digital transitions,"[4] and lastly, programmes specifically addressing medical R&D and healthcare.[5] As NGEU's more formal name, "European Union Recovery Instrument", reveals, NGEU is a key tool of the EU's stabilisation policy addressing the financial, economic, and social consequences of the Covid-19 pandemic.[6]

NGEU is a temporary instrument that is not part of, but complements the 2021-2027 Multiannual Financial Framework (MFF). It is noteworthy as, for the first time in the EU's financial policy, it will be financed by common debt – an instrument many EU Member States, especially Germany, fiercely opposed in past financial crises. Therefore, NGEU should be seen as evidence for deeper European integration and hence increased internal sovereignty as well. In order to guide the flow of investments funded by NGEU, the EC has declared the European Green Deal the "EU's recovery strategy",[7] and has described the issue of circular economy, renewable energy, and more environmentally friendly transportation and logistics

[1] European Commission, "Europe's moment: Repair and prepare for the next generation", Press Release, 27 May 2020, COM(2020) 456 final, p. 2.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] European Commission, "NextGenerationEU", in recovery Plan for Europe.
[6] European Commission (2020).
[7] Ibid.

as key. Further, NGEU funds shall strengthen the single market and advancing the EU's adaption to the digital age by improving (5G) connectivity, strengthening (or, in fact, developing) European industrial and technological capacities in cutting-edge technologies such as Artificial Intelligence or cloud services, and increasing cyber resilience.[8]

Given these prioritised areas of investment, it is safe to say that the interrelated goals of digital and technological transition lie at the core of the NGEU strategy. It is therefore important to examine how these goals can be met, as obtaining crucial technology and increasing productivity are far greater obstacles than merely insufficient funding. At the same time, it is necessary to understand how both the European industrial landscape and European citizens will be affected by and be able to benefit from the twin goals of digital and technological transition, as opportunities are unevenly distributed across European regions and conflicts of interest between national and European strategy remain widespread. Lastly, a sharp increase in European digital and technological advancement will not only affect the European industry, economy, and society – it will also change the EU's capabilities in shaping international relations and allow the EU to strengthen its geopolitical position. However, this only means that digital and technological advancement will equip the EU with the necessary capacities to have a geopolitical impact – the twin transitions themselves cannot generate political will to capitalise on this potential and translate it into a coherent external digital strategy complete with the development of appropriate tools for external action.

Consequently, digital and technological transitions can only be truly successful when they come hand in hand with an active effort to advance European digital and technological sovereignty both internally and externally. While the EC declared strengthening digital and technological sovereignty a key goal of the so-called "digital decade" 2020-2030 prior to

[8] Ibid.

the onset of the Covid-19 pandemic, this aim has only gained in importance since the global spread of Covid-19 revealed painful dependencies and worrying supply bottlenecks, and has increased in urgency even further since the Russian attack on Ukraine challenged and arguably transformed the European security order. Hence, successful implementation of the digital and green twin transitions is intertwined with the twin challenges of strengthening sovereignty and security. Both challenges share the benefit that if planned and implemented strategically, digital and green transition as well as internal and external (digital) sovereignty are mutually reinforcing – strengthening the one helps strengthening the other.

Understanding European Sovereignty Since Lisbon: Dimensions of Internal and External Sovereignty

In order for the EU to be able to plan the twin transitions and meet the twin challenges successfully, it is first and foremost important to develop an understanding of sovereignty that reaches beyond traditional legal definitions and takes into account both the manifold dimensions of sovereignty now discussed in the national security debate and the sui generis nature of the European Union as a supranational organisation.

The term "technological sovereignty" or "digital sovereignty" has become quite a buzzword in the political debate since it was coined by industry representatives in the early 2010s. They cautioned that industrialised nations and global exporters of technology products are dependent on the availability, integrity and controllability of state-of-the-art security technologies, and should thus focus the political debate more specifically on "dual use", taking into account both civilian and military needs in the field of security technology in order to identify shortcomings and develop policies and standards that would ensure that relevant technologies are available, controllable and

part of a secure infrastructure in the future. The term was then expanded to encompass all technology and not only security technology (although both those who use the term and various discourse analyses concur that there is no clear definition of what specifically makes technology a security technology) but really any kind of technology and especially rather "new" or digital technologies – to include anything from Artificial Intelligence over 3D printing to quantum computing.[9] The terms have been adopted by the EU as well; in a 2020 guest commentary, President of the European Commission Ursula von der Leyen declares that she was a "tech optimist" because she saw great potential in the European industry – aided by her Commission's investment program in digital industries, especially such which can help increase environmental sustainability[10] – and hence believed that the EU had the power to shape emerging industries according to its ethical norms, to include the responsible use of new technologies and the development of fair standards.[11] Given that many concerns regarding the vulnerability of critical technological infrastructure are often also discussed as cybersecurity issues, the term "digital sovereignty" has emerged and is sometimes used interchangeably with "technological sovereignty." In a 2020 strategy paper, the European Parliament defines "digital sovereignty" as follows: "Europe's ability to act independently in the digital world", elaborating that

> [s]trong concerns have been raised over the economic and social influence of non-EU technology companies, which threatens EU citizens' control over their personal data, and constrains both the growth of EU high-technology companies and the ability of national and EU rule-makers to enforce their laws.[12]

[9] S. Mair, "Sicherheit durch technologische Souveränität!", *Bund der Deutschen Industrie*, 29 October 2015.

[10] European Commission, "Global Gateway", 1 December 2021.

[11] Ursula von der Leyen, "Europas technologische Souveränität", *Handelsblatt*, 19 February 2020.

[12] European Parliament, "Digital sovereignty for Europe", BRIEFING EPRS Ideas Paper Towards a more resilient EU, p. 1.

These laws – or rather the process of their genesis – is what should be at the core of a modern understanding of European sovereignty in its manifold dimensions. The concept of sovereignty has become very complex and is nowadays better understood as a process, not a status quo. In other words, sovereignty no longer merely refers to a legally defined status – instead, it needs to be understood in the context of EU actors' moderating capacity of legitimising their positions through transparent, internal opinion-forming processes and exercising them effectively internationally in multi-stakeholder bodies and institutions.[13] European debate on norms harmonisation and subsequent standardisation contributes to deepening integration and thus advances internal re-sovereignisation, whereas European rules and laws backed by all Member States also carry significant political capital that can be transformed into successful externalisation of European norms and standards, even including a certain degree of regulatory power over foreign (and bigger) markets than the European one.[14] This way, a coherent, credible and sustainable European mandate that has emerged from the European comitology procedure – which is also expression of an internal re-sovereignisation process – can strengthen European external re-sovereignisation, which underscores the mutually reinforcing nature of internal and external sovereignty.

[13] S. Bendiek, "The Impact of the Digital Service Act (DSA) and Digital Markets Act (DMA) on European Integration Policy", SWP Working paper, 2 April 2021, p. 5.

[14] A. Bendiek and I. Stürzer, "Advancing European Internal and External Digital Sovereignty Deutsch the Brussels Effect and the EU-US Trade and Technology Council", SWP Comment 2022/C 20, 11 March 2022, 8 Seiten.

Understanding European Security in a Globalised and Confrontative Security Order

The EC has often proven that it is well aware of the internal and external re-sovereignisation processes and has strengthened its position among the European institutions by initiating many directives addressing the regulation of new and emerging digital technologies, to include regulations concerning both users and market competitors. For instance, the EC takes great pride in the fact that the European General Data Protection Regulation and its provisions shaped not only the terms of service of leading social media platforms, to include the platforms operated by Meta, but even impacted the data protection legislative debate in the United States. At the same time, there are concerns that the EC may excessively focus on such regulatory power over foreign markets in its external digital strategy, thus forgoeing the opportunity to discuss (hard) security implications of such regulatory regimes as well.

When presenting her college of commissioners on 27 November 2019, president-elected of the European Commission Ursula von der Leyen defined priorities of the Commission as being a "geopolitical Commission" dedicated to multilateralism and cooperation, a green Commission that defines the European Green Deal as the EU's growth strategy, and a Commission that levers Europe's ability to be a global standard setter to its advantage.[15]The Commission identified climate change as the single most important threat, needing both a European R&D effort and a multilateral, global effort to combat. Since late 2019, the dire impacts of climate change have become even more evident, but beyond that, the world has changed profoundly: the Covid-19 pandemic, intensifying Great Power competition, and the Russian attack on Ukraine have shifted priorities and made this mapped road ahead a race

[15] European Commission, Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme, 27 November 2019.

ahead, as suddenly not only ensuring that a sustainable climate for and health of European citizens are protected are of primary concern, but serious new hard security implications now factor in as well. However, while the EC responded to the Covid-19 crisis by introducing NGEU, which vows to combat the negative effects of the pandemic by accelerating the implementation of the European Green Deal, a similar strong EU response to the Russian attack on Ukraine is still missing – despite announcing the ambition of being a "geopolitical Commission".

The EC has succeeded in forming a transatlantic alliance on "democratic technology" with the United States via the EU-US Trade and Technology Council, and thus taken significant steps towards increasing both digitalisation and digital sovereignty sustainably – the former by entering into research and investment partnerships with leading technology producers that can help increase accessibility to digital services and connectivity across Europe, and the latter by entering into such agreements with companies that are obligated to adhere to legal provisions made by democratic governments.

Challenges Ahead for European Industry and Society

While the current von der Leyen-led Commission announced its plans for a "digital decade" as early in 2019 when the current EC took office, its plans for digitalisation, sovereignisation and ecologisation have been both hampered and accelerated by the Covid-19 pandemic and the Russian attack on Ukraine. Both of these urgent and concerning, albeit very different (security) crises have revealed dangerous shortcomings and potentially harmful bottlenecks in the European digital, technological, external and industry strategy. Further, these crises have underscored the importance of European integration and cooperation and fostered integration and dialogue while also highlighting discord among Member States, for instance in connectivity development, as some governments in Central and

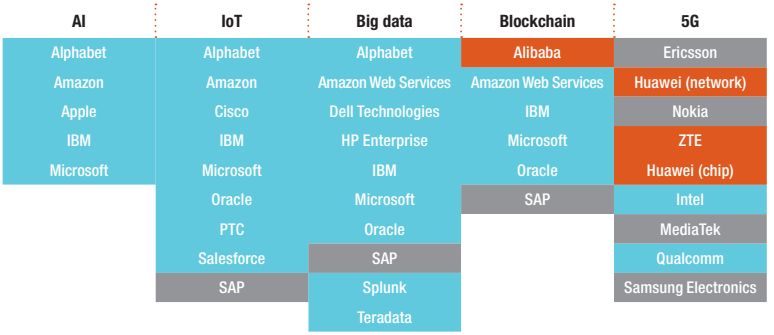
Eastern Europe have expressed concerns for the advancement of their digital connectivity if global market leaders such as China's Huawei were excluded from the internal market for failure of meeting privacy and security certification schemes.

Huawei remains the leading developer and provider of 5G products and services in terms of revenue, and as the first company world-wide put out products enabling the use of the 5G standard, it has significantly raised the profile of the People's Republic of China (PRC) as a highly technologically advanced nation after a long (and enduring) period as "the workbench of the world".[16] Still, despite its competitive edge in 5G technology, China's rise in the field of technological prowess is also relative, and other companies are catching up fast. In 2020, Huawei ranked only fourth in the list of companies filing for most 5G patents, following Samsung Electronics, Nokia, and LG Electronics. Further, Ericsson has eclipsed Huawei as top 5G provider according to the 2020 Technology and Innovation Country Readiness Index published by the UN Conference on Trade and Development UNCTAD.[17]

[16] S.-C. Fischer, *Artificial Intelligence: China's High-Tech Ambitions*, CSS Analyses in Security Policy, no. 220, February 2018.

[17] "Technology and Innovation Report 2021", UNCTAD, p. 21.

FIG. 13.1 - TOP FRONTIER TECHNOLOGY PROVIDERS - AMERICAN COMPANIES IN BLUE, CHINESE COMPANIES IN ORANGE AND OTHERS IN GREY



Source: UNCTAD (2021), p. 21

In other key digital technologies, including Artificial Intelligence, big data and blockchain technology, Chinese companies are not represented among the top providers (except for Alibaba's blockchain technology). However, the only European company included other than Ericsson is SAP, which means that the US continues to be the leading innovator in this sector. In fact, it was not until 2019 that Huawei was able to build a smartphone without manufacturing chips provided by the American Qualcomm.[18] This means that while Huawei equipment might not be replaceable immediately once a country decides to limit its involvement in 5G network development, feasible European and American alternatives exist which also possess the necessary technological know-how.[19] Huawei profited both from high public R&D investments and a targeted press campaign painting it as standard-setting company[20] and almost inevitable

[18] A. Fitch and D. Strumpf, "Huawei Manages to Make Smartphones Without American Chips", *The Wall Street Journal*, 1 December 2019.

[19] L. Cerulus, "Cracks appear in West's 5G strategy after Huawei", *Politico*, 30 November 2021.

[20] M. Scott, "Huawei's under-the-radar Brussels blitz", *Politico*, 22 September 2021.

partner. In contrast, R&D investments in the EU have been comparatively low,[21] what the EC also seeks to remedy during its "digital decade".[22]

The example of Huawei also shows a company that profited both from high public R&D investments and a targeted press campaign painting it as standard-setting company and almost inevitable partner. Another example highlighting European dependency on external partners is the recent high-profile announcement on the part of US-company Intel that it plans to invest up to €80 billion in the European Union over the next decade along the entire semiconductor value chain, with plans for a semiconductor production site in Germany, a R&D centre in France, and manufacturing plants in Ireland, Italy, Poland and Spain.[23] The announcement was received with enthusiasm for Intel's decision to invest in Europe and Europe's associated increased importance as R&D and production site for semiconductors. However, some observers pointed out that while Intel's investment is highly welcome, it was unfortunate that Europe has not produced a company of comparable intellectual property and production volume capacities, and is unlikely to do so in the near future.

While the engineering of a transatlantic alliance on trade and technology, complete with beneficial investments such as those by Intel, is an important and sustainable step towards digitalisation and increased digital sovereignty, the EU is insufficiently prepared for conflict in the digital realm – in terms of preparedness, resilience, and defence – although statements made in the Strategic Compass clearly demonstrate that the EU is aware of looming geopolitical conflict in the digital sphere.

---

[21] O. Batura, M. Flickensch, T. Ramahandry, and V. Bonneau "Key enabling technologies for Europe's technological sovereignty", European Parliamentary Research Service, December 2021, p. 29.

[22] Ibid., p. 37.

[23] https://www.intel.com/content/www/us/en/newsroom/news/eu-news-2022-release.html

In addition to the recent designation of cyberspace as domain of military operations (e.g., NATO declared it such in 2016),[24] the capacity to develop, produce, and operate new and emerging technologies is increasingly also discussed in a geopolitical perspective. Burrows et al. point out that "high tech has come to signify high politics" and thus digital and technological sovereignty are no longer limited to be the topic of trade conflicts, but can spark actual international conflict – not least Great Power conflict.[25]

Challenges Ahead for European Security

As such Great Power conflict driven by technological competition has already emerged between the United States and the PRC, the EC has strived to avoid a scenario in which Europe may become the scene of a technological proxy war between the US and China[26] by forming the EU-US Trade and Technology Council and introducing certification regimes and toolboxes, the latter also in the Strategic Compass. However, while these measures alone are insufficient for a lack of coherent understanding of hybrid threats and corresponding counterstrategy, let alone political responsibility scattered across institutions, the EU is first and foremost missing an understanding of security in terms of "sustainability" or "resilience".[27] The EU pursues digitalisation and connectivity across sectors and thus realises economic potential while also increasing vulnerabilities, yet it is not getting ready for protecting itself against the exploitation of these vulnerabilities.

---

[24] Intel, "Intel Announces Initial Investment of Over €33 Billion for R&D and Manufacturing in EU", Intel Newsroom, 31 July 2018.

[25] M. Burrows, J. Mueller-Kaler, K. Oksanen, and O. Piironen, "Unpacking the geopolitics of technology", Atlantic Council, 8 December 2021.

[26] A. Bendiek, N. Godehardt, and D. Schulze, "The age of digital geopolitics", IPS, 11 July 2019.

[27] A. Bendiek and R. Bossong "'Hybride Bedrohungen': Vom Strategischen Kompass zur Nationalen Sicherheitsstrategie", SWP-Aktuell 2022/A 40, 23 June 2022, 8 Seiten.

For instance, President of the European Commission Ursula von der Leyen declared "This is a watershed moment"[28] when announcing that the EU will finance the purchase and delivery of weapons and other equipment to Ukraine – the first time it aides a country that is under attack in such way. However, while such financing and deliveries may help guarantee a stable defence for the Ukrainian forces for some time, they do not help to shape a sustainable long-term strategy for security on Europe's Eastern border, especially once Ukraine, which now has EU candidate status, joins the European Union at some time in the future. The Russian attack on Ukraine is complemented by cyber operations with targets in Ukraine and abroad, to include European companies whose capacities are either purposely attacked or simply are collateral damage – either way, Europe's digital infrastructure is affected and threatened by hostile cyber operations. Recently, for instance, the European wind energy sector has repeatedly suffered from cyber-attacks.[29] Prominently, on the day the Russian invasion started, the remote monitoring and control of thousands of wind turbines of a German operator failed as satellite connection had broken down.[30]

The fact that windmills were affected strongly bolsters the case for a more holistic approach to "sustainability"– after all, when transitioning to renewable energies such as wind power in order to be more ecologically sustainable and more independent from fossil fuel and gas suppliers, the wind mills need to function safely and reliably, in order words, the need to be sustainable and resilient. Therefore, EU policy-makers would be well-advised to think sustainability not only in terms of "green", but also in terms of "resilient", and thus need to provide investment opportunities for cyber security and defence just like investment

[28] European Commission, "Statement by President von der Leyen on further measures to respond to the Russian invasion of Ukraine", 27 February 2022.
[29] C. Stupp, "European Wind-Energy Sector Hit in Wave of Hacks", *The Wall Street Journal*, 25 April 2022.
[30] M. Willuhn, "Satellite cyber attack paralyzes 11GW of German wind turbines", *PV Magazine*, 1 March 2022.

opportunities are provided for developing technologies and infrastructure for the digital and green transition. Arguably, much like European sovereignty is best understood as a process rather than a status quo, security in the digital age can be better understood as resilience of infrastructures,[31] to include security and defence measures.

No New Digital and Technological Sovereignty for Europe Without a New Understanding of Security as Infrastructure Resilience

The already contested road towards a sustainable digital infrastructure has been transformed into a race by the Covid-19 pandemic and the Russian attack on Ukraine. Rather than simply progressing green and digital transition for the economy and industry via the European Green Deal, the EU now needs to balance strengthening partnerships while strengthening its domestic industries, mitigating negative consequences of the Covid-19 pandemic while providing investment incentives, consolidating its finances while fighting recession, and enmesh itself from technology and energy provider agreements that create unipolar dependencies.

To be able to not only keep up with both its competitors and partners in the race ahead, but to excel in this race, European policymakers are well advised to draw on a new understanding of European sovereignty as well as a more holistic understanding of sustainability. Just like the EU reacted swiftly to the adverse economic effects of the Covid-19 pandemic by introducing NGEU – as in line with its key principles of procedural sovereignty as it is innovative – it needs to create a more holistic security policy and develop a strategy accordingly.

[31] A. Bendiek and J. Neyer, "Smarte Resilienz. Wie Europas Werte in der Digitalisierung gestärkt werden können", Bertelsmann Stiftung, July 2020, p. 8.

The EU has accelerated the twin digital and green transitions as envisioned in the current Commission's European Green Deal by designing NGEU as a stimulus package that specifically targets investment opportunities in relevant fields. At the same time, European integration was deepened and internal sovereignty strengthened by NGEU, given that it marks the first time that all EU Member States agreed to common debt for financing the recovery instrument. Thus, NGEU is a promising tool for increasing sustainability, quite literally by ideally helping to contribute to a circular and green European economy, and politically by anchoring the European Green Deal as mutually agreed on European growth strategy within the Union. The fact that NGEU is financed by the first common debt in the EU's history expresses even further momentum for European integration and internal re-sovereignisation, however, a common resolute response to the Russian attack on Ukraine that encompasses security and defence instruments is still missing.

To remedy that oversight, EU policymakers should acknowledge that sustainability has another dimension beyond ecologisation: sustainability in terms of resilience, or security as the integrity of infrastructures. Only if both ecological and resilience considerations are accounted for when further developing the European digital infrastructure as well as the EU industry, digital, and external strategy, will such strategies be sustainable and the EU will be able to maintain and strengthen its digital and technological sovereignty in the race ahead.

14. EIB Financing of Digital Infrastructures for a Green Transition: the Challenges in the EU and in the Neighbouring Countries

Gelsomina Vigliotti

We stand on the brink of a new industrial revolution, driven by digitalisation and new-generation information and communication technologies (ICT). Digital technology has proved ivaluable for a number of businesses and sectors to tackle emergencies such as the Covid-19 pandemic and the challenges deriving from climate change. The European Investment Bank (EIB), the public policy bank of the European Union has embraced innovation and digitalisation as one of its policy goals to promote related technologies in the European economy. This is definitively a priority as most of the leading digital technology companies are currently based in the United States or China, while the European Union has fallen behind in adopting digital technologies. The comparatively lower growth performance of Europe can be explained by the fact that the digital sector is relatively small with respect to the following parameters. First, in terms of the Information and Communication Technology (ICT) sector's value-added share in total manufacturing. Second, in terms of the ICT sector's prospective innovation capability in light of the relatively low level of business investment in R&D in the ICT sector. For instance, Taiwan spends 75% of its business R&D expenditure in the ICT sector, Korea 53% and the US 33%. With the exception of Finland and Ireland,

all EU countries are generally far below the US level.[32] Last, but not least, the lack of widespread access to broadband communications infrastructure. Quantitative estimates show that significant growth opportunities are foregone in many European countries because of low broadband penetration.[33] However, the EU still has some areas of excellence which should help it keep up provided it seizes the opportunities arising from automation, artificial intelligence and other digital technologies. Next-generation digital infrastructures and emerging applications are key to fighting the world's existential challenge: the climate emergency.

The EIB is the largest funding institution of Europe's digital infrastructure, with annual lending of around €2.5 billion, supporting the roll-out of optical fibre projects, capacity upgrades and coverage expansions of advanced mobile networks. This is planned to be enhanced by the *Innovation, Digital & Human Capital* (IDHC) lending programme,[34] which aims to fully embrace the opportunities deriving from digitalisation, while providing targeted and effective support for their accelerated deployment, in line with its commitments under the Climate Bank Roadmap.[35] This includes the financing of, among others, digital infrastructures and innovative business models that will propel the decarbonisation of the economy. This note briefly spells out why digital infrastructure is strategic both for Europe and for its neighbouring and global partners, especially Africa, and how digital infrastructure is contributing to tackling the climate-related challenges we are facing.

---

[32] *OECD Digital Economy Outlook*, OECD, Paris, 2017.

[33] For instance, N. Czernich, O. Falck, T. Kretschmer, and L. Wössmann, "Broadband Infrastructure and Economic Growth", *The Economic Journal*, vol. 121, 2011, pp. 505-32.

[34] European Investment Bank, *Innovation for inclusive Green and Digital Transition*, 17 February 2022.

[35] European Investment bank, *The EIB Group Climate Bank Roadmap 2021-2025*, 14 December 2020.

Why Digital Infrastructure Is Important

Digital infrastructure is the backbone for the digital transition of advanced economies. Digitalisation is a broad-based concept that includes both the development and the deployment of digital technology across a wide range of economic sectors. Digital infrastructure ultimately allow for fast, economical and reliable data connections between firms, households and public services and the upgrading of the performance of this infrastructure to very high speed is key for developing advanced digital services. Building on this, innovative digital technologies such as artificial intelligence (AI), big data and Internet of Things (IoT) then serve as facilitators of new business models and organisational innovation, which are the ultimate drivers of job creation and growth. The contribution from the most ICT-intense industries to labour productivity growth has risen in Europe in recent years, currently even exceeding that of the United States.

The Covid-19 pandemic is a sobering reminder of the relevance and necessity of digital technology for the operation of a number of businesses and sectors: from health to retail services, from manufacturing to education. The pandemic has exposed certain vulnerabilities of the EU, such as excessive dependence on imports of critical goods and services, whose supplies were disrupted. Relevant sectors/economic activities for strategic autonomy mentioned in the European Commission's *New Industrial Strategy Communication36* include, among others, strategic digital infrastructures (5G, cybersecurity, quantum communication infrastructure) and key enabling digital technologies such as robotics, microelectronics, high-performance computing & data cloud infrastructure, blockchain, quantum technologies and photonics. The resilience of these industries and their capacity to continue to meet the needs of

[36] EU Monitor, COM(2020)102 – Communication, Commission Communication A New Industrial Strategy for Europe.

EU citizens calls for some additional investments in the short term. The very ambitious recovery programmes launched due to the crisis offer the EU an opportunity to embrace digitalisation to catch up with global competitors. Digital companies are not only more innovative and faster growing than non-digital businesses, they also create more jobs.

The manufacturing industry is one of the pillars of the European economy, in particular in large countries such as Germany and Italy, where its value added represents 18% and 15% of GDP respectively.[37] This is bound to change drastically with a new industrial revolution, driven by digitalisation and new-generation information technologies such as the Internet of Things (IoT), cloud computing, big data & data analytics, robotics and 3D printing. They open new horizons for industries to become more innovative and more efficient, mainly by innovating processes and developing innovative products and services. Despite several weaknesses, particularly in transforming new knowledge into business successes, the European industry is strong in some digital sectors such as electronics for automotive, security and energy markets, telecom equipment, business software, and laser and sensor technologies. Europe also hosts excellent research and technology institutes. However, high-tech sectors face strong competition from other parts of the world, and successful companies in the digital domain typically originate from other regions. Europe is still anchored in many traditional sectors and relies heavily on small and medium enterprises, which are typically lagging behind in digitalising their business. There are also significant disparities in digitalisation between regions. Digitalisation levels are low, much below the EU average, among companies in Eastern and Southern Europe and in traditional sectors, such as construction and basic goods manufacturing. This clearly emerges from the 2021 Digital Economy and Society Index (DESI) compiled by

[37] The World Bank, Manufacturing, value added (% of GDP).

the European Commission,[38] which tracks the progress made in EU Member States in digital competitiveness in the areas of human capital, broadband connectivity, the integration of digital technologies by businesses and digital public services. Apart from Estonia, Slovenia and Lithuania, all other Eastern European Member States are far below the EU average. Without intervention, there is the risk that the digital gap will increase over time as the companies driving digital change continue to digitalise at a faster rate, while others fall even further behind and risk losing their overall competitiveness.

EIB Support to Digitalisation Opportunity Within the EU and in Its Neighbouring and Global Partners

Europe's future digital competitiveness depends on seizing the digital opportunities in areas in which the EU is strong – and putting strategic digital technologies in focus, such as Artificial Intelligence (AI) and Internet of Things (IoT). Development, deployment and diffusion of digital technologies is key for Europe to thrive in the digital age, where there is an urgent need to accelerate digital adoption across the EU ecosystem.

There are considerable needs for additional investment in the digital transformation, currently estimated by the EIB at €125 billion per year. Increasingly, Europe's economic prospects depend on innovation in general, and particularly on digital and new frontier technologies, including AI and IoT – and the merger of the two into AIoT (Artificial Intelligence of Things) – as well as quantum computing, virtual and augmented reality, blockchain, and the integration of biology and engineering. A key aspect of the mission-critical requirements for future business success in Europe that needs to be mastered is to understand these technologies, develop expertise in them, and deploy them at scale.

[38] European Commission, The Digital Economy and Society Index (DESI).

In neighbouring countries in Eastern Europe, and even more so in Africa, the opportunities for economic development that derive from the evolution towards a digital economy are unique. They result from rapid developments in a number of separate but interdependent technologies, such as data centres, artificial intelligence, the internet of things, next-generation networks such as 5G, and the overall affordability of technology. All this allows for leapfrogging into the adoption of state-of-the-art technology without the burden of phasing out already installed legacy technologies. A study by the EIB[39] illustrates how Africa has a unique opportunity for ecologically sustainable economic development and growth through the better use of data, instead of persisting on an outdated development pattern based on old technologies that consume fossil fuels. Digitalisation has many benefits: It speeds up the spread of information, brings people closer together, creates jobs and makes societies more efficient.

With the transition to a digital era, new technologies' development cycles have shortened and their disruptive impact is often greater. This changing technological landscape creates opportunities for development finance institutions to back innovative, high-impact projects. However, it also generates risks for long-term financing institutions because existing borrowers may face increased pressure from current and new entrants.

The EIB has elaborated a toolkit[40] to tackle the investment hurdles that induce the private sector to perceive it as too risky to invest in telecommunications infrastructure and explains the ways the Bank can increase financing in the market and offer technical assistance to improve projects and encourage expansions into rural areas. The EIB's technical assistance enables the Bank to bring external expertise to address quality gaps in projects, enhance standards and best practices, and provide guidance on bridging financing gaps. The scope of these activities includes

[39] European Investment Bank (EIB), *The rise of Africa's digital economy*, 5 May 2021.
[40] European Investment Bank, European Investment bank, *Rural connectivity toolkit*, 17 May 2021.

support for upstream project development and the subsequent skill development of public authority personnel, improving access to finance and enhancing the business environment in general. The most common types of advisory services include market and sector studies to understand the needs of various industries and regions, business plans and strategy definition, risk mitigation and skill development.

The Bank puts particular emphasis on the contribution of digital infrastructure and technologies to promoting environmentally sustainable economic growth paths, not only in the EU but also abroad. For example, it is one of the Bank's priorities that Africa has access to state-of-the-art data and knowledge for key sectors. The rapid diffusion of mobile payments has shown that such technologies drastically reduce the adoption barriers for cutting-edge services.

The EIB takes a comprehensive approach to financing the digital economy, with investments ranging from telecom infrastructure to digital services, digital transformation of the economy and environmental sustainability. These areas are all highly interconnected, as digital transformation is a transversal phenomenon. Inclusive digital services require universally accessible, high-capacity infrastructure. Connectivity is based on fixed and mobile access networks, as well as their connection to the internet backbone through transmission networks and related infrastructure such as data centres. Technologies like electronic identification (e-ID) provide further enabling infrastructure for public services, including for establishing public safety net projects, which are much needed amid emergencies such as a pandemic.

Digitalisation Helps Tackle Challenges Deriving from Climate Change

Digitalisation is a key enabler in the fight against climate change. The Global e-Sustainability Initiative,[41] an initiative of the ICT industry, predicted that the sector will enable a 20% reduction of global CO_2 emissions by 2030, holding emissions at 2015 levels.[42] Digitalisation would contribute to decarbonisation across several sectors. ICT sector projects deliver a positive enabling impact through multiple levers, as they have use cases across various industries.

The new generations of fibre optic networks and 5G mobile technology are great examples. The improvements in performance – such as speed, latency and connection density – are also expected to come with a large improvement in energy efficiency, especially if based on the amount of energy required to transmit each byte of data. Therefore, in order to be able to provide enhanced services to their customers and at the same time control their operational costs linked to the energy consumption, telecommunication operators will be eager to invest in this infrastructure.

Concerning the so-called objective of climate change mitigation, ICT and digital infrastructure provide opportunities to improve efficiencies in other sectors and hence reduce GHG emissions. Two well established examples are: **i)** building energy management systems enabled through IoT-connected sensors and IT control systems; **ii)** vehicle fuel reduction as a result of improved driver behaviour and optimised logistics, enabled through IoT connections to vehicles, telematics and control systems. The latter provides an opportunity to develop integrated smart transport solutions, which can decrease energy use, increase efficiencies and reduce travel time in the coming years. Smart grids are also a key

[41] https://gesi.org/

[42] #SMARTer2030. ICT Solutions for 21st Century Challenges, GeSI, 2015.

enabler of renewable energy and advanced energy efficiency applications.

The strategy for the climate change adaptation objective is to strengthen infrastructure systems by developing climate services. Improving weather and climate risk information to enhance resilience raises awareness and improves education delivery. For instance, improved real-time environmental monitoring, forecasting and risk assessment is essential to facilitate better decision-making in the transport, water and energy sectors. This can be seen as part of the development of smart cities.

The role of ICT and digital infrastructure in enabling climate action in other sectors is well acknowledged, although it is currently quite challenging to measure. As the *EU Climate Bank*, the EIB is therefore also keen to show how the contribution of digital infrastructure investment projects stimulates further investments in high-impact climate action. Experience from projects shows that isolating direct impact mechanisms by economic sectors may be very challenging, as projects targeting a specific economic sector are quite rare. Therefore, it seems more appropriate to group sectors by the relevant ICT investment areas. This allows to identify several key economic areas where digitalisation investment projects enable material impacts.

The transition towards a more sustainable economy is possible only through innovation and digitalisation. The digital industrial revolution provides the opportunity to support a green recovery. This gives Europe the opportunity to tackle climate action, become more competitive and use resources better. Digital infrastructure allow end customers to reap the benefits of the energy transitions by optimising their energy bills, if not actively participating in the energy market and profiting from it. Next-generation digital infrastructures and emerging applications are key to fighting the world's existential challenge: the climate emergency.

For instance, the digitalisation of energy systems, networks, and resources is fundamental to improving the power sector's operations. They spur the efficient use of energy by end

consumers. Intelligent electricity grids can integrate ever-greater shares of renewable generation capacity, helping make our energy supply climate-friendly. The digital industrial revolution and the climate emergency require considerable investments at a time when the immediate fallouts of the pandemic must also be addressed. Smart meters and smart appliances, decentralised generation and storage resources and vehicle-to-grid are just some examples of the possibilities offered to end customers by digitalisation. All these opportunities require a well-performing, very high capacity digital infrastructure network.

EIB's Support to Tackle the Investment Gap for Europe's Digital Infrastructure

Telecom companies currently face an adverse investment environment due to potential supply chain breakdowns, delays in spectrum auctions and standard settings, reduced revenues and last but not least, the consequences of war in Ukraine. Moreover, network operators have been focusing on network support and maintenance during the pandemic lockdown period instead of fibre and 5G roll-outs. These factors have led to a roll-out delay and underinvestment in the sector, which can impact innovation and competitiveness due to the important social and economic benefits generated by the sector. High average infrastructure investment costs per household and low and uncertain revenues reduce the financial incentive for private investors to provide very high speed infrastructure in rural areas. The existence of positive economic externalities justifies public financial aid to deal with the market failure, particularly in countries with a large share of the population living outside urban areas.

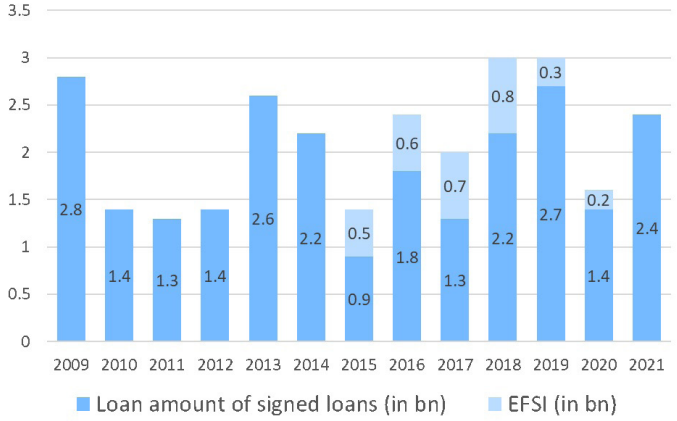
The EIB conducted a study[43] to estimate the investments required to achieve the objectives of the European Gigabit Society by 2025, covering all households in urban and rural areas and socioeconomic drivers with very high capacity networks as well as all urban areas and transport hubs with 5G. Private investments on their own are unlikely to cover a large part of the required investments, and certainly not within the envisaged timeframe. The estimated ensued investment gap amounts to €250 billion. The main factor is the market failure areas in scarcely populated rural regions where private investors are reluctant to invest due to the high unit costs of high-speed broadband networks. This is where public support is needed to achieve coverage targets, and where the EIB's role is most important.

The figure shows the evolution of EIB lending for digital infrastructure. EIB is the world's largest funding institution of digital infrastructure with annual lending of around €2.5 billion in 2021, supporting the rollout of fibre projects and capacity upgrade and coverage expansions of advanced mobile networks. A part of the lending was also supported leveraging resources from the European Commission (EFSI)[44] for projects with a higher risk profile. The projects generally support the objectives of the European Gigabit Society to achieve the full economic and social benefits of digital transformation and to avoid excluding the market failure areas from the benefits of digitalisation. Moreover, the investments in the sector will provide further network resilience to combat challenges like pandemics and to prepare for an increasingly digital future.

[43] For details see slides 5 and 6 in https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2020/RRF/Session%202_Harald%20Gruber_ITU%20301120%20%281%29.pdf.

[44] EFSI, also known as the Juncker Plan, has been launched as a joint initiative of the European Investment Bank Group and the European Commission to generate €315 billion of new investments. In the current financial framework the EFSI working principles has been taken over by InvestEU, https://www.eib.org/en/products/mandates-partnerships/efsi/index.htm.

FIG. 14.1 – EIB ANNUAL LENDING FOR DIGITAL INFRASTRUCTURE



Given the importance of digital infrastructure in furthering economic growth, European recovery programmes provide ample room for such investments. In the RRF, up to around €18bn funding is linked to 5G and gigabit networks across the 20 countries' plans. Additional funding of €78bn is provided by the related National Broadband Plans (NBPs). The plan also aims to reinforce the digital identity regime as part of a wider package for digital services and citizenship.[45] The EIB aims to support to the extent possible the RRF projects in the digital domain, if there are suitable portions left to be financed (5G, fiber networks, public administration, digital education, …). In the context of the European Commission's budget programmes such as InvestEU, the strategy of the EIB's actions is similar to that in the previous budget cycle under EFSI. EFSI support focussed particularly on areas of market failures. i.e. less populated areas, where the incentive for private financing of access to Very High Capacity (VHC) networks is particularly low. In any case, the financing of the EIB is complementary to financing from European and national support mechanisms.

[45] Source of data: Deloitte, *The contribution of National Recovery and Resilience Plans to achieving Europe's Digital Decade ambition*, Deloitte LLP Report, 21 June 2021.

Conclusion

The transition to a digital economy is changing how people interact, by enhancing the effectiveness of economic activities and offering new solutions across all sectors, with extensive economic benefits. Digital services require the layout of universal infrastructures. Following the EU policy objectives and more particularly, the harmonisation of digital markets and regional connectivity, the Bank takes a comprehensive approach to financing the digital economy, from investments in telecom infrastructures to digital services.

The roll-out of VHC fixed and mobile networks across Europe is a critical complement to business sector innovation, but market failures hold back the speed of this rollout. 5G networks serve as the foundation for new digital services, digital innovation, and the digital transformation of the business and public sectors, including the health and education sectors. Ultimately, the resulting collection and processing of big data based on Artificial Intelligence (AI) will be a key driver of productivity growth and the development of innovative new business models, which are critical to sustaining Europe's global competitiveness in coming decades. In alignment with the European Commission's digital targets for 2030 (Digital Compass), the EIB will continue to support very high capacity digital communication infrastructure and services.

Digitalisation is also a key enabler of the greening of other sectors of economic activity and of the shift towards more circular and less carbon-intensive industrial resource flows; all of which rely critically on the ability to – in real time – collect, analyse, and optimise processes using large amounts of information.

Digital technologies and services are proven enablers of sustainable development and inclusive growth. They can be key to improving lives even in the poorest countries, in particular by empowering women, enhancing democratic governance and transparency, and boosting productivity and

job creation. Significant financing is necessary along the value chain, in particular in Africa, to make a full transition to the digital economy. EIB supports investments digital economy infrastructures. The EIB's lending for digital technologies and infrastructure is pursued in all areas, with a particular focus on investments that support sustainable economic and social development, including private sector job creation, youth employment and women's empowerment.

15. Italy's Digital Strategy

Gianluca Sgueo

Italy's Digital Strategy in a Nutshell

Italy is the main beneficiary, in absolute terms, of the two main NGEU instruments, the Recovery and Resilience Facility (RRF) and REACT-EU. The RRF has allocated to Italy resources amounting to €191.5 billion, to be used over the period 2021-2026. The Italian government has supplemented this with an additional €30.6 billion through the Complementary Fund, financed directly by the State, giving a total of €222.1 billion.

In line with the EU's strategy for recovery, the final goal of Italy's National Resiliency and Recovery Plan's (NRRP) is to "install" long-term and pervasive transformation in Italian public administrations, industry, academia and society at large. This includes repairing the economic and social damage caused by the pandemic crisis, addressing the structural weaknesses of the Italian economy and leading the country along the path of digital and environmental transition. The NPRR commits Italy to implementing 190 measures (58 reforms and 132 investments) and hitting 525 targets in 5 years.

Out of a total of 6 missions composing the NPRR, three are directly concerned with digitalisation. Mission 1 ("Digitisation, Innovation, Competitiveness, Culture") allocates a total of €49.2 billion (of which €40.7 billion from the RRF Facility and €8.5 billion from the Complementary Fund) to promoting

the country's digital transformation, supporting innovation in the production system, and investing in tourism and culture. Mission 4 ("Education & Research") allocates a total of €31.9 billion (€30.9 billion from the RRF Facility and €1 billion from the Complementary Fund) to strengthening the education system, digital and technical-scientific skills, research and technology transfer. Mission 6 ("Health") allocates a total of €18.5 billion (€15.6 billion from the RRF Facility and €2.9 billion from the Complementary Fund) to strengthening local prevention and health services, modernising and digitising the health system and ensuring equal access to care.

Overall, 27% of the funds mobilised through the Italian NRRP, equivalent to €50 billion, is earmarked to advancing the digital transition. Present and future efforts – in line with the EU's goals and vision – are directed firstly to simplifying regulations and administrative processes, secondly to encouraging skills/knowledge/know-how sharing between private and public actors in key sectors from telemedicine to broadband infrastructures and thirdly to continuous skill development to enhance citizens' use of and benefit from technology.

Between 2021 and 2022, the spending commitments of the Italian Ministry for Technological Innovation and Digital Transition amounted to €9.5 billion – equivalent to 48% of the total resources available under the Ministerial mandate. Interventions focused on 3 main areas: connectivity, digitalisation of the public sector, and e-health. The following paragraphs will explore these areas in more detail, focusing on strategic aspects, reporting on implementation and analysing related challenges.

Broadband Connectivity

Let us begin with connectivity. Under the national NRRP, the Italian government has committed €6.7 billion to improving network reach and connection quality across the country. The

goal is to have 1 Gbps connectivity for families, businesses and organisations and 5G coverage nationwide by 2026.

As regards the roll-out of ultra-fast broadband, the national broadband strategy adopted in May 2021 aims at guaranteeing a download speed of 1 Gigabit and an upload speed of 200 Mbit/s in areas of market failure. These areas have been defined via a mapping exercise conducted in cooperation with telecommunication operators. Albeit coverage with connections of at least 30 Mbit/s has increased significantly in recent years (with Italy now in line with the EU average) the country is still ranking 22nd among 27 EU states in the roll-out of superfast broadband according to the DESI index published yearly by the EU Commission.

To bridge this gap and achieve the targets set in the NRRP, the government has supported infrastructural interventions with ad hoc regulatory measures aimed at speeding up administrative procedures and accelerating the roll-out of broadband infrastructures. Following the regulatory simplifications introduced in 2021, administrative procedure times were reduced from 250/300 days to 90 days. Along the same lines, the government has enhanced its substitutive powers in the event of default by public administrations; it has shortened the time limit for public administrations to exercise powers of self-redress from 18 to 12 months and, finally, has reinforced cases of silence-consent ("*silenzio-assenso*"). According to the new rules, public administrations have 10 days to acknowledge a request and issue a certificate electronically. Administrative inaction past this 10-day limit is equivalent to acceptance and the certificate may be replaced by a declaration of the concerned party.

The first public tenders were also launched in 2021 and awarded in June 2022. These include "Connected Schools", "Connected healthcare facilities" (providing both areas with 1 Gigabit broadband connectivity) and "Connected minor islands" (by providing fibre optic connections to the mainland, the government hopes to have at least 18 islands equipped with ultrafast broadband connectivity by December 2023).

It is worth noting that in all these cases, the government has adopted a subsidy model (greenlighted by the EU Commission) partnering with Telecom operators and covering up to 70% of related expenses.

"5G Italy" aims at providing 5G connections in areas of market failure. The government has committed €2.02 billion to investments in this project. The goal is to have the Italia 1Giga plan completed by June 2026. The strategy trusts businesses to choose and adopt the technology most appropriate to their development, acquisition and commercialisation needs and requirements.

Digitalisation of the Public Sector

Moving on to the second area of intervention, digitalisation of the public sector, the Italian NRRP assigns €6.14 billion to sustaining the digital transition of the public sector, simplifying it for citizens and businesses and reducing time and costs.

According to the timetable set by the Italian government, at least 80% of essential public services will be digitalised by 2026. This is not an easy task. According to Eurostat, in 2021 only 42% of Italians aged between 16 and 74 years have basic digital skills (compared to 58% in the EU), and this will have a significant impact on the use of digital services.

To implement this process efficiently, governance has firstly been structured on two levels: the Ministry for Technological Innovation and Digital Transition, the Department for Digital Transformation, and the Ministerial Committee (chaired by the President of the Council of Ministers or by the Minister responsible for technological innovation and the digital transition) are tasked with providing strategic guidance. Territorial administrations are actively engaged in implementation measures.

Secondly, it was decided to avoid "one size fits all" solutions. Hence, best performers will be able to operate as aggregators of skills/ideas/projects, whereas under-performing administrations

will be assigned a dedicated task force, nested in the Ministry for Technological Innovation and Digital Transition, to provide the necessary guidance.

Thirdly, available funds have been distributed to territorial administrations via a digital platform – "*PA Digitale 2026*" – through which administrations can apply for and access funding and undergo check-ups and assessments in a fast and simplified manner.

Four areas are strategic to the government's strategy. The first consists of fostering the widespread adoption of key digital public services, primarily by reinforcing digital identity systems. The goal is to have at least 75% of the population with digital identities by 2026. Results have been encouraging. In 2022, 43% of Italian citizens already possess a digital identity. The adoption rate is in line with other European countries like France and Belgium and far ahead of adoption rates in German-speaking countries.

This area of intervention also includes measures aimed at fostering the digital skills of citizens and the workforce (for example via re-skilling and up-skilling the public sector workforce). With specific regard to digital skills, two public-funded programmes are available: "Digital Civil Service" kicked off in June 2021. The first phase (concluded in 2021) consisted of training 1,000 volunteers to become "digital enablers" and provide support to local projects for the promotion of citizens' digital skills. The second phase began in January 2022 and involved 10,000 volunteers. The second programme is named "*Repubblica Digitale*". This is a multi-stakeholder initiative that promotes digital skills at all levels of the Italian economy and society. The idea is to select a pool of digitalisation best practices that could be scaled-up and reused by other public administrations.

The second strategic area consists of advancing the interoperability of platforms and data services via an API catalogue that allows central and peripheral administrations, depending on their authorisation level, to draw on cloud data,

process them, and deliver services to citizens and businesses who will be asked to provide information only once.

In January 2022, for instance, the government announced the completion of the digitalisation of the civil registry, allowing Italians living in Italy and abroad to access 14 documents in digital format. Another example, digital wallets, is an area where Italy has taken a leading role in Europe. The Italian public mobile wallet "IO" – featuring notices and communication from public administrations regarding application deadlines, documents, and payments – went from around 10 million downloads in 2021 to 31 million downloads in 2022. An average of 6 million users access it on a regular basis. The App currently hosts 6,895 public administrations and offers 77,000 services to citizens and businesses. A monthly average of almost €5 billion in financial transactions is done through another payment facility (*PagoPA*) to central and local public administrations.

The third area concerns securing digital data, via a cloud infrastructure hosting all the information held by public administrations. The national cloud strategy was released in September 2021. The first public tender for cloud providers was published and awarded in 2022. The Public-Private Partnership for cloud infrastructure was signed on August 2022. This cloud infrastructure will be responsible for the expansion of secure, energy-efficient and affordable data processing capacities. The government aims to exploit the value of data through data interoperability and effective implementation of the once-only principle: by making databases interoperable and accessible, it will allow central and peripheral administrations to draw on cloud data, process them and provide services to citizens and businesses.

The fourth and final area involves the scaling up of innovative private solutions capable of smoothing administrative procedures. The GovTech start-ups that play a central role in our national AI strategy are a case in point. On this subject, it is worth remembering that the EU as a whole is not competitive

on AI. Out of 10 cutting-edge technologies (including AI, quantum computing, cloud, etc.) the EU currently leads only on 2: Next-Gen materials and Cleantech. For this reason, the EU AI Act has been designed to boost research and industrial development while ensuring safety and fundamental rights. Investments mobilised from the private sector and EU Member States are expected to reach an annual volume of €20 billion over the next decade.

E-Health

The last area of intervention relates to e-health. There are €15.63 billion available in the Italian NRRP for this area. One part of these funds is intended to modernise and digitise the health system – and specifically to renew digital systems and ensure dissemination of electronic health records.

Electronic health records have become operational in all Italian regions and have been activated by the large majority of citizens. In 2022, the government started to work on improving the level of uptake by both people and healthcare professionals and on reducing variations across regions. Public investments focused firstly on supporting the completion and interoperability across regional systems of electronic health records and data usage for health risk monitoring (€1.7 billion available), secondly on boosting the use of telemedicine solutions (€1.3 billion), and thirdly on the digital upgrading of hospitals and diagnostic equipment (€1.5 billion).

Looking Ahead: 2023 and Beyond

Both NGEU and national RRPs have introduced a new model to foster transformation, sustain economic upswing, and spark a new phase of innovation in Europe. NGEU's approach to funding complements incentives (for sound national fiscal and economic policies) with reforms (to address national structural

challenges and foster innovation) and measurement/milestones agreed between Member States and the EU.

First results have been encouraging for Italy. In the 2021 DESI Index the country scaled up 5 positions. It scored particularly well on integration of digital technologies (up 12 positions from 2020) and digitalisation of public services, due to the sharp acceleration in the adoption of major enabling platforms for digital public services by public administrations. Constant check-ups and monitoring across all phases of the tendering process (from the awarding of contracts to the implementation and deployment of planned interventions) guaranteed that deadlines could be met and extra costs stemming from delays avoided (the daily cost of delays in the implementation of the NGEU is estimated at €120 million).

Yet a bumpy road lies ahead. Four key challenges remain to be addressed. The first is reducing over-regulation by reaching widespread consensus on the legal boundaries to be applied to new technologies, safeguarding the individual and collective rights of users without unduly restricting technological progress. According to the Italian Poligrafico dello Stato, there are 110,000 laws in force in our country – a shocking figure. This regulatory hypertrophy hampers attempts to implement reforms.

The second consists of combating the cultural resistance to change and experimentation embedded in public administrations. This resistance stands between defending the status quo and achieving a digital transformation that could benefit citizens and companies. The third relies on fostering experimentation by putting in place "regulatory sandboxes" to facilitate controlled experiments with innovative products. The fourth and final challenge lies in nurturing human capital by encouraging digital competencies in the population via dedicated public programmes, strengthening STEM competences in the school system and university education, and hiring managerial and technical skills in public administrations.

16. China's Digital Transition: Balancing Development, Security, and Sustainability to Lead the Fourth Industrial Revolution

Rebecca Arcesati

As of March 2022, China had installed some 1.4 million base stations for fifth-generation telecommunication mobile networks (5G).[1] Thanks to domestic industrial and R&D strength as well as a state-led campaign to "forcefully advance 5G network construction" amid the Covid-19 crisis, China has positioned itself among the global frontrunners in 5G network deployment.[2] Coverage of urban areas has been achieved, bringing the country one step closer to the target of ubiquitous connectivity and full coverage of cities and towns by 2025.

Behind this top-level embrace of digital infrastructure (also dubbed "new infrastructure") and its underlying technologies – 5G and 6G, Internet of Things (IoT), industrial internet, data centers, cloud computing, gigabit optical fiber networks, Ipv6, blockchain, Artificial Intelligence (AI) – stands a strategic government vision. Beijing has identified digitalisation, along with innovation, as the pillar of China's future socioeconomic development.[3] Taking 5G as an example, the most attractive

[1] "MIIT: this year, China will strive to reach 2 million 5G base stations" (工信部：今年我国5G基站力争突破200万个), *China News*, 8 March 2022.

[2] P. Triolo, R. Creemers, and J. Lee, "Beijing Authorities Push Rapid 5G Deployment Despite COVID-19 Headwinds", *New America*, 21 April 2021.

[3] "Outline of the 14th Five-Year Plan for Economic and Social Development

rewards will stem from the technology's ability to fuse the physical and digital worlds by enabling ultra-fast, reliable, and low-latency data transmissions, with immense innovation and productivity gains across multiple sectors such as energy, manufacturing, transportation, and healthcare. Mastering 5G and integrating it with the real economy therefore will be crucial to China's economic and industrial upgrading and the country's transition towards sustainable, green, and high-quality growth.

This ambition is fully embraced by Chinese Communist Party (CCP) General Secretary and China's President Xi Jinping, who oversaw the formulation of relevant, interlocking strategies such as Digital China and Cyber Great Power. Digital infrastructure and tech breakthroughs are seen as key to optimizing domestic governance by delivering public goods to the people while augmenting social control, hence securing the CCP's survival in power.[4] Xi's administration has further identified the Fourth Industrial Revolution as a unique opportunity for China to reclaim its rightful place as a global power. Amid an intensifying rivalry with the United States over global technological leadership, China's leaders view information infrastructure as a battleground of geopolitical competition. This diagnosis explains China's efforts to secure domestic networks and other critical information infrastructure, data, and digital industries from external threats, while simultaneously exporting digital infrastructure to reap technological and market advantages and more firmly control the systems that shape how goods, services, and information move on a global scale.

It is difficult to predict whether China's plans for the digital transition will succeed and the extent to which the country will be able to make equal progress on all its goals, from environmental sustainability to global power projection. Not

of the People's Republic of China and Long-Range Goals for 2035" (中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要), *Xinhua*, 13 March 2021.

[4] K. Drinhausen and J. Lee, *The CCP in 2021: smart governance, cyber sovereignty and tech supremacy*, MERICS, 15 June 2021.

all targets listed in policy documents will be met and some are aspirational. But the direction of travel is clear. Liberal market economies would be wise to pay attention to their impacts on global markets and, where appropriate, learn from China's approach. Although not always efficient in short-term economic terms, Beijing's comprehensive, all-of-state approach to managing the digital transformation, starting with the infrastructure layer, may offer some valuable lessons to other countries. That includes democracies seeking to compete with China's growing digital prowess, while managing the security and (geo)political risks arising from global infrastructure and networks increasingly built and controlled by Chinese vendors.

Drivers Behind the CCP's Digitisation Campaign

Key drivers behind China's concerted digitisation efforts are concerns over economic growth, national security, and geopolitical competition. During the first wave of the Covid-19 pandemic, digital technologies and industries guaranteed the resilience of China's economy by facilitating remote work, consumption and public service delivery, while helping contain the public health crisis.[5] The pandemic acted as a catalyst for digital transformation and hi-tech development, which China's leaders had already identified as priorities for bolstering national socioeconomic development and competitiveness.[6] China's government is heavily invested in the digitalisation of the real economy. The CCP banks on the deep integration of digital information infrastructure and new technologies with the country's economic and social fabric, with the aim of boosting

[5] K. von Carnap, K. Drinhausen, and K. Shi-Kupfer, "Tracing. Testing. Tweaking. Approaches to data-driven Covid-19 management in China", *MERICS China Monitor*, Mercator Institute for China Studies, June 2020.

[6] R. Arcesati, "Competing with China in the digital age," in *Towards a Principles First Approach in Europe's China Policy: Drawing lessons from the Covid-19 crisis*, MERICS Paper on China, Mercator Institute for China Studies, September 2020.

productivity and efficiency. Despite impressive strengths and successes, national "informatisation" – the Chinese policy term for the digital transformation – still faces notable shortcomings, such as insufficient integration of data-driven technologies with traditional economic sectors like agriculture and manufacturing.

Authorities want the digital sphere to underpin China's economic upgrading and transition towards innovative, high-quality growth, thus enabling the country to escape the middle-income trap. In a major speech delivered in October 2021, Xi Jinping described the digital economy as a "critical force in reorganising global [production] factor resources, reshaping global economic structures, and changing patterns of global competition".[7] Underlying this assessment is the designation of data as a new "factor of production" alongside land, labor, capital, and technology.[8] Xi believes that data and data-driven technologies, such as AI and the IoT, are giving rise to a radically new development paradigm due to the rapid fusion of the virtual and the physical domains.

Beyond economic upgrading, China's leaders view digitalisation as a panacea for optimising the CCP's domestic governance. The Digital China strategy – a centerpiece of China's 14th Five-Year Plan (FYP) – envisages a smart, informatised society, where Big Data, AI and other emerging technologies make government and public services such as healthcare and education more efficient and inclusive.[9] The 14th

[7] Xi Jinping, "Constantly strengthen, improve and expand my country's digital economy" (不断做强做优做大我国数字经济), main part of General Secretary Xi Jinping's speech at the 34th collective study session of the 19th Politburo on 18 October, 2021, *Qiushi* (Xi Jinping 2021).

[8] R. Arcesati, *China activates data in the national interest*, MERICS, 4 July 2022.

[9] Digital China is a concept and strategy directly ascribable to Xi Jinping. See, in particular, *Xinhua* (2021); Central People's Government of the People's Republic of China (中华人民共和国中央人民政府), "Xi Jinping sent a letter congratulating the opening of the first Digital China Construction Summit" (习近平致信祝贺首届数字中国建设峰会开幕), 22 April 2018; Cyberspace Administration of China (中华人民共和国国家互联网信息办公室), "Xi Jinping: from 'Digital Fujian' to 'Digital China'" (习近平：从"数字福建"

FYP for National Informatization, the blueprint for China's digital transformation over the next five years, also devotes considerable space to the digitalisation of social governance and public security work, for example through the construction of smart cities and smart community management systems.[10] Importantly, smart public service provision is part of a broader program through which the CCP aims to automate social and political control to protect state security, hence its own survival in power, in what scholar Samantha Hoffman has termed "tech-enhanced authoritarianism".[11] In the northwestern Xinjiang region, where the CCP has been waging a brutal campaign of repression and arbitrary mass detention against Muslim minorities, expansive technological infrastructure underpins an all-seeing digital surveillance system.[12]

On the international front, Beijing views the current round of technological innovation through the lens of geopolitical competition with the US. Dominating new information technologies and consolidating China's role as a Cyber Great Power are key to strengthening national competitiveness and "comprehensive power".[13] The Fourth Industrial Revolution is

到 "数字中国), 12 October 2020.

[10] R. Creemers, H. Dorwart, K. Neville, and K. Schaefer, "Translation: 14th Five-Year Plan for National Informatization Five-Year Plan", *DigiChina*, Stanford Cyber Policy Center, 24 January, 2022.

[11] S. Hoffman, "China's Tech-Enhanced Authoritarianism", Testimony before the Congressional Executive Commission on China, Hearing on "Techno-Authoritarianism: Platform for Repression in China and Abroad", 17 November 2021.

[12] J. Chan, "China's surveillance infrastructure powered by U.S. tech", *China Digital Times*, 23 November 2020; for in-depth accounts of the role of technology and smart city infrastructure in the Chinese government's repression campaign in Xinjiang, see D. Byler, "Producing 'Enemy Intelligence'": Information Infrastructure and the Smart City in Northwest China", Project MUSE, *Information & Culture*, vol. 57 no. 2, 2022, p. 197-216; and D. Byler, "Chinese Technologies of Population Management on the New Silk Road", in M. Abraham and L. Myers (Eds.), *Essays on the Rise of China and Its Policy Implications*, Washington, D.C., Woodrow Wilson International Center for Scholars, 2022, pp. 7-34.

[13] Wang Yukai (汪玉凯), "Cyber great power: the only way to modernization

a major force underpinning what China's leaders have dubbed "profound changes unseen in a century," or historic transitions that are affecting the global balance of power and bringing about unprecedented challenges and opportunities. The Xi administration is convinced that advances in disruptive digital technologies have opened a strategic window of opportunity for China to achieve global leadership and re-shape the international order in its favour.[14] Policy guidance and support for the export of PRC-origin physical and virtual information infrastructure – ranging from optical fibre cables and wireless network equipment to cloud storage systems and smart logistics platforms – particularly via the so-called 'Digital Silk Road', in part follows this logic.

Despite these strategic opportunities, the Fourth Industrial Revolution is also viewed as posing enormous security challenges for China. Particularly since Edward Snowden revealed the scale of the US government's global intelligence collection, the Chinese party state has been intensely preoccupied with reducing reliance on foreign-controlled telecom infrastructure.[15] Securing networks, critical technologies and data are top priorities of China's digital policy.

— Studying "Excerpts from Xi Jinping's discourse on cyber great power" (网络强国：走向现代化的必由之路 – 学习《习近平关于网络强国论述摘编》), *People's Daily*, 8 February 2021; E. de la Bruyère, "The Network Great-Power Strategy: A Blueprint for China's Digital Ambitions", *Roundtable in Asia Policy*, vol. 16 no. 2, The National Bureau of Asian Research, 28 April 2021.

[14] R. Doshi, "The United States, China, and the contest for the Fourth Industrial Revolution", Statement before the U.S. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Security for the Hearing "The China Challenge: Realignment of U.S. Economic Policies to Build Resiliency and Competitiveness", 30 July 2020.

[15] E. Binder and K. Northrop, "The Snowden Effect," *The Wire China*, 6 December 2020.

China strives for domestic growth and global leadership in key technologies
Digital development and innovation are key items of the 14th Five-Year Plan

CATEGORY	FOCUS AREAS	MAIN GOALS IN THE 14TH FIVE-YEAR PLAN
Key technologies	Quantum information sciences	Development of free-space quantum communication, quantum computing prototypes and quantum precision measurement technologies.
	Integrated circuits	Improvement of R&D in circuitry design, key equipment and semiconductors.
	Cloud computing	Large-scale development of cloud services, including storage, computing and virtualization.
	Big data	Innovation in big data collection, storage and analysis; development of relevant standards, applications and procedures in this field.
	Internet of Things	Development of technologies such as sensors and software necessary for autonomous vehicles, smart homes, and other areas.
	Industrial internet	Promotion of an ecosystem of "internet+ smart manufacturing," especially development of standards, safety management and research in the use of internet in industry and home appliances.
	Blockchain	Development of smart contracts, asymmetric encryption, use of blockchain in financial technology, supply chain management and government services.
	AI	Development of dedicated chips for AI, deep learning, algorithmic decision-making, as well as speech, image and video recognition.
	Virtual reality and augmented reality	Development of VR/AR and VR/AR-based software and hardware solutions.
Product application	Smart transportation	Autonomous driving, smart management of infrastructure (e.g. traffic signals) and the use of smart tools in airports, ports, etc.
	Smart resources	Use of smart tools for efficient resource management and extraction, such as in mines, oil and gas fields.
	Smart manufacturing	Development of technologies such as networked equipment, digital production links, intelligent supply chain management, etc.
	Smart agriculture and water resources	Promotion of technologies for precision-use of agricultural resources (e.g. seeds, fertilizier, pesticides); construction of a "smart water conservation systems."
	Smart education	Integration of online courses and other digital teaching tools, also to improve quality of rural education.
	Smart medicine and health care	Development of smart medical devices and technologies to help diagnosis and supervision. Establishment of electronic health and medical records, digital prescriptions, etc. and promotion of data sharing across institutions.
	Smart neighborhoods	Integration of government service platforms, emergency systems and smart monitoring systems for residential communities.
	Smart household appliances	Development of technologies such as voice control, remote control of home appliances, e.g. smart lighting, security monitoring, wearables and service robots.
	Smart government services	Development of "one-stop" online government services as well as electronic certificates, signatures and files; improvement of review systems.

Source: K. Drinhausen and J. Lee, "The CCP in 2021: smart governance, cyber sovereignty and tech supremacy," The CCP's next century: expanding economic control, digital governance and national security, MERICS Paper on China, Mercator Institute for China Studies, June 2021.

First, while the country has built the world's most powerful censorship and digitally enabled surveillance apparatus, expert assessments of its cyber capabilities find consistent weaknesses in cyber defenses.[16] These weaknesses explain longstanding efforts to promote "secure and controllable" equipment and software in information and communication technology (ICT) procurement – by favoring indigenous solutions over foreign ones – as well as the recently beefed-up rules on protecting national critical information infrastructure.[17]

Related to the above is Beijing's campaign to strengthen the innovative capabilities of China's digital industries. Since coming to power, Xi Jinping has said that "core technologies being under the control of others represents our greatest hidden danger".[18] US trade and investment restrictions on Chinese technology firms, particularly Huawei, have added further urgency to boosting national self-reliance in critical technologies and industries, such as integrated circuits and basic software. Planning documents highlight the need to achieve indigenous research and technological breakthroughs, in addition to building an "early warning system for the digital economy" to guarantee the security and resilience of key industrial and supply chains. [19]

The third line of effort is data security. China's new Data Security Law, the centerpiece of its data governance regime along with the Personal Information Protection Law, stipulates that the state should promote the development of the digital

[16] "Cyber Capabilities and National Power: A Net Assessment", International Institute for Strategic Studies, 28 June 2021.

[17] R. Creemers, S. Sacks, and G. Webster, "Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)", *DigiChina*, Stanford Cyber Policy Center, 18 August 2021.

[18] Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informatization" (在网络安全和信息化工作座谈会上的讲话), *People's Daily*, 19 April 2016.

[19] China State Council (国务院), *State Council Notice on Printing and Distributing the "14th Five-Year" Plan for the Development of the Digital Economy* (国务院关于印发"十四五"数字经济发展规划的通), 12 December 2021.

economy, but also establishes a hierarchical protection system for different data classes according to their respective importance for national security.[20] The party state views data and information as strategic resources to be protected and harnessed, with the ultimate goal of preserving and expanding its own power.[21] This strategic thinking is important to consider for countries that are choosing Chinese vendors to power their own digital transformation, as later sections of this chapter will discuss.

In sum, China is carefully balancing development and security in its bid to dominate the Fourth Industrial Revolution. But there is a third dimension – environmental sustainability – which is deeply intertwined with the digital transition. The next section will introduce the country's 'new infrastructure' campaign and examine how it might interact with its decarbonisation targets.

China's "New Infrastructure" Campaign and the Sustainability Question

Beijing has a broad range of ambitions and, as explained earlier, it is not always clear which will take priority when choices need to be made. This section takes a closer look at China's lofty targets for digital infrastructure rollout over the next five years and highlights their possible relevance for the country's green development agenda, providing a general picture of how

[20] National People's Congress of the People's Republic of China (全国人民代表会), *Data Security Law of the People's Republic of China* (中华人民共和国数据安全法), 10 June 2021.

[21] This consensus had already begun forming prior to the official designation of data as a factor of production, see People's Daily Online (人民网), "National Big Data Strategy – Xi Jinping and the fourteen major strategies of the '13th Five-Year Plan'" (国家大数据战略 – 习近平与"十三五"十四大战略), 12 November 2015; for an in-depth discussion of the role of data within the PRC's national security strategy, see in particular S. Hoffman and N. Attrill, "Mapping China's Technology Giants: Supply chains and the global data collection ecosystem", Australian Strategic Policy Institute, 8 June 2021.

the Chinese political system tends to deal with these kinds of tensions and uncertainties.

In response to the Covid-19 crisis and related economic headwinds Beijing doubled down on so-called "new infrastructure", placing it front and centre in its 2020 relief package.[22] This technological infrastructure officially encompasses three areas: 1) innovative infrastructure, including science and technology parks, R&D facilities, and other infrastructure supporting, science, education and research; 2) information infrastructure, which includes 5G, IoT, industrial internet, cloud computing, blockchain, AI, data centres, and internet network infrastructure; and 3) integrated infrastructure, such as charging stations for electric vehicles (Evs), ultra-high voltage (UHV) power transmission, and other applications of advanced technologies to upgrade traditional infrastructure.[23] Such infrastructure is expected to serve multiple, interconnected policy goals, such as job creation, green development, industrial upgrading and, ultimately, productivity increases and greater national competitiveness in emerging technology fields.

Digital infrastructure still remains a top priority. Infrastructure, Xi Jinping highlighted, shall become "high-speed, ubiquitous, intelligent and comprehensive". It should "have 5G networks, a nationwide integrated data centre system, and the national industrial internet as starting points and integrate space and earth, the cloud and networks, be intelligent and agile, green and low-carbon, secure and controllable, and connect the "main arteries" of information for economic and social development".[24] In April, a top-level meeting on of

[22] C. Meinhardt, "China bets on 'new infrastructure' to pull the economy out of post-Covid doldrums", Mercator Institute for China Studies, 4 June 2020.

[23] National Development and Reform Commission (国家发展和改革委员会), "The National Development and Reform Commission held its April press conference presenting the macroeconomic operational situation and responding to pressing questions" (国家发展改革委举行4月份新闻发布会介绍宏观经济运行情况并回应热点问题), 20 April 2020.

[24] Xi Jinping (2021).

CCP leaders on the economy reiterated the importance of technological infrastructure such as supercomputing, cloud, and broadband internet access.[25]

A Chinese industry research firm estimated that new infrastructure investment will reach CNY 1.7 trillion in 2022, up 11.5% from 2021.[26] The MIIT's 14th FYP for the ICT industry set ambitious targets for 2025, such as growing total ICT infrastructure investment from the 2020 figure of CNY 2.5 trillion to CNY 3.7 trillion and expanding data centre computing power from 90 to 300 ExaFLOPS (see Figure 13.1).[27] Progress shall be made on deepening applications of 5G, the IoT and cloud computing across multiple sectors, such as transportation, urban management, manufacturing, agriculture, water, and energy conservation.[28] China is also devoting considerable efforts towards building a domestic industrial ecosystem around BeiDou,[29] the indigenous satellite navigation system used for anything from monitoring land erosion to connecting smart transport networks – by 2025, Beijing wants intelligent connected vehicle sales to account for 50% of all vehicle sales.[30] Meanwhile, early research efforts into 6G, the next generation mobile network technology, are starting to pay out.[31]

---

[25] F. Tang, "China's big new infrastructure plan prioritises national security in face of 'extreme conditions' at home, abroad", *South China Morning Post*, 28 April 2022.

[26] "Policy support – infrastructure investment will accelerate" ("政策力挺 基建投资将跑出"加速度"), *Xinhua*, 6 May 2022.

[27] Ministry of Industry and Information Technology (工业和信息化部), *Ministry of Industry and Information Technology Notice on Printing and Distributing the "14th Five-Year" Development Plan for the Information and Communication Technology Industry* (工业和信息化部关于印发"十四五"信息通信行业发展规划的通知), 11 November 2021.

[28] DigiChina (2022).

[29] "Beidou system high on agenda", *China Daily*, 7 April 2022

[30] "Roadmap lays out path for connected vehicles", *China Daily*, 16 November 2020.

[31] J.P. Tomàs, "Chinese lab claims breakthrough in '6G' mobile technology", *RCRWireless News*, 7 January 2022.

Tab. 16.1 - Key Targets For The Digital Transition During The 14th Five-Year Plan Period

CATEGORY	FOCUS AREA / INDICATOR	2020	2025
General targets	Digital China Development Index	85	95
	Scale of netizens (million)	989	1200
Technological innovation	Added value of core digital economy industries as percentage of GDP	7.8	10
	Cumulative investment in the ICT industry (trillions of yuan)	2.5	3.7
	New-generation ICT industry invention patent holdings per 10000 inhabitants	2.7	5.2
	ICT project investment proportion of all social fixed asset investment (%)	3.5 (2019)	5.8
	Strength of R&D investment in the computer, telecommunications and other electronic equipment manufacturing sectors (%)	2.35	3.2
	R&D expenditure of basic telecom enterprises as a percentage of revenues (%)	3.6	4.5
	Nationwide number of high and new technology enterprises (1000)	275	450
	Software and ICT service industry volume (trillions of yuan)	8.16	14
	ICT service industry volume (trillions of yuan, in 2019 current prices)	1.5	3.7
Infrastructure	5G user adoption rate (%)	15	56
	Number of 5G base stations every 10000 people	5	26
	5G penetration rate in administrative villages (%)	0	80
	Number of 5G virtual private networks (VPNs)	800	5000
	1000M and higher-speed optical fibre access users (1000 households)	6400	60000
	Number of terminal connections to telecommunication networks (billion)	32	45

	Global internet access bandwidth (terabytes per second)	7.1	48
	Ipv6 active users (million)	462	800
	Share of IpV6 mobile internet traffic (%)	17.2	70
	Data center computing power (exaFLOPS)	90	300
	10 gigabits per second (10G-PON) and higher passive optical network ports (million)	3.2	12
Sectoral applications	Proportion of completely digitized enterprises in critical operational segments (%)	48.3	60
	Enterprise industrial equipment cloud usage rate (%)	13.1	30
	Number of public service nodes for industrial IoT identity resolutions	96	150
	Industrial internet platform usage penetration (%)	14.7	45
	Number of industrial internet identification registrations (billion)	94	500
	Online retail value (yuan trillions)	11.76	17
	Scale of electronic transactions (yuan trillions)	37.21	46
	Information consumption scale (yuan trillions)	5.8	7.5
	E-government service real-name usage scale (million)	400	800
	Provincial-level administrative licensing online handling rate (%)	80	90
	E-litigation proportion (%)	18	30
Energy conservation	Range of total energy consumption decline for enterprise telecommunication services (15%)	---	---
	Power usage effectiveness of newly constructed large and very large data centres (PUE)	1.4	-1.3

Source: MERICS based on the 14th Five-Year Plan for National Informatization, 14th Five-Year Plan for the Development of the Digital Economy, and 14th Five-Year Plan for the Development of the ICT Industry.

Given these ambitions, it is worth considering how China's ambitions for its digital economy relate to its similarly lofty targets for green and low-carbon development. Beijing's greening agenda is closely tied to its plans for technological innovation and high-tech leadership. A strategic policy focus and sustained R&D investment have produced significant breakthroughs in green technologies, such as renewable energy technologies.[32] Another area where government support and corporate innovation have clearly paid off is green mobility. China has become a formidable innovation hub for the EV industry value chain.[33] The emerging internet of vehicles (IoV) is, also rapidly forging ahead, thanks in part to investment in supporting infrastructure and efforts to formulate cybersecurity and data protection standards.[34] So long as they are powered by clean electricity and energy-saving battery technologies, autonomous vehicles can contribute to GHG emission reduction.

Yet, connected vehicles embody a major challenge facing China's digital transition: new infrastructure, such as 5G networks and data centers, requires lots of energy for round-the-clock operation and cooling of the equipment. China's data centre power consumption was projected to grow 66% by 2023, producing an amount of carbon emissions equivalent to those of a medium-sized country unless China's current energy

[32] A. Holzmann and N. Grünberg., "'Greening' China: An analysis of Beijing's sustainable development strategies", Mercator Institute for China Studies, 7 January 2021.

[33] G. Sebastian, "In the driver's seat: China's electric vehicle makers target Europe", Mercator Institute for China Studies, 1 September 2021.

[34] For example, the municipality of Shanghai has emphasized IoV infrastructure in recent years, see Shanghai People's Government (上海人民政府), *Notice of the Shanghai Municipal People's Government on Printing and Distributing the Action Plan for Promoting the Construction of New Infrastructure in Shanghai (2020-2022)* (上海市人民政府关于印发《上海市推进新型基础设施建设行动方案（2020-2022年）》的通知), 29 April 2020; Fraunhofer, "China Electric Vehicle and Connected Vehicle Security and Privacy: Government, Industry and Standardization Perspective (2015-2021)", *Survey*, July 2021.

mix changes.[35] Investment in big data centres is expected to exceed 3 trillion yuan until 2025.[36] Depending on the specific energy choices made in the new infrastructure rollout, China's digital transition could make or break its low-carbon transition.

The central government is taking steps to address the issue. Over the 14FYP period, the MIIT has further raised its requirements for data center power usage effectiveness (PUE). This will likely incentivise more provincial governments to act, as Beijing, Shanghai and Shenzhen already started doing in recent years. However, as China Dialogue reported in 2020, only a few cities were working to replace fossil fuel with renewables to power their data centres. To meet tech industries' fast-growing computing power requirements and promote green development, the National Development and Reform Commission (NDRC) is now overseeing a massive plan, first proposed in 2020 and known as "Eastern Data, Western Computing". Under the plan, eight computing hubs and 10 data centre clusters will be built. The idea is to transfer data from the more populous and economically dynamic coastal areas to resource-rich provinces in western China to improve the energy efficiency of the national data centre system.[37]

Whereas making digitalisation greener is a major challenge, digital technologies also bring enormous potential to sustainable development, in China and beyond. For example, State Grid

---

[35] H. Wang and R. Ye, "The climate cost of China's digital infrastructure rush", *China Dialogue*, 15 April 2020.

[36] "National Development and Reform Commission: Investment in big data centers expected to grow at an annual rate of more than 20% during the 14th Five-Year Plan period" (发改委：预计十四五期间大数据中心投资将以每年超20%速度增长), *Beijing News*, 15 April 2022.

[37] National Development and Reform Commission (国家发展和改革委员会), Concerning Accelerating the Construction of a Nationally Integrated Big Data Center: Guidance on Collaborative Innovation Systems (关于加快构建全国一体化大数据中心 协同创新体系的指导意见), Development and Reform of High Technology 2020, no. 1922; J. Groenewegen-Lau, "Oceans of data lift all boats: China's data centers move west", Mercator Institute for China Studies, 6 July 2022.

– the largest utility corporation in China and worldwide – is extremely advanced in the deployment of smart grids.[38] In 2019, it launched a plan to build an integrated IoT network for electricity distribution, earmarking 75 billion euros to modernise the country's grids through advanced technologies such as 5G and AI.[39] The digitalisation of utilities is also tied to the development of smart cities, an area where China has become a global leader.[40] Cities across the country have integrated the cloud-based urban management platform developed by Alibaba to mitigate traffic congestion and air pollution.[41] The same company recently made its self-developed immersion liquid cooling technology freely available to third parties to reduce the energy consumption of data centres, illustrating the crucial role tech firms will have to play in a sustainable digital transition.[42] The stakes are global: not only are Chinese tech companies also driving China's digital transformation, but increasingly also that of other countries around the world, especially in the Global South.

[38] Smart grids are electrical networks that leverage digital technologies and advanced metering infrastructure to improve the two-way flow of energy and data between a utility and its consumers, allowing for more smooth and efficient power transmission and consumption.

[39] State Grid Corporation of China, "Internet of Things in Electricity", White Paper, 2019; "China's largest 5G smart grid project complete", China.org.cn, 23 July 2020.

[40] K. Atha et al. "China's Smart Cities Development", Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, January 2020.

[41] D. Wang, "Beijing meets City Brain" (北京遇上城市大脑), *Leiphone*, 21 August 2020.

[42] Alibaba Cloud, "Alibaba Group Joins Low Carbon Patent Pledge to Accelerate the Adoption of Green Technology", 26 April 2022.

China's Digital Silk Road Is Reshaping Global Connectivity

Thanks to a combination of commercial initiatives and massive state support, China has emerged as a major exporter of digital infrastructure.[43] This is visible on the African continent, where it was estimated that some 70% of 4G networks have been built on Huawei's components.[44] Under the oceans, one of the world's top providers of cable systems is a Chinese company, Hengtong Group (via its majority-owned HMN Technologies), while in space China's BeiDou system has surpassed the accuracy of GPS in the Asia-Pacific region.[45] While Chinese ICT firms began their internationalisation journey in the 2000s, since 2015 Beijing has elevated the role of digital technologies in its infrastructure foreign policy via the Digital Silk Road (DSR), or the technology dimension of the Belt and Road Initiative (BRI), Xi Jinping's signature foreign policy initiative. By providing a strategic umbrella for the global projects of Chinese tech firms in areas ranging from subsea cables and network broadbands to smart cities, smart policing platforms, and the digitalisation of logistics and trade, Beijing hopes to align them with its geo-economic, technology, and geopolitical objectives.[46]

---

[43] Concerning the role of Chinese state credit in supporting the global expansion of Chinese network wireless infrastructure providers, see in particular this study on Huawei: M. Hart and J. Link, "There Is a Solution to the Huawei Challenge", Center for a New American Progress, 14 October 2020.

[44] A. MackInnon, "For Africa, Chinese-Built Internet Is Better Than No Internet at All", *Foreign Policy*, 19 March 2019.

[45] HMN Technologies, "Experience"; "Mapping China's Digital Silk Road", Reconnecting Asia, Center for Strategic and International Studies, 19 October 2021.

[46] Accurate and reliable estimates of DSR-related investments are hard to come by, given the murky scope of the initiative. Some estimates have put the total value of DSR investments at $79 billion (as of 2019), although the count also included credit line agreements which had not necessarily been put to use. See S. Presso, "China's Digital Silk Road Is Looking More Like an Iron Curtain Is Looking More Like an Iron Curtain", *Bloomberg*, 10 January 2019. Others have calculated the value of Chinese state loans for ICT infrastructure projects on the

Much commentary frames all commercial investments by Chinese internet giants such as Alibaba or Tencent as an extension of China's central government policy and strategy. However, official language on the DSR tends to emphasise two dimensions (in addition to regulatory and governance alignment), namely infrastructure and cooperation on the digitalisation of the real economy. China's Informatisation FYP lists the following DSR-related tasks: 1) improve land, sea, and space-based telecommunication network infrastructure and 2) promote "applied infrastructure" in areas such as data centres, the IoT, and industrial internet.[47] Xi Jinping articulated this second objective in a 2017 speech, calling for the integration of new technologies such as AI, cloud computing, smart cities, quantum computing, big data, and nanotechnology into the BRI to foster innovation-driven development.[48]

Maintaining and securing connectivity has arguably become more urgent, since China's bandwidth usage is growing against the backdrop of rising geopolitical tensions around digital infrastructure. US authorities have vetoed several undersea cable projects with American involvement in the Asia-Pacific region, rerouting them away from Hong Kong due to concerns with Chinese government access to data traffic.[49] As scholar Charles Mok suggests, Beijing's decision to create an "international data free trade port" for the Greater Bay Area (GBA) in Nansha, Guangdong province, which will include cross-border data transfer facilities and subsea cables, may be viewed as an attempt to seek alternative digital connections,

African continent, estimating a total of arriving at the figure of $10.2 billion over the 2000-18 period. Tugendhat and J. Voo, "China's Digital Silk Road in Africa and the Future of Internet Governance", Working Paper No. 2021/50, China Africa Research Initiative, School of Advanced International Studies, Johns Hopkins University, Washington, DC.

[47] DigiChina (2022).

[48] Xi Jinping (2021).

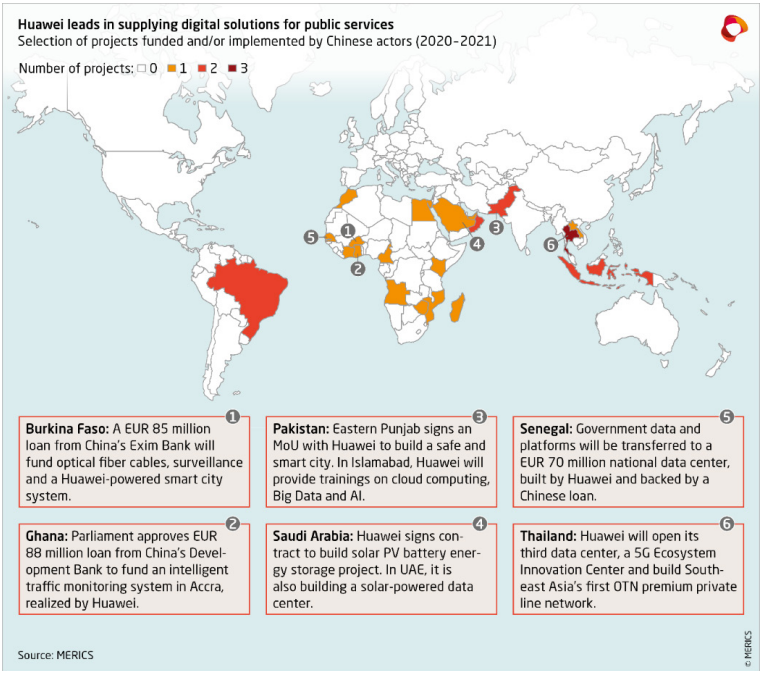
[49] M. Hui, "A Chinese firm is giving up on its long delayed US-Hong Kong undersea cable", *Quartz*, 4 March 2022.

possibly with BRI countries.[50] While it remains to be seen whether this strategy will succeed, these developments, much like the restrictions on Chinese 5G equipment vendors across most advanced economies, point to the emergence of 'splintered' digital ecosystems increasingly shaped by national security interests and great power competition.

The second dimension of the DSR, digitalising the real economy, falls under the "digital economy cooperation" rubric – essentially the web of efforts by China's central and local government bureaucracies to forge deeper links between Chinese technologies and digital ecosystems worldwide. It also ties with a major theme in China's cyber diplomacy, namely bridging digital divides in the Global South where demand for digital connectivity is highest. Multi-ministry guidelines issued last year encouraged Chinese digital firms to participate in the upgrading of traditional infrastructure such as municipal administration, transportation, energy, power, and water conservancy in third countries.[51]

[50] C. Mok, "Geopolitics Reshaping the Internet in East Asia", *Friedrich Naumann Foundation*, 15 June 2022.

[51] Ministry of Commerce, Office of the Central Commission for Cybersecurity and Informatization, and Ministry of Industry and Information Technology, *Notice of the Ministry of Commerce, Office of the Central Commission for Cybersecurity and Informatization and Ministry of Industry and Information Technology on Printing and Distributing the "Work Guidelines on Outward Investment and Cooperation in the Digital Economy* (商务部、中央网信办、工业和信息化关于印发《数字经济对外投资合作工作指引》的通知), August 2021.



Numerous countries have chosen to give Chinese vendors a significant role in their digital transformation plans. In October 2020, for example, the Ivorian government tasked Huawei with assisting in designing the national digital economy and broadband development strategies.[52] A year later, state-owned China National Technology Corporation was contracted to build two data centres to support the country's e-government system.[53] In the past, Cote d'Ivoire had already received Chinese government loans to introduced a Huawei-built e-government data centre, an optical fiber cable, and a "safe" city network of video surveillance cameras which monitors urban crime and

[52] "Cote d'Ivoire strengthens ICT sector with Huawei", *China Daily*, 13 October 2020.

[53] Seetao, "CNTIC signed a contract for the National Data Center project in Côte d'Ivoire", 29 September 2021.

traffic. [54] Tying in with China's government discourse around fostering a high-quality and sustainable development of the BRI, Huawei also has been making headways into the smart energy business, signing major energy storage and low-carbon data centre projects in the Middle East. Beside utilities, Chinese firms are active in other public sector verticals, such as health and education, not only through commercial relationships, but also by forging applied research partnerships in emerging technology fields such as machine learning and cloud computing,[55] or investing in ICT innovation ecosystems locally.[56]

As the "new infrastructure" campaign finds its outward dimension in the DSR, China is positioning itself to reap the technological, commercial, and strategic rewards from optimised connections with fast-growing digital ecosystems worldwide. The size of Africa's digital economy, for example, is set to reach €681 billion by 2050.[57] Against the backdrop of geopolitical tensions and sharpened technological competition with the US and many of its allies, China is focusing on creating a secure and controllable digital ecosystem. Such ecosystem should be ias insulated from external threats and disruptions as it is possible, but still interoperable and carefully integrated with those of other countries, especially BRI partners to which China can export indigenous technology, infrastructure, platforms, and even the underlying technical standards and associated regulatory and governance approaches. The internationalisation of domestic firms – even when it follows commercial motives – is key to strengthening China's national competitiveness in the technologies and applications underpinning the Fourth Industrial Revolution.

---

[54] https://china.aiddata.org/projects/715/; https://china.aiddata.org/projects/53273/

[55] Examples: Nanyang Technological University Singapore, Alibaba-NTU Singapore Joint Research Institute, https://www.ntu.edu.sg/alibaba-ntu-jri; Yitu, "Yitu Technology opens AI R&D center in Singapore", 31 January 2019.

[56] Huawei, "Huawei Announces New OpenLab in Cairo to Build ICT Ecosystem in Northern Africa", 11 December 2017.

[57] T. Kene-Okafor, "New report examines Africa's growth in the digital economy and VC investment landscape", *TechCrunch*, 8 June 2022.

Conclusion

Digital technologies are no panacea for sustainable development. Technology adoption can only enable sustainable, high-quality growth insofar as it is accompanied by sound policy and careful implementation. In this regard, it is not apparent that the new infrastructure frenzy will manage to avoid the pitfalls of previous infrastructure stimulus packages, which have often resulted in unproductive investments and plunged local governments into debt. The NDRC expects the scale of new infrastructure investment to exceed 15 trillion yuan during the 14th FYP period.[58] As scholar Pierre Sel observes, China's smart city campaign has often proven to be an exercise in "window dressing," with many wasteful and useless projects.[59] Against this backdrop, a challenge for China's digital infrastructure rollout will lie in viable execution and coordination between the central and local governments.

Another challenge for China stems from its enduring reliance on foreign inputs, which makes its digital ecosystem vulnerable to external shock and the weaponisation of supply chains. US export controls on advanced chipsets and semiconductor technology, which have been limited and particularly targeted at Huawei's 5G business, have not stopped China's new infrastructure deployment.[60] However, Beijing's ambitions to dominate the Fourth Industrial Revolution and foster a more self-reliant, secure, and controllable digital space are constrained by dependencies on foreign hardware and software. China's AI industry, for example, still relies significantly on Western

[58] "Financial and economic energy – Central and local governments frequently put forward 'new infrastructure' to ignite the engine of high-quality economic development in the new year" (【财经政能量】央地政策频出 "新基建"点燃新年经济高质量发展引擎), *Xinhua*, 18 February 2022.

[59] P. Sel, "Smart Window Dressing for China's Urban Life", in *How AI Will Transform China*, in *China Trends* no. 10, Institut Montaigne, November 2021.

[60] Dell'Oro Group, "China 5G Deployments Drive Mobile Core Networks to Growth in 1Q 2022, According to Dell'Oro Group", 25 May 2022.

chips (especially graphic processing units, GPUs) and cutting-edge programming frameworks. Technology giants and the government are joining forces to break these dependencies and generate innovation breakthroughs. In some areas, it is likely that China's digital industries will manage to catch up and achieve significant levels of self-sufficiency in the medium to long term. However, future technology export controls enacted by advanced economies could change the picture.

Notwithstanding this unswerving commitment to indigenous innovation, Beijing's securitised approach to the digital sphere could stand in the way of both development and sustainability. The country's digital surveillance state is consuming a sheer number of resources, with some localities allocating more funds for that than environmental protection.[61] China's leaders seem confident about their ability to manage the tradeoff between development and security. Yet, increasingly burdensome data localisation requirements, coupled with legally codified channels for state authorities to access data belonging to companies and individuals, cast doubts over China's future integration with the rest of the world in the digital sphere. Additionally, an exaggerated threat assessment can generate insecurity, for example when cyber defences are weakened for the sake of controlling information flows.[62]

Despite these challenges and limitations, China's approach to managing the digital transition may offer some useful learnings to liberal market economies in Europe and elsewhere. China's government has taken a strategic and comprehensive approach to information infrastructure, combining long-term planning, financial firepower, digital industrial policy, and the orchestration of transnational digital ecosystems with developing and emerging economies. It is also working to tackle the environmental challenges associated with digitalisation,

[61] J. Batke and M. Ohlberg, "Budgeting for Surveillance", *ChinaFile*, 30 October 2020.

[62] V. Weber, "How China's Control of Information is a Cyber Weakness", *Lawfare*, 12 November 2020.

such as data centre energy consumption. Importantly, private sector innovation is being channeled to drive innovation and the digitalisation of the real economy, from transport to electricity to elderly care, in line with Beijing's strategic objectives. The recent regulatory crackdown on China's consumer internet sector in part follows this logic.[63]

Moreover, the growing penetration of state-owned or state-linked Chinese companies into digital infrastructure networks overseas is set to grant China not only economic advantages, but also greater control over the systems that shape how goods, services, and information move on a global scale. In a world where entire economies and societies are becoming connected through the IoT, infrastructure power can allow a country to control trade and logistics networks, collect intelligence, prevail in a military conflict, or exploit technological dependencies for geopolitical gain. Just as Beijing increasingly distrusts foreign technology, provisions in Chinese law allowing for broad state access to data stored in and outside the country on national security grounds have fuelled justified concerns in the West regarding the DSR and vendors such as Huawei.[64]

Yet, Chinese digital infrastructure exports will continue to be welcomed in large parts of the world, especially insofar as governments in developing countries view them as solutions to unmet connectivity and development needs. Recent announcements from the transatlantic Trade and Technology Council (TTC) and G7 summit meetings in May and June, respectively, indicate that liberal democracies have recognised the strategic significance of supporting the digital transformation in low- and middle-income countries, in the form of public financing for secure and sustainable ICT

[63] "Digital industry + Hong Kong's new Chief Executive + Economic downward spiral", *MERICS China Essentials*, Mercator Institute for China Studies, 12 May 2022.

[64] D. Cave, "The African Union headquarters hack and Australia's 5G network", *ASPI Strategist*, 13 July 2018; J. Barret, "Exclusive: U.S. warns Pacific islands about Chinese bid for undersea cable project – sources", *Reuters*, 17 December 2020.

infrastructure and services.[65] However, concrete announcements of new commitments are still mostly lacking. As China was an early mover in the geopolitical competition around digital connectivity, the West urgently needs to catch up.

[65] European Commission, "EU-US Trade and Technology Council: strengthening our renewed partnership in turbulent times", Press Corner, 16 May 2022; The White House, "Fact Sheet: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment", Statements and Releases, 26 June 2022.

17. US Relaunching Competitiveness at Home and Abroad

Julian Mueller-Kaler

The consequences of today's technological revolutions are playing out on two levels. On the one hand, they substantially shape the composition of our societies, and on the other, spur an ever intensifying international competition. Unlike in the past, where the development of new tech applications was primarily seen through the lenses of economic growth and commercial innovation, high tech has come to signify high politics, too. This change is particularly visible with the second wave of digital innovations, which are not only more systemic in reach, but have the ability to determine future economic status, technological sovereignty, and respective security environments of every country and state conglomerate. With a rising China that increasingly challenges the American-lead liberal international order, it is the development of AI, quantum computing, and 6G that turns technology into the new playing field for great power competition, with both the old hegemon as well as the Asian giant striving for digital supremacy and spheres of economic influence.[1]

The ensuing economic decoupling poses an economic thread to many third parties. After years of globalisation and the reduction of tariffs and non-tariff trade barriers, the world has become so intertwined and interconnected that fights between

[1] M. Burrows et. al., "Unpacking the Geopolitics of Technology", Atlantic Council, 8 December 2021.

the two largest economies come with a heavy price tag for global growth and export oriented industries, particularly in Europe, where close economic ties with China enabled huge corporate profit margins and protected the middle class. In worrying about an escalating rivalry, many countries and state conglomerates have started to pursue their own digital sovereignty, yet they are finding themselves on the sidelines, lagging the necessary tools to persist in the global race of tech development, innovation, and cyber capabilities.[2]

Much like during the last *Cold War* and to satisfy the moral commitment of American foreign policy, many argue that the intensifying rivalry between the United States and China must also be seen through the lens of ideology, making it a clash of systems that distinguishes between authoritarianism on the one side and democracy on the other. Ultimately, the fate of each system will depend on more than just competitiveness, innovation, and efficiency increases, as the ability to mitigate negative externalities that come with new industrial revolutions is increasingly defining destiny. It is within these parameters that one has to evaluate the challenging quest of digital transformation, both to boost US growth and maintain American leadership in the world.

The Challenge at Home

The Biden administration is committed to advance competitiveness and increase potential for tech innovation within the United States for a number of reasons: First, to outcompete China and continue to lead the world in technological development. Second, to build a more tech-skilled, inclusive workforce and stop the ongoing deterioration of the American middle class. And third, to catch up in erecting a green economy and benefiting economically from measures to

[2] M. Burrows and J. Mueller-Kaler, "Smart Partnerships amid Great Power Competition", Atlantic Council, 12 January 2021.

combat climate change. It goes without saying that the latter two objectives were absent during the Trump administration and might alter again come the US presidential election in 2024. The bottom line of American policy, however, won't change anytime soon. Namely, stunting China's rise as a tech leader, slowing the PRC's economic growth, and luring manufacturing, which includes high-tech industries, back to the United States. *Foreign policy for the middle class* exemplifies thereby a continuation of economic protectionism and industrial policy. And with recent legislations such as the CHIPS and Science Act or the Inflation Reduction Act, one could even argue that in order to outcompete China, the United States is becoming more like it.

Relaunching American competitiveness, making the workforce fit for a digital future, and protecting the country from the erosion of liberal democracy along the way is going to be a challenging endeavor, as technology will inevitably transform many sectors of life. Warnings that significant portions of American jobs will be automated within the next decade or two have not only been expressed by Oxford University researchers Carl Benedikt Frey and Michael Osborne some ten years ago,[3] but more recent studies inter alia from the European think tank Bruegel, the McKinsey Global Institute, and the Organisation for Economic Co-operation and Development (OECD) show the potential of automation affecting between fourteen and fifty-four percent of jobs in the near future.

Even if job ramifications derived from increasing automation lie at the lower end of predicted disruptions, the adaptation of digitalisation and emerging technologies accelerate ongoing trends – with potentially major political consequences. Four years ago, a study from the Brookings Institution indicated that since 2010, the fifty-three largest US metropolitan areas accounted for roughly two-thirds of increase in economic output and almost three-quarters of job growth, despite making up just

[3] C. Frey and M. Osborne, "The Future of Employment: How Susceptible Are Jobs to Computerization?", Oxford Martin School, Oxford University, 2013.

56% of the country's population.[4] Since then, such economic and job-growth patterns only intensified and small-town areas saw their share of the nation's economic output shrink by 6.5% between 2010 and 2016.[5] Biden's winning base of 520 counties in the 2020 presidential election, for example, encompassed a staggering 71% of America's economic activity, while Trump's losing base of 2,564 counties represented just short of twenty-nine percent of the economy.[6]

With the transformation from a production-based to a service-based economy, the geography of growth has undoubtedly shifted, and technical advancements such as digitalisation or automation will further expedite the process. A trend that becomes particularly problematic, if people no longer move to economic opportunity, as Richard Florida points out is increasingly the case in the United States.[7] Given the number of citizens that already suffer from a strong sense of economic decline and their specific location in rural, politically overrepresented areas, it is no surprise that economic transformations brought social cleavages wich continue to spawn frightening externalities. The lack of upward social mobility, the experience of entrenched poverty despite having a job, and the consequences of a health care system that cares more about profit than patients have hollowed out the promise of the American dream, deepened small-town resentment of coastal, cosmopolitan elites, and caused rust-belt Americans to elect Donald J. Trump as president in 2016.[8]

---

[4] M. Muro and J. Whiton, "Geographic Gaps Are Widening while U.S. Economic Growth Increases", Analysis of Moody's Analytics data in *The Avenue* (blog), Brookings Institution, 23 January 2018.

[5] R. Florida, "America's Polarization Threatens to Undo Us", Bloomberg Media Group, *CityLab* (newsletter and website), 25 January 2018.

[6] M. Muro et al., "Biden-voting Counties Equal 70% of America's Economy. What Does This Mean for the Nation's Political-Economic Divide?", *The Avenue* (blog), Brookings Institution, 10 November 2020.

[7] Florida (2018).

[8] C. Hendrickson et al., "Countering the Geography of Discontent: Strategies for Left-behind Places", Brookings Institution, November 2018.

To illustrate this further, not just because of the pandemic, life expectancy actually stagnated and recently declined in the United States for the sixth year in a row, making it a complete outlier in the group of economically developed countries. It sounds dystopian, but Trumpism may as well be regarded as a prelude to the political upheaval that could come from the economic and social implications of digitalisation and unregulated automation, particularly if one believes that the rise of populism mainly derives from the declining faith in the problem-solving capacity of democratic institutions. The truth is simple: Most economic hubs don't need the amount of cheap, uneducated labour that contributed to building wealth in the industrial age. Today, the availability and search for highly educated workers is centered around prosperous, big, and thriving metropolitan areas, reinforcing the vicious cycle of geographical agglomeration in many democracies, especially the United States.[9]

Reviving the Middle Class Through Innovation

It is of course too early to determine whether Biden's policies will have any effect in empowering rural communities and to what degree the government succeeds in spreading tech skills and innovation to disadvantaged communities. However, it should come as no surprise that technology and good paying jobs are at the center of the President's economic agenda, particularly when it comes to tackling climate change. Trying to counter the Republican propagated view that a transition to a green economy will lead to a loss of jobs, Biden follows the Obama administration's narrative and continues to highlight the creation of new, high-quality jobs as a center piece of his green energy push. Irrespective of such plans, facilitating a transition for many workers that have to move out of fossil fuel-dependent

[9] E. Porter, "The Hard Truths of Trying to 'Save' the Rural Economy", *New York Times*, 14 December 2018.

industries will require great effort and coordination between the public and the private sector.

Furthermore, subsequent legislation is trying to put the United States back in the center of the global electric vehicle market by subsidizing eco-friendly infrastructure, aiming to deliver thousands of electric school buses and ferries to districts across the country. The Inflation Reduction Act also tries to reenergize America's power infrastructure with substantive spending on protection against super storms, floods, wildfires, and droughts. Some of that will involve making the nation's fragmented power grid more secure and efficient, while Biden hopes to empower greater telework and less commuting with the expansion of broadband internet access, intending to lessen carbon emissions thereby.[10]

Another interesting focus is the role of technology itself, emphasised as a potential solution to climate change. The expert consensus at the White House-organised Leaders' Summit on Climate in 2021 suggested that much of the needed technology is yet to be invented or scaled. Remarks from Fatih Birol, Executive Director of the International Energy Agency, included the admission that "reaching net-zero emissions by 2050 would depend in large part on the use of technologies that were not yet ready to be used at scale, such as carbon capture and storage, and the use of clean hydrogen as fuel"[11] – a Herculean task, he added, make no mistake.

Similarly to the climate investments, subsidies for innovation and the intended on-shoring of high-tech industries follows a very similar pattern, namely the practical political side of heaping opprobrium onto the Chinese competitor. Undoubtedly, it has become a way to create consensus in a system that is increasingly defined by political trench warfare between the two major parties in Washington. To put it simple, it is a way for

[10] K. Lobosco and T. Luhby, "Here's What's in the Bipartisan Infrastructure Bill", *CNN*, 15 November 2021.

[11] "Climate Commitments Are 'Not Enough', says Birol", *World Nuclear News*, 23 April 2021.

the administration to get the Republicans as well as the public behind Biden's ambitious spending plans. Officials continuously point to the fact that US federal spending on research and development has tired in recent years, while China increases its financial commitments to R&D annually, and in big numbers. They point to rising pattern-developments in the PRC or the influence of Chinese big tech companies such as Tencent, Alibaba, or Huawei on the global market. Instrumentalising great power competition has become a successful tool for the American private sector, too, with many representatives from big tech companies arguing against antitrust laws or any kind of regulation in an environment that has turned critical towards them across the political spectrum.

The Challenge Abroad

On the international level, Biden is continuing the China-and-technology focus of the Trump administration, with one major difference: The goal of slowing Chinese growth and deterring its economic influence is no longer pursued unilaterally, but together with allies and partners in Europe and Asia. Arguing that Chinese technologies like facial recognition or the country's social credit system equals authoritarianism, helps with the Biden administration's argument that Beijing's rise as a technological superpower is a threat to the foundations of the Western liberal order – it also serves as justification for calling on allied and democratic partners to help the United States in its fight for supremacy.[12]

So far, US allies and partners have been rather reluctant to join America's anti-China club due to worries it would inflict major economic pains, even though most share the concerns about unfair Chinese trade practices as well as the country's blatant usage of technology to reassert authoritarian rule. Nevertheless,

[12] M. Burrows and J. Mueller-Kaler, "Tech Cooperation at a Precarious Junction", Atlantic Council, 14 March 2020.

many have developed such close ties with the Chinese market that a strategic retreat would not be possible without suffering significant economic losses that populations in democracies might not be willing to accept. While Europeans, for example, have adopted a compete, cooperate, and confront approach to dealing with China that enables them to collaborate when interests overlap, the debate in the United States around technologies and China is increasingly defined by national security concerns. Accordingly, both the Trump as well as the Biden Administration have been trying to cajole countries around the world into blacklisting Huawei technologies or join the US's clean network initiative. Obstacles to these efforts are primarily the fact that for many, Chinese technologies are simply the better option. For developing countries in particular, Huawei offers a cheap entrance fee for good quality 5G cellular networks – and connected economic development. Regional splits due to secondary sanctions or export control mechanisms could therefore have serious economic implications for the rest of the world.

To wich extend such economic concerns as well as the skyrocketing inflation will put a break on decoupling trends remains to be seen, but the securitisation of innovation and tech development will surely remain a constant – wich does not bode well for the future. Decision makers in Beijing see the field of emerging technologies both as a resource of social control as well as the one area in wich coequality with the United States on the global stage can be achieved sooner rather than later. They also know that without major advances in innovation, China is likely to be stuck in the middle-income trap. And after the rapid advances of the past three decades, any substantial economic slowdown would result in a plateau in household incomes, making it harder for China to achieve its goal of reaching Western living standards and undermine the legitimacy of the Communist Party. The fact that the country still lacks significant capabilities in certain high-tech areas such as computer chips and semi-conductors, combined with the

realisation in Beijing that the US is serious about its desire to slow Chinese growth and preserve American supremacy, gives them further incentives to speed up innovation capacities and increase economic influence internationally. A vicious cycle that will heavily impact the rest of the world. After years of globalisation, the world is on a path of global fragmentation with dire consequences for technological cooperation, the prospect of tackling climate change, and enabling sustainable development for the poorest members of the international community.

The question whether the competition will go off the rails entirely, depends mostly on the resilience of the respective domestic systems. Focusing on the internal dimension of international conflict is therefore of outmost importance for a critical analysis. On the one hand, failing efforts to manage the next industrial revolution right and fairly distribute its benefits, could further create negative externalities and seriously threaten American democracy, though the opportunity of getting it right, might restore the promise of free, democratic, and market oriented societies.

18. African Digital Sovereignty: Threats and Remedies

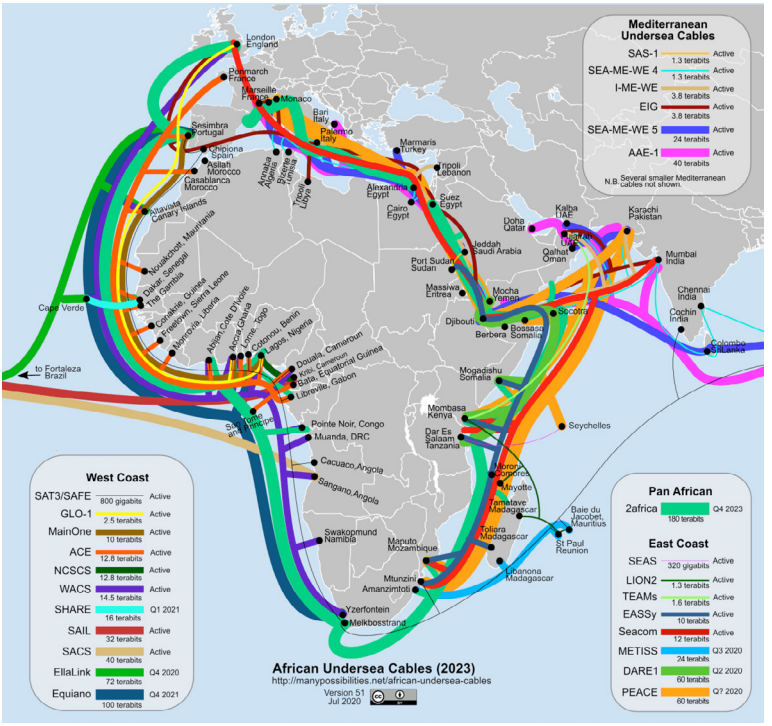
Rafiq Raji

According to Coleman (2019), "digital colonialism refers to a modern-day 'Scramble for Africa' where large-scale tech companies extract, analyze, and own user data for profit and market influence with nominal benefit to the data source" (p. 417).[1] The instinct to enact data protection laws as a bulwark hardly measures up to the challenge, argues Coleman (2019). "An analysis of Kenya's 2018 data protection bill, the General Data Protection Regulation (GDPR), and documented actions of large-scale tech companies exemplifies how those limits create several loopholes for continued digital colonialism including, historical violations of data privacy laws; limitations of sanctions; unchecked mass concentration of data, lack of competition enforcement, uninformed consent, and limits to defined nation-state privacy laws".[2]

[1] D. Coleman, "Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws", Michigan Journal of Race and Law, vol. 24, no. 2, 2019, pp. 417-39.

[2] Ibid. (p. 417).

FIG. 18.1 - AFRICAN SUBMARINE CABLE LANDINGS



Source: https://manypossibilities.net/african-undersea-cables/

It is tempting to attribute the digital scramble to the ugly western legacy of slavery and colonialism. This would be lazy and inaccurate. What Big Tech firms are looking to do in African countries started at home, until the media and academia began to call them out, with laws such as the GDPR enacted quickly thereafter. It is underpinned by surveillance capitalism, which Zuboff (2019) defines as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction and sales".[3] In other words,

[3] S. Zuboff, *The Age of Surveillance Capitalism: The fight for a human future at the new*

Big Tech sees data as raw material, in the same way as other industries see crude oil or metals as raw material, for refining into finished products of even greater value. What makes Africa particularly vulnerable, however, is a dearth of state capacity and political will to keep Big Tech in check. In the face of basic needs like food and infrastructure, African governments easily make the trade-off of focusing on these basic priorities when negotiating with western partners in exchange for concessions on data protection and ownership. Pushed by deep-pocketed Big Tech lobby groups, one of America's major requirements in its delayed trade negotiations with Kenya relates to data ownership, for instance.[4]

Tab. 18.1 – The digital divide in Africa

Digital development metric (2021)	Africa	Europe
Individuals using the internet	33%	87%
Inhabitants with a fixed telephone subscription	1%	31%
Inhabitants with a fixed broadband subscription	1%	35%
Inhabitants with a mobile cellular telephone subscription	83%	118%
Inhabitants with an active mobile-broadband subscription	41%	105%

Source: International Telecommunication Union[5]

The foreign takeover is taking many forms and faces little resistance owing to the comfort it provides for a continent long deprived of basic services. Ride-hailing apps like Uber and Bolt provide a better taxi service than the local alternatives, and without any of the hassle that characterises the latter. Netflix, a video-streaming company, provides more attractive

frontier of power, Profile, 2019.

[4] M. Omino and I. Rutenberg, "Why the US-Kenya free trade agreement negotiations set a bad precedent for data policy". *Centre for Global Development*, 1 June 2021.

[5] International Telecommunication Union, Measuring digital development: Facts and figures 2021, Geneva, ITU, 2021.

programming and a more convenient service than local media in many African countries. Google's long reach not only derives from users' emails, but also from their location, what ads they see, and the information that surfaces in their web searches. Although these services are making the lives of many Africans much more bearable, they come at great costs, because they transfer an invaluable trove of data to foreign servers, thus perpetuating the continent's continued dependence on the West. "Thus, tech corporations have expanded their products across the globe, extracting data and profit from users all around the world while concentrating power and resources in one country, the US (with China a growing competitor)".[6]

Africa Is Selling Its Digital Future for Free

As Africa lacks the capital and the know-how to build its own digital infrastructure, it has to rely on foreign development partners and their firms. Most of these are western, but increasing numbers are Asian. There is growing evidence that the continent might be mortgaging its digital future in the process, however.[7] Regulation can still work, some argue, if it is smart, fit-for-purpose and adjusted for the myriad contexts and varied circumstances of African countries.[8] But data protection laws have to be in place before the argument can be made about their efficacy. As it is, barely half of African countries have such laws, compared to almost all European countries, for instance. Hitherto overlooked, there is growing interest in the American dominance of global tech, especially as it bears all the semblance of the labour and resource colonialism of African countries in

[6] M. Kwet, "Digital colonialism is threatening the Global South", *Aljazeera*, 13 March 2019.
[7] "Digital colonialism: Cheap internet access for Africa but at what cost?", *DW*, 29 May 2019.
[8] N. Elmi, "Is Big Tech Setting Africa Back?", *Foreign Policy*, 11 November 2020.

the ugly past.[9] Supposedly free digital products and services are not really so, as they require users to grant access to their personal data free of charge, with software and data increasingly centralised in cloud systems domiciled abroad. There is growing recognition in some African countries and the broader developing world of the importance of digital sovereignty.[10] South Africa, and a number of developing economies, refused to sign the "Osaka Declaration on Digital Economy" or so-called "Osaka Track" at the G20 summit in Osaka, Japan, in June 2019, for instance, arguing that their input was not sought beforehand.[11] Senegal was the only African country mentioned in the final document, in addition to Argentina, Australia, Brazil, Canada, China, the European Union, France, Germany, Italy, Japan, Mexico, South Korea, Russia, Singapore, Thailand and Vietnam.[12]

It is easy to understand why digital sovereignty has hitherto not been taken seriously by African countries. Great enthusiasm for technology in Africa, as it has been the solution to myriad infrastructural handicaps on the continent, has enabled Big Tech to enjoy a carte blanche of sorts, with governments throwing caution to the wind to sustain their custom.[13] As there is no shock and awe of the kind associated with the military-backed economic colonialism of the past, the argument about local data ownership comes across as more than a little puzzling to the still predominantly agrarian African population and its largely conservative ruling elite.

---

[9] M. Kwet, "Digital Colonialism: The evolution of US empire", *TNI*, 4 March 2021.

[10] J. Hicks, "'Digital colonialism': why some countries want to take control of their people's data from Big Tech", *The Conversation*, 26 September 2019.

[11] M.P. Goodman, Parsing the Osaka G20 Communique, Center for Strategic & International Studies, 3 July 2019.

[12] G20, Osaka Declaration on Digital Economy, METI, 28 June 2019.

[13] C. Gorey, "How the rise of 'digital colonialism' in the age of AI threatens Africa's prosperity", *Silicon Republic*, 8 May 2020.

TAB. 18.2 – AFRICAN TELECOMMUNICATION INFRASTRUCTURE PROJECTS FINANCED BY CHINA (2010-2020)

Country	Project	Financier	Borrower	Implementation	Amount	Year
Tanzania	National ICT Broadband Backbone (NICTBB) Phase II	Exim Bank	Tanzanian government	CITCC, Huawei	$100m	2010
Cameroon	National Broadband Network Phase I: 4G mobile broadband (LTE)	Exim Bank	Cameroonian government	Huawei	$168m	2011
Kenya	National Optic Fibre Backbone Infrastructure (NOFBI) Phase II: E-government	Exim Bank	Kenyan government	Huawei	$71m	2012
Nigeria	Galaxy Backbone project for national security development system	Exim Bank	Nigerian government	Huawei	$100m	2012
Ethiopia	Telecom Transformation & Expansion (4G network & mobile expansion) 6 Circles – ZTE	Exim Bank	Ethiopian government	ZTE	$300m	2013
Ethiopia	Telecom Transformation & Expansion (4G network & mobile expansion) 7 Circles – Huawei	Exim Bank	Ethiopian government	Huawei	$800m	2013
Tanzania	National ICT Broadband Backbone (NICTBB) Phase III	Exim Bank	Tanzanian government	CITCC, Huawei	$94m	2013

Nigeria	National Information Communication Technology Infrastructure Backbone (NICTIB) Phase I	Exim Bank	Nigerian government	Huawei	$100m	2013
Guinea	National Backbone fibre optics	Exim Bank	Guinean government	Huawei	$214m	2014
Cameroon	National Telecommunications Broadband Network Project Phase II	Exim Bank	Cameroonian government	Huawei	$337m	2015
Ivory Coast	Abidjan Video Surveillance Platform	Exim Bank	Ivory Coast government	Huawei	$57m	2016
Cameroon	South Atlantic Inter Link (SAIL)	Exim Bank	Cameroonian government	Huawei	$85m	2017
Nigeria	National Information Communication Technology Infrastructure Backbone (NICTIB) Phase II	Exim Bank	Nigerian government	Huawei	$334m	2018
Sierra Leone	Fibre Optic Backbone Network Phase II	Exim Bank	Sierra Leonean government	Huawei	$30m	2019

Source: M. Agbebi, *China's digital silk road and Africa's technological future*, Council of Foreign Relations, 2022

It has taken a while for the establishment to realise that, mobile money, Uber, breaking news on social media, and all that fun and learning on the internet could be a danger to African sovereignty. Not until African leaders became subject to sanctions by Big Tech owing to their speech or actions on social media did it finally dawn on the continent's ruling class that digital sovereignty is a matter to be taken seriously.

Bridge the Digital Divide Without Losing Digital Sovereignty

Digital colonialism is driven by Big Tech's economic imperatives, as opposed to the political goals of their home governments.[14] Even so, the current political economy of global digital trade suits the west just fine, especially as efforts are afoot by America, goaded by the Big Tech lobby no doubt, to institutionalise the lopsided status quo. While the African Continental Free Trade Agreement (AfCFTA) envisages an e-commerce protocol, doubts remain about whether one will be agreed on time, as the World Trade Organisation (WTO) is working on a global protocol, or how effective it will be (when and if it is finally put in place) in repairing the state-firm and global north-south imbalances when the implementation of more pressing and basic trade protocols has been sluggish thus far.[15] "Globally, we have seen the integration and dependency of the Internet and digital technologies spread from the West and imposed on other states, the African continent in particular".[16] The Chinese variant of this digital neo-colonialism of African countries is an interesting case in point. While China guards its digital

[14] A. Birhane, "Algorithmic Colonization of Africa", *SCRIPTed*, vol. 17, no. 2, 2020, pp. 389-409.

[15] M. Kathure, "Africa's Digital Sovereignty: Elusive or a Stark Possibility through the AfCFTA?", *Afronomicslaw*, 16 June 2021.

[16] H. McDonald, "The internet as an extension of colonialism", *Security Distillery*, 4 December 2019.

sovereignty jealously, it is even more rabid than the west in planting its flag in as many places in Africa's cyberspace as possible, doing so both covertly and overtly, from eavesdropping on conversations within the walls of the African Union (AU) headquarters it financed and built, to data acquisition through backdoors in the hardware and software that its firms sell to many African firms and governments (see Table 18.2).[17] It is no coincidence, therefore, that China has also been the largest foreign investor in African infrastructure for more than a decade (see Table 18.3).

Tab. 18.3 – Foreign direct investment for sub-Saharan Africa infrastructure (2007-2020)

Source	Amount (billion of $)
China Export-Import Bank	20.1
African Development Bank	4.5
China Development Bank	2.9
International Finance Corporation	2.4
US Overseas Private Investment Corporation	1.9
Japan Bank for International Cooperation	1.7
KfW (Germany)	1.5
European Investment Bank	1.2
FMO (The Netherlands)	1.1
World Bank	0.9

Source: Quartz Africa; Centre for Global Development[18]

[17] W. Gravett, "Digital neo-colonialism: The Chinese model of internet sovereignty in Africa", *African Human Rights Law Journal*, vol. 20, 2020, pp. 125-46.
[18] K. Cheng, "Why is the US fixated on China's rise in Africa?", *Quartz Africa*, 14 April 2022.

Big Tech companies like Facebook, Google and Microsoft have also been exploiting tax loopholes in African countries to boost profits.[19] An OECD-backed effort towards a 15% global minimum tax on multinationals, which are able to evade taxes abroad more efficiently due to the increasing digitalisation of global commerce, comes with conditions that are inimical to the digital sovereignty of African countries.[20] Thankfully, many African countries have refused to endorse it. But what other ways are there to reconcile the digital divide between rich and poor countries and the digital colonialism that increasingly thrives under the guise of the former supposedly trying to bridge the gap in the latter? The nationalisation of data as a resource like minerals or crude oil to be bid for, with royalties and taxes paid upon successful licensing has been suggested.[21] In a supposedly altruistic effort to bridge the digital divide in Africa and elsewhere, Big Tech and its allies in the NGO sector "act with urgency to connect as many people as possible, as fast as possible, neglecting considerations like content, long-term sustainability, or basic literacy on important issues such as privacy and security online".[22] Civil society groups in African countries can also be part of the solution if they are technically and financially empowered, as witness the enactment of data privacy laws in 2021 by Rwanda, Zambia and Zimbabwe, as a result of civil society groups' efforts (Table 18.4).[23,24]

[19] ActionAid, $2.8bn 'tax gap' exposed by ActionAid research reveals tip of the iceberg of 'Big Tech's big tax bill' in the global south, Press release, 26 October 2020.
[20] O. Goni and L. Miyandazi, *The global minimum corporate tax deal – an African perspective*, UNDP Africa, 7 December 2021.
[21] H. Dahmm and T. Moultrie, "Avoiding the Data Colonialism Trap", *Thematic Research Network on Data and Statistics*, 22 February 2021.
[22] R.A. Pinto, "Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies", *International Journal on Human Rights*, vol. 27, 2018, pp. 15-17.
[23] L. Vargas, "Tackling digital colonialism", *Rabble*, 10 February 2022.
[24] A. Sylla, "Recent developments in African data protection laws – Outlook for 2022", *JD Supra*, 1 February 2022.

Tab. 18.4 – Examples of African countries with data protection laws

Country	Comment
Botswana	2018 Data Protection Act in effect since October 2021 envisages a data protection authority
Burkina Faso	2021 Data Protection Act
Cape Verde	2001 General Legal Framework for the Protection of Personal Data of Natural Persons invests regulatory powers in the National Commission of Data Protection
Chad	2015 Data Protection Act invests regulatory powers in the National Agency for Information Security and Electronic Certification (ANSICE)
Kenya	2019 Data Protection Act and 2021 Data Protection Regulations
Niger	2017 Data Protection Act invests regulatory powers in the High Data Protection Authority (HAPDP)
Nigeria	Data protection responsibility resides with the National Information Technology Development Agency (NITDA) governed by the 2019 Nigerian Data Protection Regulation
Rwanda	2021 Relating to the Protection of Personal Data and Privacy invests regulatory powers in the National Cybersecurity Authority (NCSA)
Senegal	2008 Data Protection Act is to be replaced with a new law
Uganda	2019 Data Protection and Privacy Act invests regulatory powers in the Personal Data Protection Office
Zambia	2021 Data Protection Act
Zimbabwe	2021 Data Protection Act invests regulatory powers in the Postal and Telecommunications Authority of Zimbabwe (POTRAZ)

Source: Adapted from Sylla's, "Recent developments in African data protection laws – Outlook for 2022" written under the sponsorship of Hogan Lovells, 2022.

Change also has to come from Big Tech itself, barring which potential regulation could be overbearing, thus weighing on the many benefits that they bring to the continent. Nanjala Nyabola, a Kenyan author and commentator on the socio-political impact of tech in Africa, puts it rather well when

she avers that "this fantasy that you can just build platforms in Silicon Valley and spread them around the world without having to engage with the realities of the societies in which you're projecting, I think, needs to be challenged at a social level".[25] For example, Facebook, whose Free Basics initiative enables free access to Facebook in 30 African countries, and which is building a sub-sea internet cable to connect 16 African countries, has lately been subject to criticism for supporting authoritarian African regimes, whose cooperation it needs to succeed on the continent.[26] What is concerning is that Big Tech has not been any more politically responsible than the dictators it props up, when it could otherwise be a force for change. Platform collusion extends the digital domination trend, which started with the privatisation of hitherto free software, which is now increasingly centralised in the servers of Big Tech abroad ("The Cloud"). Africans are thus deprived of agency in their digital experiences via data, software and platforms, and authoritarian African governments happily facilitate this situation in exchange for tech-enabled political control.[27]

Tech Rules Should Be Global and Fair

The global nature of digital technologies requires their governance to be similarly global. Currently, there is a lack of coordination and coherence, as different jurisdictions enact digital governance laws to suit their particular needs. And even as countries have been reluctant to join global initiatives, the imperative for a global framework is writ large. Still, there is a risk that such global rules might fail to take account of the unique deficiencies and vulnerabilities of poor countries,

[25] C. Tsalikis, "Nanjala Nyabola on the 'digital colonialism' transforming Kenya's political discourse", *Africa Portal*, 18 December 2019.
[26] S. Ly, "Digital Colonialism: Facebook in Eastern Africa", *London Financial*, 1 April 2021.
[27] M. Kwet, "Digital colonialism: the evolution of American empire", *ROAR*, 3 March 2021.

especially African ones. To advance this global necessity, these considerations must be borne in mind. The US-led *Declaration for the Future of the Internet* in April 2022, which has Cabo Verde, Kenya and Niger as the only African signatories thus far, is a good start, at least, as it commits to promoting and sustaining an Internet that is "open, free, global, interoperable, reliable and secure".[28] A Digital Stability Board (DSB) under the aegis of the G20, in the mould of the Financial Stability Board (FSB) it created during the global financial crisis, has also been suggested.[29] As a minimum, the DSB will coordinate the myriad digital governance standards initiatives across the world into a more coherent global whole that engenders the G20's goal of digital trust.[30]

Several proposals for global tech governance are afoot, especially as the Covid-19 pandemic shone a spotlight on the many weaknesses of the currently disparate systems and frameworks spread across the globe and the myriad gaps in them still.[31] Suspicions about the motivations of these global digital governance initiatives remain, especially as they tend to support the entrenchment of the current western hegemony of the global digital economy. The American-led Future of the Internet declaration was initially proposed as a global alliance motivated by a desire to rein in China's Huawei and other similarly Chinese-backed tech firms, for instance, but was later redesigned as a universal declaration after much criticism.[32,33]

---

[28] US Government, A declaration for the future of the internet, White House, Washington DC, 2022.

[29] R. Fay and R. Medhora, "A global governance framework for digital technologies", *G20 Insights*, 2021.

[30] Ibid.

[31] United Nations, Report of the Secretary-General: Roadmap for digital cooperation, New York, United Nations, 2020.

[32] M. Mueller, "The Declaration for the future of the internet", Internet Governance Project, 29 April 2022.

[33] M. Mueller, "Biden's alliance for the future of the internet: Mandate for a split?", Internet Governance Project, 18 January 2022.

This is not entirely without justification. China represents an emerging authoritarian vision of global digital governance that is as robust in its coherence as much as its repressive outlook, whereas the currently unwieldy liberal democratic ideal, the European GDPR, for instance, increasingly fails in its mission precisely because of a lack of global consensus.[34] In order to be effective, a global digital governance framework must not only be integrated and coherent, but also be backed by a global multi-stakeholder and consensus-based approach.[35,36]

Critically, these global mechanisms must not exacerbate the inequalities in African countries that digitalisation is helping to reduce, from financial inclusion to digital commerce, but which it is now increasingly widening owing to digital colonialism.[37] To ensure fairness and equity, the supposed weak link that most African countries are in the global economy, insofar as many continue to suffer myriad socioeconomic and political deficiencies, must be the anchor for global tech governance.[38] Thus, the growing trend of "technology solutionism" for Africa's many developmental needs should also not become the means by which they are worsened.[39] Global digital public goods must not be commercialised in any form or manner, for instance, nor should they be restrictive owing to language, content or infrastructure requirements.[40] They must be available where the people who need them the most live, at prices that are

[34] D.F. Runde and S.R. Ramanujam, Global digital governance: Here's what you need to know, Washington DC, Centre for Strategic & International Studies, 1 October 2021.

[35] L. Signe, M. Esposito, and S. Khagram, "The new urgency of global tech governance", *Project Syndicate*, 10 September 2020.

[36] World Economic Forum, Global technology governance: A multistakeholder approach, Geneva, World Economic Forum, 2019.

[37] S. Moorehead and J.M. da Silva, "Digitalisation: A double-edged sword", OECD Forum Network, 19 January 2022.

[38] N. Sambuli, "The promises, pitfalls and potential of global technology governance", OECD Forum Network, 21 February 2022.

[39] Ibid.

[40] United Nations (2020).

affordable, with users empowered with the knowledge of their utility for improving their lives and the requisite skills needed to maximise their benefits.[41]

Conclusion

African countries have been slow to catch on to the risks to their sovereignty from digital technologies that are in the overwhelming control of firms from rich countries, especially the west. While digital governance laws have underwhelmed in a couple of African countries, they could still be effective if well designed. A globalised effort is a prerequisite for effective global digital governance. Unfortunately, proposed initiatives tend to be motivated by the security and geopolitical goals of rich countries, at the expense of those of poor countries, especially African ones. Technologically disadvantaged countries must be the anchor of global digital governance initiatives to ensure equity and fairness.

[41] United Nations Conference on Trade and Development, Technology and innovation report 2021, Geneva, UNCTAD, 2021.

19. Japan's Digital Transformation: An Uphill Path

Corrado Molteni

Japan, a technological giant, risks lagging behind other advanced countries in the arena of digital transformation (DX). The issue emerged during the coronavirus pandemic, when the government struggled to coordinate the initiatives aimed at countering the spread of the contagion and in providing cash handouts and other reliefs. The adoption of different systems and platforms by public institutions, at central and local level, has in fact been a major constraint, hampering a rapid and effective response and causing delays and failures. Faced with the need to change gear and to introduce far-reaching, sweeping reforms, the governments led by Yoshihide Suga and his successor Fumio Kishida have made digital transformation a top priority of their policy agenda. A first, important step in this direction was the establishment of the Digital Agency in September 2021. Its organisation and approach are actually based on innovative principles, a break with the past procedures that have shaped the structure and working of Japanese public entities. However, it is not yet clear whether the Agency will be able to have a deep and lasting impact on the functioning of the public administration. Recent developments, including the resignation of its chief officer, are a signal of the obstacles and difficulties it is facing – impediments that could retard or even derail the attainment of its ambitious goals.

The problems related to DX are not confined to the public sector. They are also affecting the performance of private companies, often entrenched in an old mindset preventing the adoption of new business models. METI, the Ministry of Economy, Trade and Industry, responsible for the promotion of digital transformation in the business sector, has been sounding the alarm bell for quite a long time. Several documents issued by the Ministry have underlined the risk Japanese companies face if they do not act fast and with commitment. In 2018, the Ministry launched an appeal to overcome what it called the "2025 Digital Cliff", a term that is expected to create a sense of urgency and induce companies to act resolutely. The Digital Cliff refers specifically to the need to acquire adequate human resources, implement a coherent DX strategy and renovate the "existing, closed, overly-specific and outdated systems" by 2025. If companies cannot overcome these challenges, METI estimates that from 2025 the Japanese economy will lose up to 12 trillion yen annually.[1]

The Establishment of the Digital Agency and Its Mission

According to the United Nations E-Government Survey 2020, Japan ranks 14th among the 193 member nations in the development of e-government infrastructure and services. It occupies 3rd position in Asia, after South Korea and Singapore, 13th among OECD countries and 3rd among the G7 nations, behind the United Kingdom and the United States. Though not the top runner, Japan is nevertheless in a good position among the "very high rated nations", ahead of France, which is 19th in the overall ranking, Germany (25th) and Italy (37th). Moreover, the country boasts an internet infrastructure that is among the best-maintained in the world, a remarkably fast

[1] A summary of the report is available in English at: https//www.meti.go.jp/English/press/2018/0907_004a.html

connection speed and the availability of a wide range of digital services.

Yet during the recent pandemic, Japan suffered what the authorities themselves have called a "digital defeat". Although the country has contained the spread and impact of the virus quite well, with a relatively low number of infected people, hospitalisations and deaths, it has suffered several setbacks in its attempt to use the available digital infrastructure effectively and in a well-coordinated manner. In a country where high quality public services are expected to be delivered in an effective and equal manner to all its citizens, a series of delays and failures at the central and local government level has raised many eyebrows and fostered widespread criticism. In particular, the Japanese press and the public broadcaster NHK have pointed to delays and problems in the distribution of cash handouts, as the applications made on a website managed by the central government could not be verified on the servers of local governments using different systems. In another instance, the contact tracing app promoted by the Ministry of Health, Labour and Welfare failed to notify users when they met infected people. The problem, apparently caused by a computer system error, went unnoticed for four months. There were also problems in the planning and execution of the vaccination programme and reporting of infected cases. At the start of the pandemic, reporting was done by doctors and officials filling in and faxing paper forms. A computer-based method was later introduced, but this too was not without flaws.

The poor handling of the pandemic and the severe criticisms aimed at the government, whose popularity was constantly declining, induced Prime Minister Suga to prioritise the reorganisation of the government's digital network and services. In September 2021, after an unusually rapid approval of the related laws, Japan established the Digital Agency as part of the central government organisation. The launch of the new institution was announced with great fanfare and with even greater expectations. With a staff of about 600, including

many hired from the private sector, the Agency was initially headed by Prime Minister Suga, with Hirai Takuya as Digital Transformation Minister. Then, one month later, with the transfer of power from Suga to Kishida, the young (45-year-old) female politician Makishima Karen – educated at the prestigious International Christian University in Tokyo and at George Washington University in the United States – was appointed Minister of the Agency. And Ishikura Yōko – an experienced woman with a doctorate from Harvard, a career as a consultant at McKinsey and teaching assignments in first-class universities – was appointed to the key post of Chief Officer, the highest administrative position within the Agency. This was an unusual appointment for bureaucratic Japan, where the top positions had hitherto been reserved to career officials with a long experience, normally spanning several decades, in the relevant public administration departments.

The appointment in the still male dominated public service of two women, Minister Makishima and Chief Officer Ishikura, was heralded as a clear sign of the government's determination to move forward, without being constrained by traditional attitudes and ideas. However, as pointed out in the introduction, Ishikura has recently quit the Agency, and on 26 April her post was taken over by Asanuma Takashi, an engineer who previously served as chief design officer. Ishikura left the Agency for health reasons, but in a recent interview, published in a special issue on DX of the Japanese version of *Newsweek*, she openly complained about the hurdles she faced. In particular, she mentioned the difficulty in hiring human resources with high-level training in digital technologies and, consequently, a risky dependency on "digital vendors" who are just interested in expanding their business. This, she argued, is "a major problem concerning the future of Japan". The result, according to Ishikura, is a lingering incapacity to connect the different systems and databases adopted in the past, without any coordination, by each ministry and agency, as well as by the myriad of local institutions.

Overcoming the fragmentation and integrating the various platforms is indeed the most urgent task of the newly established Agency. To this end, the Digital Agency has been granted "strong powers of comprehensive coordination", such as the authority to make recommendations to other ministries and agencies. But will the proud and powerful ministries heed the advice of a newly born institution managed by outsiders? The impression is that the Agency's success in driving bureaucratic Japan in the desired direction will ultimately depend on the extent of the commitment of the Cabinet Office and of the Prime Minister. Kishida has repeatedly declared his intention to push resolutely for a green and digital transformation of the country, but it is too early to say whether his appeals and his determination will succeed in turning the tide.

In the *Newsweek* interview, Ishikura also talked about the difficulty in changing the mentality and way of working of the public administration, including the staff of the Agency she was in charge of. To quote her, "the problem is the lack of the concept of service and of a user-first attitude", which has made it difficult to develop effective programmes, tailored to the needs of citizens.

Yet, there are also problems at the receiving end, i.e., the citizens themselves, as can be seen in the slow adoption of the My Number Card, a centralised, electronic verification document issued by local governments. The card is meant to link the personal information dispersed across multiple agencies, thus providing a social infrastructure that can be used for various administrative procedures. The Digital Agency has been put in charge of its promotion, but the diffusion of the card has been slowed by the fact that the government has left it to the discretion of the citizen to apply for it. So far, only 43% of the population has obtained the document, revealing a contradictory attitude of the Japanese toward digitalisation, perceived by many as a potential threat to individual privacy: another major hurdle on the road to digital transformation.

The Private Sector

The delay in digital transformation is also a cause of concern for private businesses. Although Japanese companies and their managers are well aware of the need to promote DX, the reality is that many firms are stuck with closed, overly complex, outdated systems and are reluctant to introduce the necessary changes. They are even more reluctant to change their established business model and way of operating. Of course, there are significant exceptions such as Sony, which has successfully accomplished a dramatic turnaround with the adoption of a new business model based on the digitalisation of many of the services it provides. The company, a symbol of corporate Japan, was on the brink of bankruptcy at the beginning of this century but it is now one of the most profitable. Many other companies are actively engaged in DX, including some of the leading manufacturing firms, trading companies, financial institutions, construction companies and convenience store chains. For example, Komatsu, the world-class construction machinery maker, has successfully applied AI technology to the drafting of contracts and legal documents, significantly reducing costs and raising productivity. Toyota is engaged in building a smart city, named Woven City, at the site of a former car factory at the foot of Mount Fuji. Construction work started in February 2021, and eventually Woven City will have more than 2,000 residents, working and living in an interconnected environment, powered by clean energy sources – a fully green and digitalised world, where the car maker will be able to test automatic driving and AI technologies.

DX is also contributing to the upgrading of the country's transport infrastructure and the railway sector in particular. Actively introduced by the railway companies, digital technologies are further improving the efficiency and safety of the high-speed Shinkansen train lines. Moreover, they are a key component of the Maglev superconducting magnetic levitated train line, currently under construction between Tokyo and

Nagoya due to be opened in 2027. A major technological feat, the Maglev, which has already achieved a maximum speed of 603 km/h, will be remotely controlled from ground-based facilities via a fully automated train operation system, constantly monitoring the train position, speed And rolling stock conditions.

Yet, in general, Japanese firms are lagging behind their competitors, particularly American ones. As pointed out in the previously quoted 2018 "DX Report" released by METI, "some companies have launched efforts (e.g., establishment of a new department responsible for digital technologies) in order to address and advance DX. However, many such companies face difficulties in actually reforming their businesses through these efforts. While they invest in the efforts to some extent, the success of their implementation has been inconsistent".

The major problems mentioned by the report include the excessive customisation, often department-based, of existing systems, causing them to be too complex and closed. The report also refers to the rejection by employees of DX related reforms that affect the established procedures and operations. This issue is actually related to the still widespread practices of the seniority-based reward system and the so-called "lifetime employment" system, which normally allows "regular" employees, hired just after graduation or high school, to work in the same company until they reach retirement age. If on the one hand lifetime employment protects employees and particularly senior ones, on the other it hampers horizontal cross-firm mobility, mid-term career hiring and organisational reforms. In this regard, it is interesting to note that Sony, one of the leading DX companies, has always been critical of Japanese "traditional" labour practices and has consistently advocated the adoption of an employment and reward system more focused on the actual needs of the company as well as the skills and performance of their employees.

Another weak point raised in the 2018 Report is the widespread tendency of "information system departments to

accept the proposals offered by vendors without questioning them … and vendors tend to allocate their human resources and funds to maintenance of existing systems and do not fully shift their efforts to competitive business domains". As a result, "operational departments do not execute ownership, yet complain about the results".

This rather gloomy picture has not significantly improved since then, as we can infer from the 2021 White Paper on DX recently issued by IPA, the independent Information-Technology Promotion Agency. The report provides a detailed and comprehensive picture of the present state of DX in Japan. It is a picture with a few bright spots and many dark corners. The weaknesses and delays of DX in Japanese companies emerge quite clearly in the comparison with their American counterparts, based on a survey of 534 Japanese large and medium sized firms and 369 American ones active across a wide spectrum of industrial and service sectors. Carried out with the support of METI, the survey was conducted during the pandemic, between July and August 2021, via a questionnaire sent to top managers and those responsible for ITC departments. The purpose was to obtain information on three aspects: 1) the company's DX strategy; 2) the availability of human resources equipped with DX related skills and knowledge; 3) the extent of the use of digital technologies and the obstacles preventing their adoption.

In the case of Japan 30.7% of the participating firms belonged to the manufacturing sector, 20.4% were in retail and 8.1% in the financial sector. On the other hand, 24.1% of the US firms were in the ITC sector (against 7.5% of Japanese companies), a fact that might partly explain their higher propensity to engage in DX related activities.[2]

In general, Japanese companies appears to be less well-equipped to cope with the challenges of DX. The survey data

[2] A summary of the report, available in Japanese only, can be accessed at https://www.ipa.go.jp/files/000093699.pdf

confirm this point. Firstly, they show the large gap between the two countries' firms in the adoption of DX related initiatives. While 79% of the US firms are engaged in DX activities at the company or department level, this percentage declines to around 56% in the case of Japanese companies. What is remarkable is the gap in the manufacturing sector, with only 45.3% of Japanese firms implementing DX measures based on a company-wide strategy compared to 74.2% of their American counterparts. The difference in the two samples grows even larger when comparing the outcome of DX activities. While 56.7% of US firms engaged in DX already claim to have achieved significant positive results, a meagre 17% say the same in the case of Japan.

A third, striking difference relates to the degree of cooperation among top managers, IT departments and the business units. The American side boasts a large percentage of companies claiming a sufficient degree (40.4%) or a relatively satisfactory degree (45.8%) of cooperation among the three. In the case of Japanese firms, these percentages fall to 5.8% and 34.1% respectively, less than half of their competitors'. Among the obstacles preventing smooth and effective cooperation within Japanese companies is certainly the poor level of digital literacy expected from their company leaders: 9.7% in Japan against a robust 31.7% in the United States.

Regarding DX human resources, a large majority of Japanese firms state that they are insufficient (45% somewhat insufficient; 30.8% greatly insufficient). The situation is quite the opposite in the US, where a majority of respondents say that there is no shortage of ICT human resources and 10.6% believe that they are even in excess of actual needs. Another issue concerns the retraining (reskilling) of employees: while it is widespread in the US (72.1% of the companies), it is more rarely implemented in Japan (24%). This is a surprising result as Japanese firms have always invested heavily in their employees, although the traditional pattern of on-the-job-training is less suitable for the transfer of digital skills and there is an urgent need, underlined

in the report, to adopt more systematic training programmes at the company level. Japanese companies also need to be more aware of the degree of digital literacy of their employees, an aspect often neglected in Japan.

The last aspect examined in the survey is the introduction and the use of AI. In this sphere too Japan is less proactive. Although there was some improvement compared with previous surveys on this topic, only 20.5% of the firms have introduced AI technologies against 44.2% in the United States. Moreover, many Japanese firms are struggling to hire AI experts and their percentage is increasing, having grown from 39.8% in 2020 to 55.8% in the last survey.

Conclusion

While Japan is not losing ground in the field of DX, neither is it moving ahead of its competitors. At the government level and within the leading industrial and financial circles and the media there is a widely perceived need to shift gear, but, as we have seen, both the public sector and corporate Japan are slow and even reluctant to change their habits and their modus operandi. The risk is that they might act too late and, in the end, be left behind.

From a broader perspective, it is particularly important and urgent for the country to invest in human resources, in their education and training, but some recent trends point in the opposite direction and are an additional source of concern. Not only is the population declining and access to the Japanese labour market from abroad strictly regulated (even more these days), but there is also a worrying tendency to dismiss postgraduate studies as a meaningful investment. As was clear even before the pandemic, Japanese youth, living in a safe and comfortable country, has become less eager to pursue higher studies abroad. And private companies have been and are less willing to send their young employees to attend costly education programmes in foreign institutions. Moreover, the number and percentage

of young Japanese acquiring a doctoral degree is diminishing, a diverging trend from what is happening in other advanced countries. According to MEXT, the Ministry of Education, the number of PhD graduates peaked in 2006 and then started declining. This is an ominous trend for a country that absolutely needs a highly qualified workforce if it wants to remain at the forefront of scientific and industrial research. Yet, as pointed by many well-known scientists, in Japan having a Master's or PhD degree does not guarantee a stable and well rewarded job. On the contrary, in a country where wages still depend on seniority, spending many additional years in academia negatively affects career prospects. Ultimately, what is needed is a structural reform of the employment system and the workplace: a reform that could help to remove many of the obstacles currently affecting the process of digital transformation.

Conclusions

Carlo Secchi, Alessandro Gili

Digital infrastructure and technology are the engines and backbone of future economic growth. This is why governments around the world are considering digital infrastructure as a key tool for connectivity and an instrument for spreading their influence beyond national borders. Digital infrastructure is also a core element of leading nations' external strategies. Starting with the Digital Silk Road in 2015, China has invested about 17 billion dollars in digital infrastructure in Central and South East Asia, Africa and Latin America, with the goal of achieving geopolitical and strategic gains in the recipient countries. More recently, Western countries have made efforts to counter Chinese investments abroad, launching the Build Back Better World (B3W) plan announced at the 2021 G7 Summit in Cornwall. This plan aims to coordinate infrastructure investments in low- and middle-income countries and to ensure that infrastructure investments in third countries abide by and respect core human rights as well as financial and environmental sustainability. The G7 countries updated the plan in 2022, establishing the Partnership for Global Infrastructure and Investment (PGII). The G7 infrastructure framework is intended to provide about $600 billion dollars in investment in low-income countries who have considerable infrastructure gaps and need foreign capital to relaunch national growth. An important share of these investments will be devoted to connectivity and to reducing the digital gap in the recipient countries, ultimately boosting their growth and overall competitiveness. According

to the Final Communiqué, G7 leaders are eager to shape an inclusive and global digital ecosystem that fosters an open, free and secure Internet, competition and innovation, protects privacy and personal data, and promotes respect for human rights and fundamental freedoms. The idea of an open, free and secure Internet seems to be at odds with the Chinese vision of a fragmented Internet, in which national governments play a key role in regulating the flow of information through national-based data storage.

The G7 further stresses the importance of international digital cooperation within G7 Member States and with like-minded countries in order to strengthen the coordinated development of digital standards that encompass democratic values and principles and are based on a multistakeholder approach. The world's advanced economies have reaffirmed the importance of multilateral dialogues and fora to deliver democratic and market-oriented standards in technology, trade and innovation: these include the Trade and Technology Council (TTC), the Quad, the Future Tech Forum and the Global Partnership on Artificial Intelligence (GPAI), as well as the EU Declaration on Digital Rights and Principles. Against this backdrop, the G7 intends to facilitate the free flow of data across borders while addressing the challenges raised by security, privacy, data protection, and the protection of intellectual property rights.[1]

After the Russian invasion of Ukraine, the Digital Ministers of the G7 stressed the importance of protecting critical and strategic digital infrastructure (such as data centres and submarine data cables) and issued a "Joint Declaration by the G7 Digital Ministers on the cyber resilience of digital infrastructure".[2] G7 countries fear that the digital domain could become a privileged arena for hybrid conflict and have affirmed their determination to counter use of the digital sphere

[1] G7, G7 Leaders' Communiqué, Elmau, 28 June 2022.

[2] G7, Joint Declaration by the G7 Digital Ministers on Cyber Resilience of Digital Infrastructure in Response to the Russian War against Ukraine, Germany, 10 May 2022.

as a battleground. At the same time, they have denounced Russian cyber activities and information manipulation, as well as interference in the internal affairs of countries and online disinformation campaigns.

Geopolitical issues apart, the Digital Ministers of the G7 recognise that competitive digital markets are key to innovation and to the strong, sustainable, inclusive growth of the global economy. In particular, effective competition policy instruments and a new or updated regulatory and competition framework are deemed essential in view of the dynamic developments in digital technologies and markets.[3]

However, the G7 cannot be the ultimate forum to discuss and approve internationally recognised standards and principles. The G7 economies are not sufficiently representative of the international community as a whole. Shared rules and principles, as well as standards governing the digital space and digital infrastructure, must be agreed upon in a more representative forum such as the G20. During the Indonesian Presidency of the G20 in 2022, the Digital Ministers identified three main priorities for advancing coordinated digital investments worldwide, including digital connectivity, digital skills and literacy, and cross-country data flow. Building on the deliverables of the Digital Economy Working Group (DEWG), the Ministers stressed the importance of a people-oriented focus on digital infrastructure and of ensuring that investments are aimed at improving living conditions, especially in low and middle-income countries. To reach this goal, the Indonesian Presidency of the G20 established the G20 Digital Innovation Network (DIN). The DIN aims to become a privileged forum for sharing knowledge, encouraging discussion, and building partnerships among global innovation players, especially in the fields of healthcare, green and renewable energy, education technology, financial inclusivity and supply chain. The G20

[3] G7, Ministerial Declaration, G7 Digital Ministers' Meeting, Germany, 11 May 2022.

Digital Ministers also stressed the importance of encouraging international cooperation in overcoming gaps between countries and responding to the challenges of a digital future. Finally, the Ministers discussed the inclusion of justice, transparency and legitimacy in cross-border digital data governance. Ministers recognise that data has two important values: high economic value and geopolitical-geostrategic value to the sovereignty of each nation and state.[4] Previously, in 2021, the Italian Presidency of the G20 highlighted the importance of digitalisation as a means of creating opportunities for industry, transforming production processes and business models, and enhancing economic growth. The G20 has also underlined the need to support the inclusion of Micro, Small and Medium-Sized Enterprises (MSMEs) in the digital economy, since these are the backbone of the world economy, especially in developing countries. Moreover, the Italian Summit reiterated the importance of the G20 Artificial Intelligence Principles (elaborated during the 2019 G20 Summit in Japan) in ensuring the safe adoption of AI along with economic benefits for enterprises and citizens.[5]

Unfortunately, even in the most recent G20 meetings, a global approach to the coordination of digital infrastructure and investments has been missing. Cooperation among like-minded countries and regional blocs is prevailing, with a growing risk of investments overlapping in developing countries, financial distress and diverging standards in digital infrastructure investments. It is therefore of the utmost importance that international cooperative fora such as the G20, as well as technical bodies and international organisations, curb races to develop national and regional standards. Geopolitical considerations and diverging national and regional standards must be prevented from undermining the benefits of digital

[4] R. Khaerunnisa and U. Liman, "G20 Digital Ministers yields consensus on 3 priorities", Bloomberg, 4 September 2022.

[5] G20, "Declaration of G20 Digital Ministers. Leveraging Digitalisation for a Resilient, Strong, Sustainable and Inclusive Recovery", Trieste, 5 August 2021.

infrastructure. Global standards are key to promoting an open, interoperable and efficient digital and tech market. However, the world is facing uncertain times and the digital and technological fields are not immune to rising tensions. Cooperation in the technological and digital domains will probably be limited to the regional level in the near future, but conflicts and wars are temporary in nature. Competition may be beneficial to boost tech and digital advancements – as well as research – but cooperation on elaborating a minimum set of coordinated standards, principles and rules is key to fostering economic growth, promoting environmental sustainability, ensuring fair competition and avoiding chaos.

About the Authors

Rebecca Arcesati, Analyst at MERICS (Mercator Institute for China Studies).

Oliviero Baccelli, Academic Fellow at the Department of Social and Political Sciences, Bocconi University.

Annegret Bendiek, Deputy Head of EU/Europe Research Division at the German Institute for International and Security Affairs (SWP).

Monica Bennett, Director, Thought Leadership · Global Infrastructure Hub.

Seth G. Benzell, Digital Fellow at the MIT Initiative on the Digital Economy in the group on Productivity, Employment, and Inequality.

Alessandro Gili, Associate Research Fellow at the ISPI Centre on Business Scenarios and at the Centre on Infrastructure.

Pablo Gonzalez, Energy Investment Analyst at the International Energy Agency (IEA).

J. Scott Marcus, Senior Fellow at Bruegel.

Alberto Mazzola, Executive Director at CER (Community of European Railway and Infrastructure Companies).

Maxwell Means, LSU Public Policy Research Lab.

Luca Milani, Partner at McKinsey & Company.

Giovanni Miragliotta, Associate Professor at Politecnico di Milano.

Corrado Molteni, Professor of Japanese Studies at the University of Milan and ISPI Senior Advisor.

Julian Mueller-Kaler, Resident Senior Fellow with the Atlantic Council GeoTech Center.

Matteo Mussini, Advisor at CER (Community of European Railway and Infrastructure Companies).

Stefano Napoletano, Partner at McKinsey & Company.

Carlo Negri, Researcher of the Space Economy and Artificial Intelligence Observatories (Politecnico di Milano).

Ethem Pekin, Head of Economic Policy and Sustainability at CER (Community of European Railway and Infrastructure Companies)

Alessandro Perego, Professor of Logistics Management at the Politecnico di Milano and Scientific Director of the loT (Internet of Things) Lab.

Alessandro Piva, Director of the Cybersecurity & Data Protection, Cloud Transformation, Artificial Intelligence Observatories and Head of Research of the Big Data & Business Analytics Observatory at Politecnico di Milano.

Rafik Raji, Associate Fellow at CSIS (Center for Strategic and International Studies).

Andrea Ricotti, Specialist at McKinsey & Company.

Giulio Salvadori, Director of the Internet of Things and Connected Car & Mobility Observatories, project manager of the Smart City Observatory at Politecnico di Milano.

Nicola Sandri, Senior Partner at McKinsey & Company.

Carlo Secchi, Head of Centre on Infrastructure and Vice President at ISPI; European Coordinator for the Atlantic Corridor at European Commission, and Professor Emeritus of European Economic Policy at Bocconi University in Milan.

Gianluca Sgueo, Senior Associate Fellow, Brussels School of Governance - Centre for Digitalisation, Democracy & Innovation.

Isabella Stürzer, Student Assistant at German Institute for International and Security Affairs (SWP).

Angela Tumino, Associate Professor of Logistics and Production Systems Management at Politecnico di Milano.

Gelsomina Vigliotti, Vice President EIB (European Investment Bank).

George Yannis, Professor in Traffic Safety and Management at the Department of Transportation Planning and Engineering of the School of Civil Engineering at the National Technical University of Athens (NTUA).

Andrea Watt, Senior Advisor at EUROCONTROL.

Valentin Weber, Cyber Reasearch Fellow at the German Council on Foreign Relations (DGAP).

Georg Zachmann, Senior Fellow at Bruegel.

Apostolos Ziakopoulos, Research Associate, PhD, National Technical University of Athens (NTUA).